Training and Education for Network Centric Warfare: Issues for New Zealand's Defence Force.

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

Master of Arts
in
Defence and Strategic Studies

at Massey University, Palmerston North, New Zealand.

Eden Douglas Currey

2006

Abstract

The concept of Network Centric Warfare (NCW) is viewed as the next revolution in military affairs. Its introduction globally will necessarily affect the way the New Zealand Armed Forces operates in future conflicts. With the increasing use of digital technology in the military environment the need for and degree of increasing knowledge of Network Centric Warfare and its concepts must be explored. This country will have to combine its own definition and understanding of NCW into the framework of its Armed Force if it wants to continue to remain interoperable with technologically advance coalition forces.

This thesis looks into the issues and solutions which have been considered by other countries in their attempts to implement the NCW concept. It examines in detail how issues and solutions could be applied to New Zealand's attempt at NCW.

Chapters One and Two define the academic processes which have been used in this study. They also give a brief introduction to the broad idea of Network Centric Warfare and its origins.

Chapter Three examines in detail the complex evolution of the concept of Network Centric Warfare to its present state. In particular, it looks at how the events of September 11th 2001 have redefined warfare and the impact of that revolution on the traditional NCW concept. This chapter also focuses on the advantages and disadvantages of NCW which have now been proven through the experiences of Operation Enduring Freedom and Operation Iraqi Freedom. These two conflicts have been described as the first information technology wars of the 21st century.

Chapter Four focuses on how the concept of Network Centric Warfare has and will affect the specifics of personnel and make-up of the New Zealand Defence Force, as it makes the transition from a Platform Centric to a Network Centric approach in warfare. The special focus in this chapter is on

the New Zealand Army. The concepts of the ethos and cultural identity of a force are introduced here, with a view to revealing the influences that the adaptation of NCW methods and techniques can have on the organisation of that force. The discussion concludes that the introduction of NCW can have profound and permanent effect on a force's ethos and identity. This chapter also considers the influence of technology can help in the recruitment and retention of highly skilled people in the Army.

Chapter Five shows how the adoption of the concept of Network Centric Warfare also has the potential to fundamentally change the way in which higher level policy and doctrine are introduced and modified in the Armed Forces. This chapter looks at how future infrastructure and policies will need to have increased flexibility built into them from the start in order to embrace the demands of NCW for rapid developments in information technology and force-wide diffusion of such developments.

Chapter Six discusses a third important consequence of adopting the concept of Network Centric Warfare. Namely, how the introduction of NCW will affect both training and education of service personnel. In particular, it examines how the change from Platform Centric to Network Centric forms of warfare puts changing demands on the skill sets and needs required of service personnel. Examples are given of the new skill sets need in order for them to work effectively in a NCW environment.

Chapter Seven discusses the formation of a new training branch of service which will need to be set up to accommodate the new methods and skills that NCW brings to the battlefield. Included in this chapter are the imperatives of Information Warfare, Electronic Warfare, and Computer Network Operations for such a branch. Alongside Air, Land, Sea and Space NCW brings with it the creation of a fifth battle space. This battle-space is Cyberspace which encompasses the electromagnetic sphere, the Internet and all manner of Wide and Local Area Networks (WANs and LANs).

Chapter Eight returns to the issue of training and education introduced in Chapter Six, but focuses specifically on the use of simulation techniques and technologies. Such techniques will be required in order to help train soldiers to work effectively and efficiently under NCW. Why other training methods won't work well given an NCW environment, and why simulation technologies will work, is explained with examples of each. This chapter argues in particular that simulation provides the most effective training in the unified data architecture that will be needed to provide cross platform capability and inter and intra service solutions in Network Centric Warfare. Examples of data solutions are provided to help explain the underlying simulation concepts and methods.

Chapter Nine is the conclusion of this study. It reviews the results of this thesis and provides recommendations on the implementation of the Network Centric Warfare environment required in the New Zealand Armed Forces.

Preface and Acknowledgements

I would like to thank everyone who helped make this research project possible, through suggestions and research resources. I thank especially Dr Piers Reid, CBE, who supervised this project and gave guidance and direction when I needed it.

Also a special thanks goes out to my family who helped support me when the light at the end of the tunnel wasn't so bright. Knowing you were there when I needed your helped made this project possible.

A big thanks goes to the members of the Defence Centre at Massey University, especially Tania Lasenby and Major Vern Bennett, who helped answer some of the strangest questions which my research threw up, and who showed me the way through the endless paperwork.

Table of Contents

Tables and Figures

Abbreviations

2D	Two Dimensional
3D	Three Dimensional
AAR	After Action Review / Report
AARC	All Arms Recruit Course
ABCA	Australia, Britain, Canada, America
ACR	Army Capability Review
ADF	Australian Defence Force
AI	Artificial Intelligence
AKO	Army Knowledge Online
AOR	Area Of Responsibility
ATP	Army Transformation Program
AW	Asymmetrical Warfare
BBS	Bulletin Board Service
BFT	Blue Force Tracker
BOS	Battlefield Operating System
C2	Command and Control
C3	Command, Control, Communications
C4	Command, Control, Communications, Computers
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance
CDA	Command Data Assistant
CIS	Communications Information Service
CNO	Computer Network Operations
COA	Course of Action
CROP	Common Relevant Operation Picture
CSS	Combat Service Support
CWID	Coalition Warrior Interoperability Demonstration
DARPA	Defense Advance Research Projects Agency
DSTO	Defence Science and Technology Office
DCARR	Defence Capability and Resource Review
DIS	Distributed Interactive Systems
DOD	Department of Defense
DSI	Defence Sustainability Initiative
DT	Digital Technology
EW	Electronic Warfare
FBCB2	Force XXI Battle Command Brigade and Below
FLOC	Future Land Operations Capability
FOM	Federated Object Model
FPS	First Person Shooter
FSC	Full Spectrum Command
FSW	Full Spectrum Warrior
GIG	Global Information Grid
GPS	Global Positioning System
HLA	High Level Architecture.
HSS	Health Service Support
HVT	High Value Target
IA	Information Assurance
ICT	Information Communication Technology
IED	Improvised Explosive Device

IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
IPX/SPX	Internet Packet eXchange / Sequential Packet eXchange
IO	Information Operations
IO	Information Overload
IST	Information Systems Technology
IT	Information Technology
IW	Information Warfare
JCCS	Joint Command and Control System
JCIS	Joint Communication Information Systems
LAN	Local Area Network
LAV	Light Armoured Vehicle
LOV	Light Operational Vehicle
NCE	Network Centric Enterprise
NCO	Network Centric Operations
NCO	Non Commissioned Officer
NCW	Network Centric Warfare
NEA	Network Enabled Army
NEO	Network Enabled Operations
NET	New Equipment Training
NZA	New Zealand Army
NZASC	New Zealand Army Simulation Centre
NZDF	New Zealand Defence Force
MEUSOC	Marine Expeditionary Unit Special Operations Capable
MMORPG	Massively Multiplayer Online Role Playing Game
MS	Microsoft
OEF	Operation Enduring Freedom
OIF	Operation Iraqi Freedom
OPFOR	Opposition Force
OODA	Observe, Orientate, Decide, Act
PC	Personal Computer
PDA	Personal Data Assistant
RF	Regular Force
RMA	Revolution in Military Affairs
RNZAF	Royal New Zealand Air Force
RNZN	Royal New Zealand Navy
ROE	Rules of Engagement
RTS	Real Time Strategy
SF	Special Forces
SNCO	Senior Non Commissioned Officer
SOM	Simulation Object Model
SOP	Standard Operating Picture
TCP/IP	Transmission Control Protocol/ Internet Protocol
TERCOM	Terrain Contour Matching
TF	Territorial Force
TOC	Tactical Operations Centre
UAV	Unmanned Aerial Vehicle
UCAV	Unmanned Combat Aerial Vehicle
USARI	United States Army Research Institute
VR	Virtual Reality
WTS	Weapon Training System

Chapter One

Introduction: Network Centric Warfare and New Zealand

Many nations today would like to be able to enhance the capabilities of their armed forces without the need to purchase more equipment or expand the number of troops they have. Indeed, throughout history tacticians and strategists have always been trying to think of ways to project superior firepower against a numerically superior force without being required to field a force of equal numbers. Success has mostly come from the introduction of new technology and new concepts of war to the battlefield. From the spear to the catapult to the airplane, these systems have tried to increase the firepower being able to be delivered without risking soldiers' lives. The present day New Zealand Defence Force is no exception to the need for such innovation and invention.

The New Zealand Army and the New Zealand Defence Force are currently going through a transitional period in their development. With the introduction of the Defence Capability and Resource Review (DCARR) and the Defence Sustainability Initiative (DSI), the New Zealand Government is increasing the resources available to the Defence Force. These resources are targeted to regenerate and expand abilities and capabilities that have atrophied due to lower funding levels from previous governments. This development is providing the right environment for the New Zealand Army to invest in military

digital technologies and thereby catch up to international levels in Network Centric Warfare (NCW).

The New Zealand Army's efforts are guided by the Networked Enabled Army (NEA) programme. Three categories of investment are specified in this programme. (1) Investments in modern digital technologies; such as data networks, these include Internet, Intranet, Terrestrial Cable Networks plus Wireless and Satellite networks. (2) Investments in the Information Communication Technologies; these include IPv4, IPv6, TCP/IP, IPX / SPX. (3) Investments in Information Systems; these comprise Personal Computers, Personal Data Assistance, Inter vehicle Information Systems. These three categories are used to integrate individual units, weapons systems and weapon platforms that generate faster operational tempo and superior firepower for soldiers on operations.

These results come through the application of superior situational awareness on the battlefield which is made possible by such integrated digital technologies. Indeed, the very expression "I know where I am, I know where my units are and I know where the enemy is" is derived from integrated digital technologies. Given them, War Fighters have the ability to call on increased firepower from non-organic assets, assets which do not belong to or are not under the command of a selected unit, via the NCW systems.

Network Centric Warfare is not just about enhancing the capability of a particular weapons platform or system, however. Nor is it just about applying enhanced firepower from many sources to a combat situation. It is as much about the support structures that are used to keep a force moving, supplied and educated. NCW is a whole system approach and can have influence on the whole military process from training, deployment, engagement, and retrieval all the way to future policy and doctrine.

One of the key areas for the implementation of digital technology and of the NEA is in training and education. New skill sets have been identified by international NCW research; these are the skill sets which would need to be

introduced to the New Zealand Army training system if the Army wants to remain interoperable with coalition allies already proficient in NCW. New Zealand Army doctrine and Joint Force doctrine may also need to be reconsidered or remoulded in order to make available the full effects that Network Centric Warfare and Network Enabled Operations (NEO) can achieve. Such changes in training and doctrine will lead to soldiers being fully trained in digital technology methods and equipment.

Even if the New Zealand Defence Force decides that it does not want to engage in a complete conversion to Network Centric Warfare, there still needs to be an awareness of its capabilities within the NZDF. This is so because otherwise no effective defence can be maintained against external NCW threats nor modern subversive threats within New Zealand. For example, the NCW concept links the Armed Forces with both the commercial and private sectors via its integrated logistics and supply system; whatever direction the NZDF takes, these digital lines of communication and supply will have to be protected in any future conflicts just like any other physical supply line.

Network Centric Warfare can be a great benefit to the New Zealand Defence Force. Its implementation and management will take time and resources, and there are huge issues and pitfalls ahead for this concept in New Zealand. However, its implementation has the potential to produce a world-class force equal in ability to any in the world.

Chapter Two

Research Methodology

The method of research used in this thesis was to review and compare research reports created by the coalition allies that New Zealand has aligned itself with. The main resources and research documents came from the members of the so called "ABCA" – that is, the Australian, British, Canadian and America coalition. This group of nations is leading the drive in NCW research globally and provides the best indicators of where the concept of Network Centric Warfare is going. The vast amount of research documentation available from both military and commercial sources has sometimes threatened to overwhelm any constructive focus for a thesis on NCW. Early on, therefore I decided to define the boundaries of this thesis to just those methodologies, technologies and practices which it would be practicable for New Zealand to implement given the current personnel size and financial resources of its Armed Forces.

Research Hypothesis

The over-arching question that I am researching in this thesis is the following "Can Network Centric Warfare, and training and education for NCW, be made to work for the New Zealand Defence Force? " *My research hypothesis was that NCW can be implemented, starting immediately, but that there will be quite specific consequences for the methods of training required in order to make the NZDF competent enough in NCW to be inter-operable with its coalition partners.* These consequences for training have been identified through the research of this thesis; some of the methods have been tested in

practice with the New Zealand Army Simulation Centre (NZASC). To this extent the research hypothesis of the thesis has been confirmed.

The Scope and organization of the Study

The thesis is structured so that the concept of Network Centric Warfare can be defined and the decision to adopt NCW in New Zealand can be placed properly in a global context. One these issues are clarified, then further questions can be usefully raised about the impact of NCW on the personnel and organization of the New Zealand Defence Force. The thesis looks at the current situation of the NZDF and the NZ Army as it regards to NCW, it also starts to describe approaches and methodologies which other nations already fully committed to NCW have used. By assessing their results up to now at NCW, this thesis investigates whether the NZDF and NZ Army's attempts at creating a NCW environment can be smoothly up-scaled if New Zealand opts for a wholesale adaptation of NCW.

The thesis then moves onto the technical side of Network Centric Warfare and the practical application of NCW technology. The key aspect examines here is the development of processes which will help introduce service personnel to the concept and consequences of NCW. These processes and their development will be the new focus required of the traditional training and education areas.

A refinement of these issues comes by looking in detail at NCW through the application of one specific training procedure for NCW, namely simulation technology. Practical examples where simulators are used for combat training in a Network Centric Warfare environment have been developed in response to the events of Operation Iraqi Freedom and Operation Enduring Freedom. These examples are set out in detail here in order to reinforce concepts and ideas which are widely employed by New Zealand's major allies. Training by simulation also turns out to have interesting consequences for policy and doctrine in the New Zealand Defence Force.

As a means of balancing and validating the NCW concepts and methods proposed in this thesis, three nations with comparable sizes and financial resources have been selected. They are Sweden, Ireland and Norway. These nations are using the same international NCW resources which New Zealand can access. However, they are also using unique ones as well, thus New Zealand has the ABCA and the other nations have NATO. Where applicable, examples from these nations have been used to show an alternative experience of NCW or to demonstrate the real-life consequences of a certain defined action in a NCW simulation.

Limitations of the Study

Unfortunately, this study has been limited to just the areas of NCW that impact on training and education. This limitation was not anticipated during the initial phases of research. As the thesis progressed, however, research into other aspects of New Zealand's attempts at NCW ran foul of a "closed-door" approach to advanced research by external personnel imposed by the New Zealand Defence Force. This closed-door limited access to current publications and research being done within the NZDF itself, it also restricted access to key personnel and in-house research reports. The result has been a severe restriction of information about the technologies and research actually being used by the NZDF in its evaluation / implementation of Network Centric Warfare.

Another limitation is more obvious and was anticipated from the beginning. The NCW concept has a very wide scope, and many things are involved in its implementation. Issues such as force organizations and combat deployments have not been researched to their full extent.

Literature Review

The publicly available literature falls into four distinct categories: (a) Military, (b) Commercial, (c) Academic and (d) Civilian.

(a) The military documentation came from the international defence forces research sections, such as the United States' Defense Advance Research Projects Agency (DARPA), the United States Army Research Institute (USARI) and Australia's' Defence Science and Technology Office (DSTO). Documents from these sources came in the form of research reports, presentations, survey results, future doctrine concepts and white papers.

(b) The commercially available material came from major international companies such as Microsoft, Boeing, Raytheon and Rand. These documents comprised technical reports, media releases, equipment manuals and presentations.

(c) Academic resources included post-graduate theses and dissertations, conference papers, and other reports of University research (both published and unpublished) and Conferences. International defence journals, such as the International Defence Review, Janes Defence Journal and New Scientist also provided information.

(d) The civilian NCW resources came from primarily online web logs and reviews. Of special interest were the journals of soldiers and service personnel who put forward their perspectives on the use of NCW technology and techniques in combat environments. This area also included television documentaries, for example from the History Channel and Discovery Channel. I conducted no personal interviews.

The majority of all four forms of publicly available research material derives from sources within the United States. This is due to the huge financial capabilities and resources which the United States has put into NCW research. The United States has the ability to diversify its research into smaller sections and defined focuses. As a consequence of this, most of the publicly available material contains an inbuilt bias to groups with large financial resources or forces of equal capability to itself. This has different consequences for each of the four different categories.

(a) In terms of the military documents, the larger Joint picture tends to be left fractured for outside observers due to the individual service focus of the research and restricted access for non government, and non service, personnel. A single repository has not been established for easy access to all relevant research data. Individual services and branches of those services have independent repositories of relevant data. This means that any researcher into Network Centric Warfare must to look in multiple areas and services domains to gain the best view and access to relevant resources and research. There is another caution to be exercised with the current literature is showing the possible capability that the NCW systems can have on a defence force. However, these assessments are mostly made on the basis of systems which are still in development and exist only in theoretical form or prototypes. Preliminary computations from theory and results from the preliminary use of prototypes are then projected onto an active battlefield; very little of the research into NCW systems has been confirmed or disconfirmed by their actual use in combat.

(b) Most of the commercially available literature focuses on the specific aspect of NCW which the companies concerned are developing. As no company will show or demonstrate flaws or issues with their systems, particularly in a document available to the outside public, the commercial literature is skewed towards success. This has been proven with the Insis systems program from the New Zealand Police, which is still not working after nine years of constant development and modifications by the supplier and manufacturer. Such failures, and success/failure rates generally, go little published by the companies concerned. In the literature systems are discussed working at 100% and in optimal conditions.

(c) Academic resources have generally been peer-reviewed, but still of course aspects of the writers' personal beliefs and views are contained in their articles. Any biases about Network Centric Warfare which the writer, or the peer reviewer, has as an academic (and hence to an extent "outside the system") can skew starts the relevant information just as much as with the commercial literature. The researcher must exercise another caution too.

Even with the resources and personnel available to them, some journals and academic writing cannot publish full articles due to security and classified information associated with NCW. The academic literature can sometimes tell only part of the story, therefore, and sometimes cannot report even that it is partial.

(d) The special concern with the civilian resources derives from the issue of frequent anonymity of the publisher. Anonymity can be for many reasons and can hide many sins. Sometimes, however, it can be a consequence of the military's ability to punish or discipline soldiers or service personnel who speak out against a technology or method. To avoid punishment the writer is forced to hide their identity, publish under a pseudonym or change events to obscure information about themselves or others involved. This hinders the researcher's ability to verify and validate the information which the anonymous author does provide .At the very least, anonymity always leaves a speculative doubt as to its authenticity. This issue became more relevant with the use of web logs and online journals where the sources were sometimes even harder to find or validate.

There is a more general difficulty faced by any researcher into Network Centric Warfare, due to the special nature of NCW. NCW is essentially a military concern and the military restricts access to what concerns it. It is a fact of life that all of the data is difficult if not impossible. In particular, most resources that can be found by the general public have been either declassified after they become irrelevant, or have been superseded by other resources which remain classified, or have been re-modified to remove any information that could expose flaws in the systems in use or reveal concerns about specific systems or units. These sanitised reports are complete to an extent but are not the full research. The nature of the integrated systems used in Network Centric Warfare has made security issues and flaws a high priority for a military force. Their protection has become a national security concern, which allows any NCW country to restrict any information they deem fit.

Access to western research has been difficult enough, and special difficulties will be discussed as they arise in later chapters. Access to non-western research has been even more difficult for the same reason, the nature of the topic. However, a few research resources and publications have become available to give a glimpse into what non-western forces (such as China) are doing. Non-State[1] entities are also researching what benefit NCW will have on Asymmetric Warfare (AW)[2] from the point of a guerrilla group or insurgent force[3]. The tactics and techniques in countering NCW have provided a good insight into the financial aspects that NCW requires, and how to overcome them. For example, in Mogadishu Somalia, children were given cell phones to call in the direction and number of units deployed away from a US base. This simple approach completely nullified the speed and force the United States was able to deliver against the local warlords; the warlord could leave before they arrived.

The New Zealand situation is beset by restrictive access. Research and publications on NCW done here are still restricted to service personnel with a high security clearance. No access is given to the general public. New Zealand will need to open up its research base to other inputs from the science and academic community if it seriously wants to stimulate debate and research on the topic of Network Centric Warfare and its associated technologies. A closed-door policy will not help the advancement of the knowledge base. Indeed, a closed-door approach goes counter to the very definition of a knowledge based force, a core requirement of the New Zealand Defence Force's own future doctrine concept[4]. Most information about work on NCW in New Zealand has to come from public documents made by the NZDF for Parliament, such as the NZDF Statements of Intent or the NZDF Annual Reports.

---

[1] Such "Non-State entities" encompasses such entities as international crime groups, terrorist organisations, and to a lesser extent media firms.
[2] Biddle, S. (2003). "Afghanistan and the future of warfare", Foreign Affairs, vol. 82(no. 2): **Pages** 31.
[3] Venzke, B. (2003). Al-Qaeda's Advice for Mujahideen in Iraq: Lessons Learned in Afghanistan, retrieved from http://www.intelcenter.com.
[4] New Zealand Ministry of Defence, (2004), Foundations of New Zealand Military Doctrine (NZDDP–D), New Zealand Government: Page 10-1.

Chapter Three
The Concept of Network Centric Warfare.

Network Centric Warfare is the latest evolution in a long history of using computers in the conduct of war. It will be easier to understand the NCW concept if a few of the more critical stages of its evolution are explained first.

History of the Concept

The origins of modern Information Systems and computers can be traced to the early days of World War Two. Basic computer systems were heavily used by the Allies to help break the codes and ciphers employed by the military and diplomatic communications by the Axis powers. Simultaneously, the Axis powers were also using rudimentary computer systems themselves, not generally for code-breaking but for weaponry, to help guide the advanced rocketry systems being developed. On both sides, the computers used were designed with vacuum tubes, which were the precursor to modern microprocessors. Although these systems could process numbers with amazing speed for their time (the same processing strength as a modern pocket calculator), their immense size meant that they were not at all mobile and so of little use in the combat zone.

After the end of World War Two computers started to appear in universities across the United States. These systems were being put in place primarily for the advancement of the physical, engineering, and biological sciences. For example, large computer systems were used to simulate the effects of nuclear explosions or the interactions of atoms. As the simulations increased in complexity, individual computer systems could no longer cope with the data

processing requirements or the amounts of data being produced. Therefore a solution was needed to help the progression of "big" science and the growth of university-based research. The United States government decided to invest in an interlinked network of university computer systems that could share both data and processing power. (Although secrecy was not a paramount issue, it was already built into the idea simply from the fact that the individual computers networked together were each sited on a university campus and the network linking them ran through special landlines.) The project was hugely successful.

From that success the United States Department of Defence started to see a wide range of benefits to being able to securely send and receive data between computers in different locations. Of special interest was the prospect of being able to protect military information from a possible nuclear strike by having it stored in different locations to be retrieved as needed. Such an arrangement had overwhelming strategic benefits during the Cold War. For instance, logistics and personnel numbers could be stored and retrieved to help with the planning and deployment of troops any one location to any other; codes and procedures for combat could be widely dispersed so that if one command centre was wiped out another could be take its place, instantly equipped with all the combat the data the other had; indeed, the very apparatus of government could be made invulnerable from destruction by having its information base located all over the continental United States yet available from anywhere.

Military theorists and researchers in the 1960's began to explore the potential benefits of making computer systems work in a more integrated way than merely sending and receiving data. Deeper levels of integration held promise for both the operational and tactical levels of war. The first major breakthrough came by the interlinking of radar systems in such a way that the information generated by each was fused into a single whole. This gave commanders a complete air picture of the battlefield instead of the several partial views which they had to integrate as best they could themselves. Fusing data from multiple sources generates better information than those individual sources could

manage by themselves. Military scientists theorised from this success that the same approach to integrated systems could deliver a similar tactical advantage over the numerically superior forces of the Soviet Union. The Soviet forces applied the traditional approach of trying to gain numerical superiority of at least 3 to 1 in any engagement. However, United States scientists noticed that even when such numerical superiority is achieved, each unit was an individual piece, connected to other units only by voice communications or signals. The scientists reasoned that Integrating their own battlefield units as multiple sources generating fused information could well be enough to offset even large imbalances in the numbers of units deployed. Fusion of data from interlinked sources had already been proven to deliver better command information than un-fused data from those sources taken individually. It was reasonable to hypothesise that fused data is **so** much better that even increasing the number of non-interlinked sources to 3 to 1 would make little difference to the comparative quality of the data generated.

Such reasoning ushered in a change to the doctrine of warfare in the final years of the Cold War. Gone were the days of checking the numerically superior forces of the Soviet Union by the threat of tactical nuclear weapons under the doctrine of Mutually Assured Destruction (MAD). The process of overcoming numerically superior forces would now be achieved by the use of computers and information communication systems. The change here is a fundamental one. The relevant concept of war is no longer the old one, that a country must possess weapons so powerful it becomes unthinkable to deploy them. The relevant concept now is that a country must so integrate personnel and weaponry that numerical size ceases to be the prime consideration. The process of overcoming forces superior in number by forces superior in computer integration would become the main focus of the Regan administration in the 1980's. This was the focus, for example, of the (now defunct) Strategic Defence Initiative (SDI); it continues to be the focus of the research centres set up during this time by the Department of Defence and still going strong.

One might expect that the concept of Network Centric Warfare has its origins in the same place, with the other developments of the Cold War. This is not the case however. Although part of the same general evolution of computer technology for the conduct of war, the origins of NCW lay in the period of the Gulf Wars rather than the Cold War. Specifically, the NCW concept received its initial formation in the experiences gained from Operation Desert Shield and Desert Storm in the early 1990's. Several doctrines about the conduct of war swiftly developed from these experiences: First, the AirLand Doctrine of the early 1990's. Second, Rapid Dominance doctrine which was developed as the next step from the AirLand Doctrine in the middle 1990's. Third, the doctrine or concept of Network Centric Warfare which evolved from both in the late 1990's.

The Gulf War of 1990-1991 is the turning point for NCW. The Gulf War is pivotal because it introduced digital technology to the actual battlefield for the first time. Previous to that, digital technology was always in the rear. Now it was everywhere.

Thus satellites and reconnaissance planes and drones took real time images of the conflict on the ground; these were beamed directly to the Allied Headquarters in near real-time; there quick decision-making could be achieved and tactics changed as the combat situation required; decisions were communicated back to the combat units by field radio or microwave transmissions. The new Global Positioning System (GPS) gave commanders the ability to drop munitions on targets with only a six-meter error zone; linked to near real-time, fused, imaging of the whole field of combat, enemy forces could be hit and even nearby friendly forces reliably avoided. The missiles used in the Gulf War were digitally integrated systems too; they did have to have their targets pre-programmed before launching, nor were they flown by wire; Cruise missiles followed digital terrain maps to their targets, using their own, Terrain Contour Matching system (TERCOM); these maps were generated in-flight from space-based systems with near real time laser mapping technology. The M1A1 Abram Main Battle Tank used in the Gulf War was digitally integrated with other combat units as well; it was equipped with

both internal digital communications and data management system[5] these enabled tank commander's to see where all their units were at any point and thus to coordinate combat on the fly. The Abram and Bradley Infantry Fighting Vehicle (IFV) were not so digitally integrated; but they were equipped with new generation night vision systems; surprisingly the troops inside had night vision goggles too; the result was that darkness no longer gave as much cover as once it had. For the large platforms, the battlefield had become a 24-hour event[6].

The individual soldier on the ground was also enhanced by the new technology revolution. In particular, s/he had more killing power than ever before, and a lighter pack. This enhancement came from two directions primarily: new training methods and new weaponry. Both were heavily enriched by computer technologies. For a start, Gulf War soldiers were psychologically more fit for combat because of the use of computers in their training. This included effects based training, such as realistic training targets, virtual reality training and the "train as you will fight" mentality. New thought patterns and processes, constructed through simulation training, made the soldiers more self-aware and made them more lethal even before they were physically armed.

Equipped with the latest weapon systems, such soldiers became the total package for modern warfare and conflicts.[7] Digital data communications enabled the individual soldier to call up artillery and air support within moments. It also gave them access to the latest intelligence reports, weather reports, GPS positioning and digital satellite images of the battlefield.[8] Using the new battlefield laptop computers, troop movements could be traced, access to real time logistics could be provided, also fire support, and organic command assets could be ordered. The only limitation was the bandwidth available to send and receive the data.

---

[5] Antal, J. A. (1999). "The End of Manoeuvre," in Digital War. R. L. Bateman (ed). **: Pages** 153.
[6] Coker, C. (2004). The Future of War , Retrieved from www.fas.org 31/04/06
[7] Hosek, J. H. (2003). "The Soldier of the 21st Century," New Challenges, New Tools for Defence Decision-making. **Pages** 181.
[8] TACOM (2004). Future Combat Systems,. Retrieved from http://www.army.mil/fcs 15/06/06

Network Centric Warfare is the product of continued enhancements along the same lines as those brought to the battlefield in the Gulf War. The most important of these developments has been the integration of Information Systems and Communication Technology (ISCT) into the battle space. Nonetheless, Network Centric Warfare should not be regarded as just an add-on to current methods. After all, simply tacking on more and more computer technologies in a system, even integrating them with more and more of those already in place, doesn't necessarily mean that the network centricity of the whole is increased. Yet it is precisely the idea of network centricity which is the heart of the concept of Network Centric Warfare. NCW must be regarded therefore as an entirely new way of waging war. It is a whole system approach. Applied to next generation warfare, this means that all aspects of warfare, across the board, will be influenced in some manner by the methods and techniques designed to ensure network centricity.

Analysis of the concept

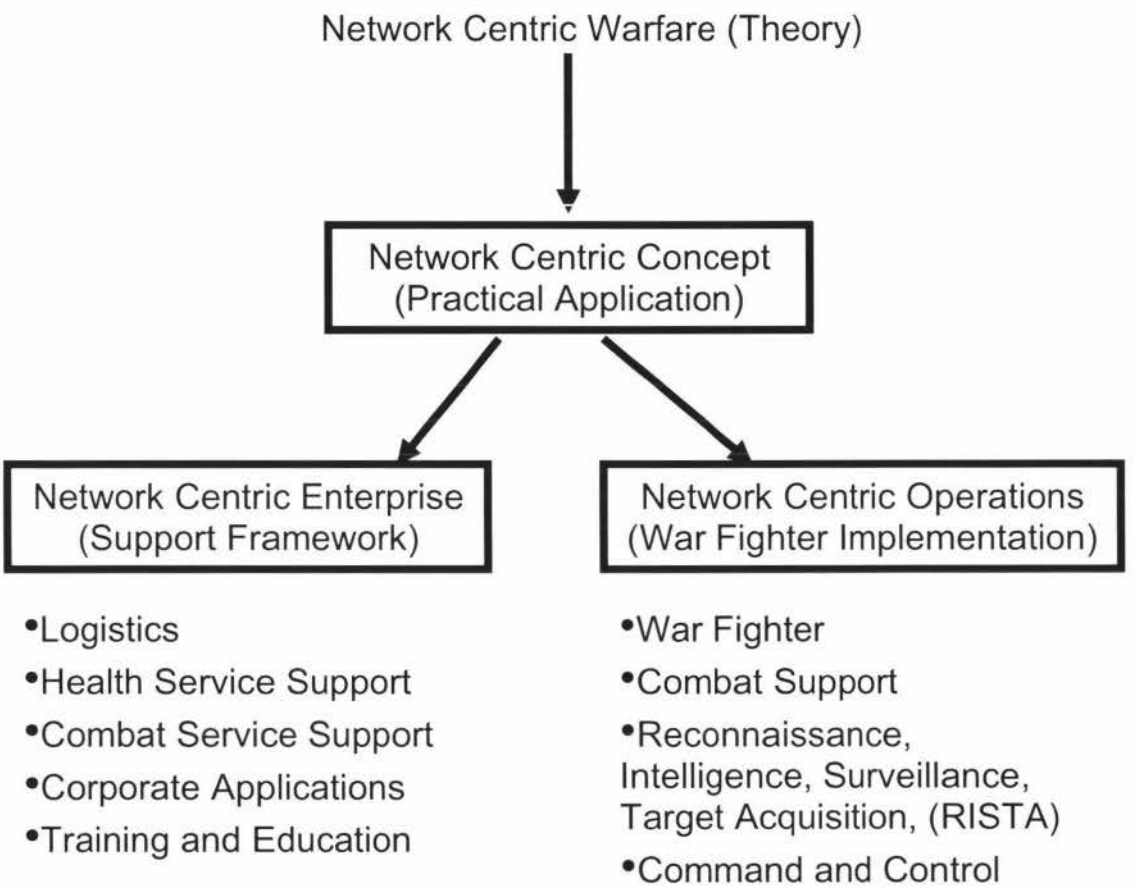
NCW has been described by most researchers as the definitive step from the Industrial Age/ Platform Centric (Tanks, Airplanes, Warships) environment to the Informational Age/ Network Centric environment. New standard and practices are being developed to ensure that the technology works to its full prescribed potential[9]. But with all of this the concept of Network Centric Warfare is still in its development stage. A unified and internationally accepted definition has yet to be created. Most countries look to the American definition for guidance, because of its influence in global military matters generally. But there are still issues to be sorted out before an adequate specification is internationally accepted.

---

[9] Talbot, D. (2004). "How Technology Failed in Iraq, " Technology Review: Emerging Technologies and Their Impact, retrieved from http:/TechnologyReview.com/Infotech/13893/page1.on 18/03/2005

Most major NCW publications suggest that Network Centric Warfare can be split into two areas, Network Centric Enterprise and Network Centric Operations[10].

Figure 1[11]



Network Centric Enterprise[12]**:** This element has strong ties to the business and commercial sectors, as most of its framework derives from the organisational structures widely adopted in the public and private sectors. The main task of the Network Centric Enterprise system is the support of the War Fighter and the running of the Rear Area of the defence organisation. Tasks

---

[10] Alberts, D. S., J. J. Garstka, et al. (2000). Network Centric Warfare: Developing and Leveraging Information Superiority. Office of Force Transformation: **Page** 287.
[11] Derived from research from Defence Advance Research Projects Agency (US), Defence Science and Technology Office (AU) and United States Army Research Institute (US)
[12] Luddy, J. (2005). The Challenge and Promise of Network-Centric Warfare,: **Page** 15.

such as general administration and formation level logistics fall into this element. Rear Area[13] tasks do too, such as logistics convoy security, formation level maintenance and refit, port security, etc. Computer systems of the Network Centric Enterprise can be used to track, trace and list stock levels, transport routes, items in transit, how ships have been packed and what is onboard, even before they reach a dock or porting facility. These systems can, and will have to, track each individual piece of equipment through the whole system from creation to destruction, its entire life cycle. There is no special need for such tasks to be performed by the forces actually engaged in conflict, since "Where's my gear?" queries can always be exchanged between Front and Rear as the situation requires. This is what makes them the proper concern of the Network Centric Enterprise element rather than the Network Centric Operations element. Likewise for the other tasks listed on the left side of Table 1.

Network Centric Operations[14]: This element covers the war fighting tasks and the engagement area of the battlefield. The responsibility of the Network Centric Operations element is best understood as the integration of all combat assets into a single lethal force, from remote sensors and the C4I (Command, Control, Communications, Computers, Intelligence) all the way to the soldier on the ground. This integration gives the War Fighter on the ground many more organic assets to utilise than were ever traditionally available under platform centric warfare. Assets now organic to the War Fighter include artillery, intelligence drones, and even satellites in space. These far-flung assets are also, of course, made organic to the War Fighter's commander thereby improving the commander's situational awareness of the battlefield and surrounding areas – and himself.

Integrating all combat assets into a single lethal force brings obvious advantages. The most general advantage is that a force can project greater

---

[13] Battlefields are divided up into 3 areas on both sides of any military engagement, Front, Rear and Deep.

[14] Enemo, G. (2005). Analysis of Command and Control (C2) in Network Enabled Operations (NEO), . **Page** 8.

power even while deploying fewer assets (in particular, fewer war fighters). More important, however, and more characteristic of NCW, is that integration allows a force to deploy a more modular force than traditionally possible, but which is at the same time more flexible than ever before. A modular force is one which is focused on military tasks and missions as opposed to personnel and equipment (as in platform centric warfare). This is a step forward. But a flexible modular force is a step further forward still. Such a force has the ability to change the tasks and missions quickly to adapt to the changing environment. Integration allows modularity and flexibility. Modularity and flexibility allow smaller forces that are tailored to their missions, and changing those missions and forces on the fly as conflict evolves. No longer required is the "catch all" force designed in advance to be able to do anything which might be expected to happen. Not only are there always surprises in war, but such forces generally take too much time and resources to deploy to be victorious in the rapidly shifting engagements typical of modern warfare. The current situation in Iraq provides a good example of the Platform Centric Warfare loosing and Network Centric Warfare winning. Traditional large armoured forces are taking too much time to be deployed and configured to the needed mission, before the next situation develops elsewhere. Compare that to the new modular, network centric, Stryker battalions, which can be deployed and active in a conflict or engagement within 48 hours globally and reconfigured on route to a new conflict. The difference is the integration provided by the Network Centric Operations element of Table 1

One common mistake in many discussions of Network Centric Warfare is getting the two concepts of network enabled and network centric, confused with each other. These are essentially different concepts and need to be kept quite separate. The first concept does lead into the second concept, but they are still distinct concepts for all that.

- **Network enabled** is a concept that strictly applies only to the physical connections between assets and locations. For example, take the visual sensors located on a reconnaissance drone in

flight and a computer system picking up its signal located on the ground. When assets and locations like these are linked via physical connections such as fibre optics, wireless, and satellite, then they are properly referred to as network enabled. Of course, ordinary phone wire can be network enabling too – though phone wire is not usually suitable on the battlefield. Whatever the physical connection happens to made of, network-enabled is not concerned with the type of data, but just the method of data transmission.

- Network centric, on the other hand, is concerned with the relationships between assets. As far as the application of the concept of something being network centric goes, the information which is being sent has more importance than how it is sent. That information uses the physical framework provided by a network enabled environment – that is, an environment in which the parts are physically connected by fibre optics or the like – but the information itself is still one thing and the physical environment another. To that physical framework, the information adds what is usually called a context framework. For example, the information being sent might be the information that such and such element of a military force is a platoon of troops and that another element is an asset such as artillery. Another example of the kind of information that might be sent over a physical framework is what such an element as a platoon of troops can do or how fast an artillery element can respond in a certain situation. Such information is obviously additional to the physical framework; what it does is create a context for the signals sent through the network of fibre optics or radio signals. The physical environment is enhanced with a contextual environment. The fact that a certain piece of information is being sent from a certain physical now "means" something: that the enemy has been spotted and the artillery can be brought to bear on that spot in four seconds and so on. A system of assets and locations connected by a physical

framework alone is network enabled. A system in which that physical framework has been enhanced by a context framework is what is properly marked off as network centric.

In Network Centric Warfare it all comes together like this. The physical framework is created by the engineers. The contextual framework is created by the military planners. They know what each element of a military force is and what it can do; that knowledge helps in the creation of the context for the, now, network centric framework. The elements are more commonly known as "nodes" on a network. And the most common context created is known as the "Sensor - Decider - Shooter" model.[15]

The "*Sensor - Decider - Shooter*" model

The context created for NCW is known by this phrase to mark the fact that any node on the network could have one or more of the following aspects:

- ***Sensor*** means that the node on the network can sense an object, either allied or enemy. Such sensing is usually through the use of optics, i.e., infra red, night vision, zoomed optics and even standard human eye sight. But the sensors are not limited to optical devices; there are also anomaly sensors, such as seismic, magnetic and thermal.

- ***Deciders***, at the node elements, are the units which evaluate alternative courses of action (COA) and choose which to take using information supplied from either other decider nodes or from sensor elements. They can send their decisions to an action node (Sensor, Shooter) for implementation. They can also send their decision onto another decider node for information sharing in the enhancement of situation awareness and information assuredness.

---

[15] Ibid.

- ***Shooter*** nodes are the action aspect of the network; these nodes employ the firepower of a force. Shooter nodes can be in the form of an offensive/ defensive platform, such as tanks, artillery, aircraft, or naval ships. But they run the whole spectrum of units which deliver firepower, down through to the unit formations of soldiers in the field and even individual war fighters if necessary.

As already mentioned above, it is possible for elements or nodes on the battlefield to have more than one aspect. For example, a sniper/scout unit has the ability to be both a sensor and shooter, and to a lesser extent a decider. The sniper/scout unit can be deployed to observe and report back its sightings to other nodes on the network in order to increase overall situational awareness or to provide information to decider nodes, such as a Tactical Operations Centre (TOC). Typically, however, sniper/scout units also have the ability to decide on their own course of action when they need to. Thus if a High Value Target (HVT) appears unexpectedly and the mission orders allows the flexibility to engage HVTs, the sniper/scout can sense its target, decide on its action and shoot, if it deems such action necessary. Higher level decider nodes, such as command centres, can intercept or stop the sniper/scout from taking the shot on the basis of a fuller awareness of the battlefield situation provided by the other nodes of the network. But equally the autonomous function of the sniper / scout unit can be allowed to run its course. The flexibility which the Sensor – Decider – Shooter model provides moves NCW away both from the directed mission command and from command that automatically takes over when it has a higher awareness[16].

---

[16] Network Centric Warfare can also be subdivided into two dimensions, the *Network Dimension* and the *Human Dimension*[16]. The network dimension is the computer and information systems side, which focuses on the technological area, and developments. Issues such as network protocols and routing information come under this dimension.

The other aspect is the Human Dimension. This focuses on how soldiers use, handle, manipulate and implement the information provided by the network dimension, and its associated technological elements[16]. This aspect also looks at how the abilities and command decisions can be enhanced and made to benefit the soldiers and their assigned tasks. Rapid intelligence updates can provide the soldier

What NCW Can Do for the War Fighter and How

The common query by defence personnel is "What NCW can actually bring to the War Fighter on the ground?" As can be seen in **Table 1**, the most immediate benefit to a force of implementing and using NCW is that it helps relieve the most intractable of problems which every war fighter has faced since war began. This is the problem caused by what Karl Von Clausewitz famously called "friction" and the "fog of war". Clausewitzian "friction" refers to the fact that in real war, as opposed to war on paper, combat is dangerous, unpredictable and physically demanding, so much so that only the most exceptional War Fighters can keep their wits about them in the heat of battle. The "fog of war" is a part of that friction, referring specifically to how confused the battlefield can seem to the war fighter while they are immersed within it because they have only unclear to non-existent information about what is going on.[17] Both phrases capture the importance of the unknown factors or variables in any military engagement. NCW provides a means to remove much of the friction and fog of war from the battle space.[18].

---

on the ground with enhanced situational awareness, which can help provide a soldier with more tactical options and get inside the enemies OODA (Observe, Orientate, Decide, Act) loop faster.

[17] Clausewitz K von (1832/1976). On War, M. Howard and P. Paret (trans.): 113-119, 193.
[18] Alberts, D. S., Garstka, J. J. (2000). Network Centric Warfare: Developing and Leveraging Information Superiority, **Page** 287.

Table 1

What Can NCW Do?

- Common Relevant Operating Picture (CROP).
- Situational Awareness.
    - Enemy
    - Allies
    - Civilians
    - Media
- All force components become organic.
- Longer reach back into Rear Areas for support.
- Network Centric Enterprise.
- Real-time or near real-time information flow.
- The ability to rapidly change plans and courses of action (COA) in response to new information.
- Flexibility in response options.
- Increased tempo, lethality and reduced response time.

Network Centric Warfare provides the foundation for data from different sources to become fused together to produce higher levels of understanding and situational awareness about the battlefield that is not available to the enemy. This increased awareness can provide for the application of surprise or mass effect to an area. This is where a force can apply maximum firepower and decisive edge to an engagement or a campaign. But a force is also more aware of external factors such as civilians and civilian assets. These variables of warfare can be avoided, or damage to them minimised, by applying the necessary force and not excessive force to achieve mission goals.

NCW can also provide a flexible response to unexpected circumstances. For example, if an infantry unit comes upon a dug in force in an engagement and the weapon systems they have with them are inefficient to remove the threat, then the commander or squad leader can look through the network to see what free assets (Air support, Tanks, Naval fire, Artillery, etc) are available to him/her within his area, what those assets are equipped with and then redirect an appropriate response to his/her target. Under NCW this process can be achieved in near real time. The same ability can be used on defensive operations where the surveillance and sensor systems of NCW, can give a

commander a form of foresight to be able to place units in an effective defensive position or to change them as needed. This gives the commander the ability to deploy a mobile defence in anticipation of an enemies attack, or provide a commander with a better response time to multiple attacks.

The Concept of Network Centric Warfare and Its Implementation

From Table 1 and other claims tabled in this chapter, it should have become plain enough that great benefits are supposed to come from implementing Network Centric Warfare. Those benefits are being displayed and researched by every corner of the international community. And the pressure is full-on from the drive by the United States Department of Defense to get its coalition partners onboard and conforming to its standards and practices. Nonetheless, NCW is not yet an accomplished fact. There are still inherent flaws and stumbling-blocks to the introduction of NCW. These flaws and stumbling-blocks are usefully discussed in this chapter because they help clarify further the NCW concept being so actively pursued.

One revealing issue about NCW is best approached by noting that the concept of NCW came about before the events of September 11th 2001. On that infamous day the United States lost a major military engagement, for that is what it was, and it lost despite all the NCW it then possessed. This is a good reminder that NCW was not designed for engagements such as September 11; it was mainly designed for conventional warfare standards of a force on force engagement. It was not envisioned to accommodate the approaches applied in Asymmetrical Warfare (AW), where a smaller force uses unconventional tactics and methods to attack a superior force. September 11 has led the United States to try and the projects it was carrying out on the day and adapt them to the new conflict standard. Specifically, the Department of Defense had to re-evaluate its research and development projects for Network Centric Warfare and see which of those NCW projects could be transitioned or modified to work in the new Asymmetric Warfare environment.

Some of its current projects had to be scrapped due to the change in operational context. For example, weapon systems such as the Paladin self propelled artillery system were deemed to be unable to reach operationally viable standards for Asymmetrical Warfare; although the Paladin system could be integrated and made an organic asset to a variety of forces – touchstones for being network centric – nonetheless it was designed for the traditional force on force conflict it couldn't be integrated and organic with forces engaged in an asymmetric conflict.. The US Army also lost its Comanche light helicopter project, due to the same issues[19].

Other NCW projects of the day could be transitioned or modified to work in the new AW environment. For example, the United States Navy enhanced its resources and research into the development of the Arsenal ship, floating weapons platforms with limited stealth capability and smaller crew numbers, which can loiter offshore to a conflict and provide fire support or launch network enabled missiles on demand

Unfortunately, most of the systems which were able to be modified to work against Asymmetric Warfare nonetheless had to be introduced earlier into deployment than was originally planned. September 11 demonstrated that AW was not something yet to come for which NCW would need to be designed; AW was already upon them. NCW required something yesterday. So that's what it got. Deploying these new AW-ready systems ahead of schedule, however, brought with it a new kind of stumbling block to the implementation of NCW. Network Centric Warfare in an Asymmetric Warfare environment might be achievable, but now it had become almost impossible to develop a unified NCW approach. The United States had to start a spiralling process to introduce new systems into service as they developed, and then to make them work with other systems they had not originally been designed for, and then to introduce more new systems as they were completed, and then to mesh those systems with the ones already in place … and so on. The result

---

[19] Barnett, T.P.M. (1999). 'The Seven Deadly Sins of Network-Centric Warfare", Proceedings of the U.S. Naval Institute: 36-39.

was an ever-increasing mismatch of systems and data formats. The fundamental principle of deeply integrating every element in NCW was in disarray

This rapid prototyping and deployment has led to serious problems on the battlefield as well. [20] When confronted by mismatched systems and mismatched data formats, the war fighter has to fill them in makeshift solutions concocted on the fly. What price NCW then? Too much of the promise of NCW derives from the (supposed) future potential of the systems, not from what is currently possible. Many of the future NCW systems are trying to take the "soldier out of the system" and replace it with a "system of systems". Most of the NCW systems actually being employed on the battlefield, however are being held together ad hoc by the War Fighters using them, while they wait for the rest of the systems to be developed and deployed. This is not merely disheartening, leading the soldiers to mistrust technology. Worse, it is just not NCW anymore. Chewing gum and No.8 fencing wire and whatever else is on hand is just not the stuff of deep integration of assets. If the behaviour of the sniper/scout unit a few pages back is the model of NCW (the "Sensor – Decider – Shooter" model), the War Fighter struggling with mismatched systems and data is certainly not that.

A second revealing issue for Network Centric Warfare is also best approached obliquely. The Department of Defense is essentially a customer, not a manufacturer. As with all customers, *caveat emptor*, buyer beware. Beware, in particular, of false advertising and inflated claims and things that should work but never do. External companies contracted to the Department of Defense are the developers of many of the NCW systems. These contractors understandably try to keep their lucrative defence contracts, which are worth millions of dollars per year. They do this best when they deliver the goods. But sometimes the goods can't be delivered. That's the time for some overly optimistic delivery dates or some overestimated expectations of the system as they intend it to be when they do deliver it. (Of course the same

---

[20] Luddy, J. (2005). The Challenge and Promise of Network-Centric Warfare,: **Page** 15

kind of inflation goes on when bidding for contracts too.) This gives the Department of Defense a misrepresented view of what the system is actually capable of. This in turn allows the development of unrealistic expectations of the equipment by those who are to use it, the soldiers.

A good example of overestimation affecting the whole process of implementation is the development of an Artificial Intelligence (AI) system to filter the large amounts of data being provided by the current NCW systems. The levels of both raw and processed data that can be created by such systems are already starting to go beyond the cognitive abilities of human beings to comprehend. Even the amounts of data being given to the War Fighter to filter for useful information, is growing exponentially. The solution to human cognitive overload has always been to dump some of that load off to a non-human cogniser; that is, to use an AI construct to help with the processing of data. AI researchers have been working on the problem for decades now. And every year they have promised that next year it will be ready to deliver. But tomorrow never comes. Even the most current AI research is producing AI constructs with ineffective cognitive abilities. Many research scientists aren't predicting a breakthrough for at least the next five years. And that may be an overly optimistic prediction itself. This means that soldiers will have to deal with the increasing data levels by themselves for the foreseeable future, just as they have always had to do up to now.

The Concept of Network Centric Warfare and Real Warfare

The concept of Network Centric Warfare is one thing. Combat as it is actually conducted in the lives of war fighters is another thing. No surprises there. But the connection between the two often displays a revealing pattern: NCW can do so and so; but at the same time it can't do such and such; yet it was expected to do both. That is, there always seem to be trade-offs with NCW. The individual trade-offs are of a bewildering variety. But the pattern of trade-offs can gradually build up a better picture of what NCW is and isn't. The remainder of this chapter attempts to build up this picture, trade-off by trade-off.

ITEM: Consider the matter of "Information vs. Intelligence", the ability to turn information into effective intelligence for use by commanders and their staff. NCW has the ability to gather incredible amounts of data quickly. Yet the adage of "more is better" no longer seems to apply to the realm of NCW somehow. The information gathered is raw, without a context. Simply because of its volume, such raw data can hide important intelligence from the soldiers interpreting it. September 11 is a notorious example. Both the Central Intelligence Agency (CIA) and the Federal bureau of Investigation (FBI) had large quantities of information about terrorist movements in the United States, but due to the size of that raw data available, they completely missed the clues to the terrorist plot[21]. NCW was supposed to be designed to make intelligence quickly available; but somehow the more and faster the data is processed, the less it becomes the intelligence NCW was designed for; indeed, the very intelligence which is needed for engagement becomes even more obscured in the information fog. One aspect of the NCW promise seems at loggerheads with another aspect of that promise.

ITEM: NCW systems at the current moment do not actually help to put munitions onto a target. Practical combat power is not easily derived from the NCW capability. True enough, the potential is there. Nonetheless, it is still a soldier or an airman who has to be in harm's way to pull the trigger on a system or weapons platform. An extreme example of this trade-off is combat in an Asymmetrical Warfare environment. The expectation has always been the war fighter would become more aware of their situation and surroundings using NCW than not using it, because the NCW provides a larger picture of the battle space and locates their own spaces within it. In an AW environment, valid targets are intermixing with civilians and civilian assets, such as churches, schools, or peaceful demonstrations. Asymmetrical Warfare is distinctive precisely because the military assets are hidden within the civilian assets. What the war fighter needs from NCW is not a larger picture but a more microscopic one. In AW combat as it is actually fought, it is not the NCW

---

[21] From the Whitehouse and Congress review of the failure of the intelligence community to stop 9/11

system that sifts the military from the civilian. The job is done by the actual War Fighter, who knows what it's like to be both military asset and civilian asset and therefore is the right asset to send to catch the enemy. To the extent that the job of sifting out the enemy is thrown back into the hands of the War Fighter, however, the benefits that NCW was designed to provide are being negated by the very thing NCW actually does provide. Once again, NCW promises two things but the more it delivers on the one the less it seems to be able to deliver on the other. In this example the War Fighters do get their enhanced awareness of the whole battle space; but the enemy is hidden somewhere inside that whole; indeed, the enemy has become better hidden now than before, and precisely because the battle space has been enhanced. It's a bit like proposing to solve a "Where's Waldo?" puzzle by making it twice as big.

ITEM: With NCW, soldiers on the ground have better access to the command group and headquarters than they could ever get if they didn't have NCW. The enhanced access is provided in part by the physical means used (digital communications and wireless data access) and in part by the fact that there are more nodes and thus more routes available (satellites, microwave towers, other War Fighters) This access means that soldiers on the ground can ask for direction and guidance from higher commands more easily. As with most features of NCW, however, this is a double-edged sword for troops. Enhanced access means that higher command can give the soldiers more awareness of battlefield conditions and developments. But with NCW the enhancement of access and awareness can become so great that it leads to soldiers becoming reliant on guidance and direction being given to them instead of using their own intuition or initiative[22]. A good example of this would be the case where soldiers have become so trusting of and reliant on their data feeds that they use them to make their combat decisions instead of actually getting out and looking at the situation around them. Such soldiers could end

---

[22] Luddy, J. (2005). The Challenge and Promise of Network-Centric Warfare,. **Page** 11

up fighting icons on a screen, instead of the enemy in front of them[23]. Asymmetrical Warfare provides another good example. In an AW environment the intelligence assets of a NCW system could lead to a misrepresentation of the target or the threat level of a target being spread through the system. Given the methods and tactics of an NCW system, particularly one running the "Sensor – Decider – Shooter" model, such misrepresentations might well have fatal consequences when the system hits the "real-world" battlefield as it were. Misrepresentations of threats could lead to non-valid target being attacked, or troops being led into an ambush, precisely to the extent that the war fighters have placed their reliance on the NCW system and the data that it provides. Both of these examples exhibit the trade-off pattern so typical of NCW. A bit of some feature NCW has been designed to provide is fine (access in this case). NCW has not been to designed to provide just a bit of that feature, however, but as much of it as the network-centric system can handle. Nonetheless, more that just the right bit of that feature and NCW is no longer a boon to the war fighters but their worst liability. What is so typical of NCW is that it becomes such a liability because of the very feature it was designed to provide.

ITEM: At a technical level there are further features of NCW, which could lead to it being more of a liability than an asset. For example, it is supposed to be a strength of NCW that it builds a context framework on top of a physical network. To the extent that the physical framework remains robust, such a system may be effective enough. But that strength turns into a weakness – indeed a positive hindrance – directly the physical framework goes down. Precisely because the context framework is build on top of the physical framework, when the physical framework goes it takes everything else with it; the context framework of the NCW no longer exists because it doesn't have anything to exist on; so the whole thing, the entire NCW, is just gone. The war fighter might as well go back to throwing rocks. This is not a hypothetical danger. When there is a loss of connectivity between assets or nodes on the

---

[23] Barnett, T.P.M. (1999). 'The Seven Deadly Sins of Network-Centric Warfare", Proceedings of the U.S. Naval Institute: 36-39.

network, either through a lost data packet[24], or a message that is delayed, dropped or lost by the network, then NCW too often leads to the loss of life or critical information[25]. The very fact that NCW works so well when it works can persuade a military force to make it more and more central to the business of war. The more and more central NCW becomes to it, however, the less and less can the business of war be carried out when it doesn't work. In terms frequently used in Artificial Intelligence, NCW systems don't tend to "degrade gracefully"; "catastrophic failure" is the norm rule. A similar example derives from the fact that an NCW system typically relies on a single source for users. Such a source can be in the form of a central database for targets, or a database for troop locations. Single source items are another boon which NCW has been designed to provide. The design of a network-centric system allows access to any node (asset) from any other node. So it makes no demands to make provision for multiple locations where the same information is stored. There are positive reasons for storing information in only one place: single source items provide the network with easy security as only one file needs to be backed up and secured. As might be expected, however, single source information is another feature which is meant to be one of the great strengths of NCW but potentially can become one of its worst liabilities. It is entirely possible for the only database of troop movements, to become corrupt or deleted, Likewise, the central database of targets could well be hosted on a server which crashes through loss of hardware, such as the hard-drive in a server system. Replacement of the damaged components and recalling the last backup could see an intelligence database offline for up to 6 hours or longer if the components or expertise are not available. During those 6 hours the entire military establishment might as well not exist. No information about targets is available anywhere in the NSW system. No node has access to the target database because the node that file was on is just gone. It's the same pattern all over again. Exactly the feature which NCW was designed to provide has become such a hindrance that it would be better not to have NCW at all than to have NCW with that feature.

---

[24] A data packet is the form that data or information takes on a network. These packets can be lost or crash into each other on a network causing corruption in a file or complete loss.
[25] Luddy, J.(2005). The Challenge and Promise of Network-Centric Warfare, : Page 6

ITEM: One final trade-off reveals itself when the scope of NCW is widened. The cases so far have been confined to individual forces by themselves. But most forces today are deployed as part of a coalition or alliance, – thus the United Nations peace-keeping forces deployed in practically every hot-spot on the globe or the coalition forces which carried out Operation Desert Storm in 1990 (30 nations) and Operation Iraqi Freedom in 2003 (40 nations). It has always been part of the promise of implementing NCW that it could make such coalition forces tight and efficient. Very roughly, all that is required to build up a coalition force is to make the forces of each new coalition partner a new node in the coalition NCW up and running. By being made a node the whole network becomes just as much open to the new force as it already is to the other forces, who too are really just more nodes of the system. In real-life warfare, however, the provision of network integration and resource allocation turns out to be another of those cases displaying the pattern typical of developments in NCW: the very strength the system is designed to deliver becomes the worst obstacle to the business for which such systems were desired in the first place, making war. For many nations NCW networks already provide the foundation of C4I (Command, Control, Communications, Computers, Intelligence). When those nations join up to form a coalition force, their individual networks need to be able to share information between each other if they are to obtain the full benefits of the network integration which NCW brings. (Information is shared by becoming a node of the coalition network.) At the same time each nation remains an autonomous entity and of course is concerned to keep its own secrets secret. However, the network integration delivered by NCW is so thorough that the security and stability of each coalition partner's own network is in danger of being compromised directly it becomes a node of the coalition network. (Becoming a node it gains access to every other node, but equally every other node gains access to it.) Security and integration make uncomfortable bedfellows. Precisely because the degree of integration is so strong in a coalition network, each of the coalition partners must increase the level of security protecting their own network. But the higher they set their network's level of security, the lower becomes the degree of integration of the coalition network. This spiral has led

in some cases to critical networks not being accessible by commanders in a coalition environment, thereby defeating the whole purpose of having NCW at all. As an example, during Operation Iraqi Freedom, the Australian Defence Force was denied access to the air mission planning system, because of the multiple levels of security that the United States had put onto its data networks. This made it impossible for them to access the assets which were needed for Australian troops on the ground. As well, they lost the ability to integrate their air assets into the available pool of combat resources. This hindered the coalition and strained the command relationship.

* * * * *

Both the development of Network Centric Warfare and its behaviour in real-life combat, display an intriguing mixture of failures and successes. This shouldn't be too alarming. The concept of NCW is a new concept. And it is being implemented for the very first time. Much the same thing happens with any new concept through the period it is being realised. The anomalies which are so striking in NCW are just the result of the new systems being introduced, then, and for most of them solutions are already in development.

Nothing said in this chapter should stop the New Zealand Defence Force from investing in NCW systems and growing the three services into world class forces. Nonetheless, a healthy awareness of the pros and cons of introducing these concepts into the NZDF is a priority. The next chapter will look at some of the issues that the NZDF could face in the next couple of years as it introduces baseline[26] NCW capabilities.

---

[26] "Baseline" capabilities cover the areas of communications, logistics, tactics and command development, along with the introduction of ICT technology such as integrated service networks and intra-service network messaging.

Chapter Four

Effects of NCW on Personnel and Organisation

New Zealand has been called upon to work with other countries in coalitions and alliances more frequently in the first seven years of the twentieth century than at any other time in its history. New Zealand soldiers are well respected in the international community for the skill and ethics they bring to coalition engagements all around the world. Foreign force commanders have stated that the New Zealand service personnel have an unusual ability to solve any situation with "Kiwi Ingenuity" and their "can do" attitudes. An example is the A-4 Sky-hawk's avionics equipment called the Kahu (Maori for Eagle), which was developed and maintained by the Air Force to compete with the most sophisticated commercial systems available to allies nations.

For all that, New Zealand is right now in serious danger of being left behind, and therefore left out. The technological developments being introduced in the pursuit of Network Centric Warfare are well beyond the reach of the skills and ingenuity for which New Zealand forces are so praised. The decision to opt in or to opt out of the NCW project as a whole is urgent and unavoidable.

Bearing this in mind, New Zealand has started to shift its focus to a modular organisation so that the three services (Army, Navy and Air Force) can be integrated into a joint force more easily. But currently the digital interaction is not present in those modules to any usable degree[27]. The New Zealand Defence Force (NZDF) is looking at investing in a Joint Command and Control System (JCCS) to help with this issue[28]. This system will interact with each

---

[27] Currently the Army and Air Force have a joint material management system running to co-ordinated logistical supplies on a SAP Database system, with the navy to soon join.
[28] New Zealand Defence Force (2006.). New Zealand Defence Force: Statement of Intent.. **Page** 21.

service's Command and Control (C2) system and make each military platform a node on the network – the basic design mechanism of all NCW.

Digital Technology

Given that some degree of NCW has been deemed to be the new goal for the NZDF, some external observers such as the Australian Defence Force, have argued that the New Zealand Army needs to start investing immediately in new training techniques and methods to increase the uptake in digital technology. Otherwise it won't be in any position to leverage the advantages provided by a digital force such as the NZDF envisages or to utilise the benefits of digital technology.

Those benefits are substantial. For a start, digital technology is a force enabler Force enablement can be defined as:

"The ability, method, technique or technology to allow a force to achieve an operational level previously inaccessible or unattainable."

As well, digital technology is a force multiplier. Force multiplication can be defined as:

"The ability of a force to apply enhanced firepower through the application of new methods, techniques or technology which is disproportionate to a force of equal size without the enhancement"[29].

At no point in history has the battlefield been more visibly observable than it is now because of digital technology, such as infra red, thermal, satellite, radar, lidar (Laser based radar). Commanders now have the ability to see the total observable picture through digital feeds coming into their headquarters from soldiers on the frontline and from the support groups in the Rear Areas. These data feeds can be integrated into new Command and Control (C2)

---

[29] Definitions distilled from the information provided by Wikipedia. http://en.wikipedia.org

systems, which have input from intelligence assets and other military assets to give the Commander a high level of operational awareness. With this the Commanders can increase the tempo at which they can command. This is known as Information Superiority. Information superiority is defined as[30]:

> *"The ability to collect, process, and disseminate an uninterrupted flow of information while exploiting and/or denying an adversary's ability to do the same".*

Information Superiority can speed up the commander's OODA (Observe, Orientate, Decide, Act) cycle. This can be adapted to temporarily halt the enemy, stop the enemy or turn an engagement into a favourable outcome for a force commander. This gives the commander the tools to be able to send smaller forces into a combat environment, which are tailored to suit the battle's needs. Assets, which aren't organic to a fighting force, such as Artillery or Combat Engineers, can be added to the task group without major issues. Such integrated digital technology, which is being fielded, is known as self-synchronisation systems. The NZDF has already begun to put self-synchronisation systems into the field.

This information superiority is not as superior as its name suggests, however. This was shown through the events of Operation Iraqi Freedom and Operation Enduring Freedom. Self-synchronisation systems were designed for a conventional war, where units and assets are used in force on force engagements. They were not designed for the current Asymmetrical Warfare environment, where the battlefields are in built-up areas and the opposition force hides amongst the citizens and employs guerrilla tactics. Using NCW in such a combat environment as that, the commander does indeed have an enhanced view of the battlefield, that advantage is minimised due to a lack of valid conventional targets. The commander has an understanding of the

---

[30] United States Department of Defence (1996) Joint Doctrine for Command and Control Warfare, Joint Publication 3-13, **Page** 14

physical battle-space, but not of the enemy force. There is no genuine information superiority in that. There is only the pretext of one propped up by the presence of admittedly superior equipment. "Superiority" here is a consequence of the IT culture being insinuated into the Armed Forces, where the existence of technology is the solution to all problems.

Digital Technology and the Kiwi Ethos

The possibility of digital technology changing the culture and ethos of the New Zealand Army is dependent on the approach which the NZ Army decides to take to the introduction of the new skill sets and technology. With more of New Zealand's operational deployment being in conjunction with other nations either in United Nations led peacekeeping, peacemaking or peace enforcement[31], the need to be interoperable with them is becoming more critical. In particular both operational and logistical support are being digitized and fed through command and control systems, in such missions. These systems must be usable by New Zealand troops both in operations around the world and back in New Zealand itself for logistical support.

The current "Kiwi" mentality of things being able to be put together and made to work with the "old Number 8 wire" technique may no longer apply in the realm of "high end[32]" digital technology. Quick fix solutions may not work well and could have a detrimental effect on the whole system, even to the extent of crashing it or making is unrecoverable.

With this in mind, new and current soldiers will need to change the way they think in relation to the Kiwi attitude. New skills are needed be added to the core skills and ideologies that the New Zealand army instils into its soldiers. **Appendix A** shows a selection of current and new skills that have been researched by the United States Army Research Institute (USARI) and have been adapted for New Zealand, that work together to enhance soldiers, and

---

[31] Part of the United Nations chapters 6 and 7 of the UN charter.
[32] Such as, Integrated circuits, nano-wire, or quantum computing.

make them more effective in the implementation of NCW and Network Enabled Operations (NEO).

For the New Zealand army, a cultural change would be needed to fully implement and accept the new technology. Australian and British research has shown that this can be achieved by wide spread decision, debate, experimentation and broad acceptance across all of the branches. Correct information about what a Networked Enabled Army (NEA) would look and act like needs to be explained at the beginning of the NCW process. Clear direction at the outset has been proven to save time and frustration later on in NCW developments. With out this consultation process the United States Army found that its troops were not using the systems to their full capacity, causing delays and operational pauses as the information that was requires at the out set was provided.

Adding Information technology to the military is not just an add-on effect, it's not just an army that is networked, it is a shift to a networked army, meaning that it is so integrated into the whole, that the network cannot be separated out or subtracted. Once it has been introduced, it becomes part of the military foundation, with such a deep effect that if it was attempted to have it removed its effect would still resonate in the military. The military's ethos and culture would still have an awareness of it.

The Army will face the same issues if it proceeds with the introduction of the network capability. It will not become the New Zealand Army (with Network Enabled Features and Capability) (NZA (NEFC)) it will still be the New Zealand Army, with network capabilities integrated ***into*** it, not ***onto*** it.

Culture and Ethos have been proven to be critical to a force; this is where it draws its unifying strength. History and tradition can shape a force and hold it together beyond its logical physical means. For example, soldiers fight for the person beside them and for their unit identity. Inter unit rivalry provides a great cohesive environment for a unit; with inter unit challenges and competitions lifting the standard for all units involved. But many believe that when network

technology comes it will diminish many positive aspects that individual units have developed through unit identity[33], Network forces bring in the possibility of more modularity to a force make up, selecting elements of a unit to deploy instead of whole units. With the joint force environment the possibility of being aligned with some one from a whole different service can provide a real headache to command structures. Even with clear command lines designated through doctrine and training, it is human nature to align oneself with aspects that are a reflection of ones beliefs and ideals. This has led to people seeking out members from their own service and unit, above or outside an established command and control system, for advice and solutions to issues. With a joint networked force there will be a need to establish a higher order of ethos and culture for soldiers and units to identify with and to help form cohesion between separate services and unit elements.

With commands coming through digital networks from commanders who might not be of the same service as the unit receiving them, there is the possibility of command breakdown or confusion becoming an issue that could have substantial consequences[34].

Soldiers have been shown to experience dislocation with the digital joint force modular command structure. The soldiers have started to inadvertently overlook command elements that have directed control over them for elements that are from their service. As an example, the Australian Defence Force (ADF) has experience command dislocation during its time in Operation Iraqi Freedom (OIF). The Network has provided them with better access to resources from bases in Australia, and the ability to influence mission events back in Australia, such as training. Even with a dedicated coalition command structure in place, external elements started to take an effect on the operations[35].

---

[33] Warne, L., I. Ali, et al. (2004). The Network Centric Warrior: The Human Dimension of Network Centric Warfare. **Page** 108.
[34] Ibid.
[35] Smith, H. (2004). "The military profession in Australia: Crossroads and cross-purposes?" Future Armies, Future Challenges: Land warfare in the Information age. **Pages** 184.

Soldiers could have the ability to bypass command elements and go directly to the resource required through the network and NCW; this is especially relevant to the logistics branch, which crosses command paths to get to stores and resources. This might be the most efficient way of getting resources and stores to the people in need, but it can have a detrimental effect on coalition operations. The ADF has seen times when soldiers have gone about tasks with the methods taught by the ADF, that have conflicted with their coalition allies; forcing the system to slow down or be halted while transition processes have been implemented[36].

As a consequence of this, the United States armed forces have the ability to put officers into positions and responsibilities that other allied forces cannot match. The ADF has seen in OIF situations where a NCO has the same tasks and responsibilities on a digital network as a US forces officer. This can lead to a command conflict where two soldiers with identical responsibilities cannot achieve their tasks due to the rank structure. For example, where a NCO has more responsibilities, resources and officers answering to them. This problem can be compounded on coalition networks where a. NCO could be answering inquiries from foreign forces Officers or resource requests from multiple coalition officers and has to decide who gets what and when, this runs counter to the traditional Officer-NCO relationship.

Therefore, the culture and ethos that needs to be established or maintained, is one that holds the NZDF core values at its heart but also has the flexibility to adapt to both joint and coalition needs. Intra-service and coalition interoperability will need to be experienced and trained for, before it is needed in an operation, this has the potential to be achieved without the need for a large exercise, by using digital technology and simulation systems, (which will be covered in chapters 6-8).

---

[36] Talbot, D. (2004). "How Technology Failed in Iraq, " Technology Review: Emerging Technologies and Their Impact, retrieved from http:/TechnologyReview.com/Infotech/13893/page1.on 18/03/2005

Most of the available literature shows that a networked force will be an integrated force, and the soldiers behind it making it work will need to know that their ethos and values are still important. Analysis of the results from USARI testing and experiments have shown that single integrated cultural identity within a NCW context and environment, provides a unifying factor for the troops and service personnel involved no matter the individual service that they cam from. But the cultural side is only one factor in the successful development of a NCW concept, the other side is the research and development of the technical tools in use.

Network Centric Warfare and the New Zealand Budget

The United States has an annual defence budget of over 1.1 trillion dollars. About 1 to 2 percent of that goes into NCW, this equates to about 10 to 20 billion dollars annually going towards the research and implementation of NCW[37]. With this large amount of funding available, the ability to try out new methods and do rapid prototyping of needed services and products is possible.

The same is not possible in New Zealand. In New Zealand the total annual defence budget is only about 1.7 billion dollars. Even with the new funds being provided by the Defence Sustainability Initiative (DSI) and from the Defence Capability and Resource Review (DCARR), the funding of NCW is nowhere near the levels of the United States, therefore there is the need to be very careful about which directions are taken in regard to the NEA and NCW. A single unified approach from the New Zealand Defence Force is needed to maximise the limited resources, both in financial and personnel resources that can be put into researching NCW.

With the strategic environment that New Zealand is in, increased expenditure on defence is not justified, but the NZDF must still be able to interact with its

---

[37] Thomas, J. A. (2005). Evaluating the Claims of Network Centric Warfare. **Page** 103.

allies and coalition partners on operational deployment[38]. To this end the NEA program is one which must be done right the first time. The implications for not setting the correct foundation could end up harming New Zealand's reputation overseas with allied partners, by making working with New Zealand forces more of an issue than and advantage. This is what revises the problem, the issue of using other nation's results to plan and direct the NZDF and the NZ Army's NCW approach.

There is a significant danger that the NZ Army will take on board the cultural ethos and cultural identity, through the use of another countries tailored NCW solution. The technology and soldiers must be able to work, interact, and be a valued asset to any international operations, by maintaining correct training, standard and procedures prescribed by larger coalition partners. But as it has been stated before the NZDF must keep its identity and heritage intact. This is important as New Zealand has an international reputation of being a highly respected force and a good global citizen[39].

Three discussion points present themselves from this issue:

1. New Zealand should take a focused holistic approach to the implementation of its network enabled army or joint force, taking the lessons learnt from the United States attempts in NCW research and development. But it needs to have the ability to select options from other nations who are also trying to find their direction, countries such as the United Kingdom, Canada or Australia. In this way New Zealand can develop its own digital identity but also remain interoperable with our allies and close friends. A mix and matched approach without guidelines or an end state, can lead to operational issues with technology. Which would not work or communicate with other systems, thereby causing delays in the command cycle.

---

[38] New Zealand Defence Force (2006.). New Zealand Defence Force: Statement of Intent.. **Page** 19.
[39] New Zealand Defence Force (2006.). New Zealand Defence Force: Statement of Intent. **Page** 17.

2. New Zealand will never get to the funding levels that the United States or the United Kingdom is investing into NCW or Network Enabled Operations (NEO) as the UK calls its initiative because of the large difference in national Gross Domestic Product (GDP). However the NZDF can be a productive junior partner in the development of coalition technology.

This aspect has been displayed by New Zealand's participation in the Coalition Warrior Interoperability Demonstration (CWID)[40]. CWID has already been assessed positively:

"NZDF participation in annual CWID activities is the best available means to assess allied developments in the interoperability of Command and Control (C2) systems technology. It provides a measure against which the NZDF can assess its C2 developments and interoperability, and a unique opportunity to expose interoperability shortcomings before they arise in coalition operations. Participation also provides experience for NZDF operational commanders and staff with current and emerging C2 systems and technology."[41]

3. This program is helping to define what technology will be needed to remain interoperable with coalition allies in the future. It includes technology needed in the information arena. The CWID is interacting with the development and deployment of New Zealand's own Joint Command and Control System (JCCS). This system will become the backbone of the NEA plan and its service-wide use. It is the focus point for the Joint Forces approach, which the NZDF is aiming for[42].

---

[40] New Zealand's CWID site: http://www.nzdf.mil.nz/operations/cwid/default.htm, Retrieved 15/04/06
[41] Ibid
[42] MacMillan, K. (2005). Evolving Command & Control: The Challenge for Smaller Defence Forces. **Page** 13.

New Zealand's JCCS will never be up to the technological level of the United States Force XXI Battle Command Brigade and Below (FBCB2) battle management system. In particular, it will most likely lack an equal capability to the United States integrated Blue Force Tracker (BFT) system, which can monitor and display both friendly and enemy units in near real time, with the assistance of multiple satellite systems and high bandwidth tactical networks technology, which New Zealand does not have access to.

Nonetheless, all ABCA members recommend that any joint command and control system is a good step in the right direction in the implementation of the NCW concept; its use could have a major beneficial outcome to all three services, as it will be designed for the New Zealand tri-service environment. This will lead to the retention of the services individual identity and cultural ethos within a joint context and identity, but it will need to be supported by the services themselves if the full benefits will be realised from the introduced systems.

Recruitment and Retention in a NCW Defence Force

With the factors of culture, identity and technology being focused on, in the initial frame work of a NCW for the NZDF; the factor of recruiting and retaining the correct personnel becomes an increasing issue. Both the United States Army and the British armed forces, believe that the right people in the right locations will help to improve the uptake of new NCW skills and technology. The New Zealand Army should be aware of the need to recruit and retain highly skilled personnel.

Currently unemployment in New Zealand is at an all time low at approximately 3.9%[43]. The market for people is tight and the New Zealand Army must fight for the same human resources that the other services and the public/private sectors are vying for

.

---

[43] New Zealand Department of Labour statistics, quarter one, 2006

In the latest statement of intent published by the NZDF[44] it states that:

> *"Given the higher range of technologies, the sophistication of modern platforms, the time required to become proficient in their use, and doing more with fewer personnel, demands high calibre service personnel who are prepared to make the services a fulltime career."*

This shows that the government is aware that the armed forces are getting more technologically based and that personnel used to fill the gaps and needs are diminishing.

Currently it is an employee's market and the military needs to be aware of this and adapt its recruiting and retention policies to reflect this. This trend is present in all of the ABCA nations. With this in mind the NZ Army in particular will need to focus on getting the right people at the start. Training them to the required standards is vital, and the army must do all it can to focus on keeping their trained personnel, otherwise they run the risk of loosing them to the private sector or other organizations. This fact has been shown in the United States where most of their highly skill technologically aware troops have been poached by the commercial sector. Digital technologies appeal is not just for Rear Area soldiers but across the battlefield, so the requirements and understanding of digital technology are needed across the ranks too.

The old idea of the Army being a place of hard men who don't need technology, just his mates and a job to do, will no longer apply to the current and future NZ Army. The need globally, is now for a type of soldier who can continue to learn and adapt to new technology. A person who is capable and comfortable with technology and can learn new digital tasks when required.

This image impacts on at least three different recruiting pools for the NZDF and the NZ Army.

---

[44] New Zealand Defence Force (2006.). New Zealand Defence Force: Statement of Intent. **Page** 20.

1. ***The traditional recruiting pools:*** Are the lower socio economic areas, which have strong ties to the NZ Army. People, who have not had much exposure to computers, networks or the internet, could find the Networked Enabled Army to be a place they don't understand or worse still even fear due to its high technology use. Such an example would be the use of digital displays to show religious and racial divides in a city, or the use of Inter-Vehicle Information Systems (IVIS) which are prevalent in most modern combat vehicles. This issue has been offset by both the US Army and the US Marines, by using real examples of troops from all branches and socioeconomic levels, which have picked up concepts and technology which have then been displayed in recruiting campaigns.

2. ***The "techno-savvy" pool:*** The current virtual recruiter advertisements that are playing on television, such as the virtual Viv (The main character) advertisements for the NZ Army, are a good example of a state-of-the-art solution. The dual nature shows the traditional needs that the army wants but also shows that it isn't afraid of using new technology for advertising. The online "Force 9" interactive games bring people who have a familiarity and experience of the Internet to the Army's websites to play the games. The Royal New Zealand Navy has used a similar type of marketing campaign in its drive for technologically aware personnel; in its recruitment advertisement the deliberate use of the words "Video Games" would have captured the attention of the gaming community. This community is very technologically orientated and has the required skills to jump-start many major technology programs.

   Another avenue that has been taken by Australia, the US and the UK to jump start the NEA or NCW projects is access to tertiary IT training providers, such as polytechs, not just the standard universities. With some of the providers giving high-level multi year training with industry experts, the skill sets gained by the students of these diplomas and degree courses can be a valuable resource. These students have been shown in USARI research to reduce the time needed to train a raw

recruit in IT.

3. ***The career orientated pool:*** With such a limited number of potential recruits available for military service, the need to look in other directions is becoming more important. All four services of the United States know that the basic reactive recruitment isn't enough to get access to the right people. Going to career days with posters and brochures does not get the interest of most generation Xers, generation Y and generation Next[45]. Psychologists have stated that their environment and attention is not static, books and posters will not get them engaged. The New Zealand armed forces needs to be more interactive, especially the NZ Army. There needs to be more effort in showing that the services can provide an enriched career option instead of a short term job prospect. The United States Army has achieved a level of this in its recruitment campaign called "Americas Army" which was an interactive demonstration of career choices. This method led to a larger recruitment intake for the US Army.

The NZ Army has more potential to implement new ways of recruiting from their traditional recruiting pools than do the Air Force and Navy, because of its land force focus. For example, one new way proposed in response to this research would be a LAV demonstration on a school field with more than one unit and the troops brings both the equipment and experience right into the potential recruit's environment. With two units, the technology and weapon systems that the NZ Army uses can be on display as well as the people who use it as well. These demonstrations could provide a means of increasing the recruiting footprint available, and to offset the gap that has developed between the NZ Army and local communities.

The capacity of the NZ Army to show what it has to offer a potential recruit interested in Information Technology (IT) should not be underestimated. They

---

[45] Generation X is defined as people born from mid 1970's to the start of the 1980;s; Generation Y is from the early 1980's to the beginning of the 1990's; and generation Next is defined as the children born from the 1990's onwards

might be interested in any of a variety of things – what prospects there are for training in IT, what role IT plays in operations, what weapons platforms use IT, and so on. Regardless, there is no dearth of accurate information that can be supplied and all manner of ways to get it across. Unrealistic expectations of what the New Zealand Army can do, and comparisons between itself and the United States Army do need to be remedied, so that a realistic portrayal of what the New Zealand Army can achieve and do is possible. A focused and targeted approach is needed.

Due to the rapid developments in IT and global communications the information revolution has given the generations X, Y, and Next, an overdose of technology. In the last twenty years the entertainment market has gone from games arcades with simple 2 dimensional graphics and controls, with the processing power of a modern calculator, through to high fidelity, 3 dimensional, 5.1 Dolby surround sound, and home entertainment systems using enough processing power to create seamless Virtual Reality (VR) environments[46]. These are the types of things that recruiters must embrace and take on board when developing their marketing plans.

The line has started to blur between commercial games and military training simulations[47]. Video games come in different forms such as the First Person Shooter (FPS), Real Time Strategy (RTS) and Massively Multiplayer Online Role Playing Games (MMORPG). These games work on systems and concepts that are being developed and funded by defense researchers in the United States.

An example such as "*Battlefield 2*", which is available on PC, X-Box and X-Box 360, shows the career paths that are possible in the US Army as playable characters. The game player goes though a basic boot camp as a tutorial for the game, and then they can then select what infantry type to take, from

---

[46] Macedonia, M. (2005). Entertainment Technology and Virtual Environments for Military Training and Education. **Page** 2

[47] Lenoir, T. (2000). "All But War is Simulation: The Military Entertainment Complex.". http://www.stanford.edu/dept/HPS/TimLenoir/MilitaryEntertainmentComplex.htm 16/12/2005

common infantry rifleman to the Special Forces commander to be deployed onto the multiplayer battlefield scenario. The game records what skill you have trained for and what your accuracy rates with different types of weapons were. The player is rewarded with medals and ribbons that are representative of skill levels with the weapon systems.

Research and literature from USARI has proven that people who play these games start to get a basic form of indoctrination into the army ethos and culture. From there it is a simple step to them wanting to do the real thing. More about video games as trainers will be covered in Chapters 7&8.

The global gaming environment also exposes people to the networking side of things. People want to be able to set up their computers to be able to play online and Local Area Network (LAN) games. This gives them the needed knowledge about computer protocols such as TCP/IP (Transmission Control Protocol / Internet Protocol) and IPX/SPX (Internet Packet Exchange/ Sequential Packet Exchange). These Protocols are the building blocks of the NEA and NCW environment.

Weapon systems such as the "Predator" Unmanned Aerial Vehicle (UAV), which is an intelligence gathering asset, uses control systems that would not be out of place on a modern computer flight simulator. The monitors provide a real time feed back so that any input to the controls responds in real time with the correct expected responses. The only difference between this system and games such as *Microsoft's Flight Simulator* are that the weapons fired on the Predator are real. The new generation of Command and Control systems, such as JCCS have displays and graphics which most gamers would find out-dated but would be able to pick up and use with not much initial training.

A percentage of the new recruits who are now starting to enter the armed services world wide are highly technologically aware and they have the skill to be able to pick up new systems. The main concern comes in the form of retention as these personality types seek out new experiences. These people

have been shown to need mental stimulation often, by giving them new problems to solve, new skills to learn, and technology to use[48].

The technologically aware recruits have gained most of their skills through the development of video games and the Internet. Both the available literature and research show that this group can be divided into two separate communities, "Gamers" and "Hackers". Gamers are the sociological types who enjoy competition in events or enhancing their skills through video games and online human versus human competition. The other group, Hackers, enjoy testing and improving their skills in challenges against established computer networks and servers.

Hacking is a digital method of a common task that the military has been doing for many decades. The military had (or has, but denies their existence) groups that were task with trying to break into secure complexes to plant replica bombs or to remove sensitive materials from secure locations. In the United States these were known as "Tiger Teams" or "Red Cells"[49]. Their popularity within the military was not very high because the consequences of the teams succeeding meant that there had be a breach in security or security protocols This could cost a commanding officer his job or even his career if the offence was serious enough. The aim of the team was there to bring awareness to security issues, just as the hackers are there to raise the same issues in the digital realm.

In a NCW environment hackers do have a place in the Offensive Information Operations (IO)[50]. IO covers many areas, which are becoming more important as technology increases, such as the traditional Psychological Operations (PSYOPS), Electronic Operations (EW) Operational Security, and Civil

---

[48] Chatham, R. (2001). "A Tale of Training Superiority, Games, and People Stuff." DARPA DSO: **Pages** 1-5.
[49] Tiger Teams, from en.wikipedia.org, keyword Tiger Teams, Retrieved on 15/08/06
[50] Brown, B. R. and Anderson, L (1999). Cognitive Requirements for Information Operations Training, **Page** 250.

Affairs[51]. But new technology has also created new areas that must be taken seriously by any modern, globally aware force, such as Computer Network Operations (CNO) also known as cyber warfare[52]. There has been speculation by some foreign observers and international journals that China has a group of hackers assigned to this type of tasks, ready for an attack if provoked or suspected of being under digital attack. These groups would come under the coverage of black operations (Black Ops), which allows the armed forces to deny that they have the ability or resources to go and achieve offensive digital operations.

Both the Gamers and Hackers can be valuable members of the defence organisation. But the military needs to understand the culture and sub ethos that comes along with the groups. This is why the United States has started to sponsor and attend both gaming and hacking conventions annually.

For example, Gamers have the ability to interact with the command and control system, in a tactical and operational context much faster than a person being introduced for the first time. The skills and learnt ability helps them to adapt to the complex and fluidic environment that is present in a NCW context. The gamers can become great members of a digital training team because of their awareness of what makes people learn and develop digital skills. Their ability to be able to modify and construct learning elements for digital trainers provides a resource of great value to the defence organization.

Another example reinforces the point: Hackers can provide the grounding and framework for effective information operations, both offensive and defensive. They have the ability to be able to enhance the security of local systems by using the knowledge they have gained through their experiences. This makes

---

[51] DOD Information Operations Roadmap, 30. October 2003, Definition of Information Operations:

'The integrated employment of the core capabilities of electronic warfare (EW), computer network operations (CNO), psychological operations (PSYOP), military deception, and operations security (OPSEC), with specified supporting and related capabilities to influence, disrupt, corrupt, or usurp adversarial human and automated decision making while protecting our own.'

[52]Maiers, M and Rahn, T, "Information Operations and the millennium challenge". **Page**. 86.

it difficult for an opposing force to attack critical system and digital infrastructure. Hackers can give the armed forces a form of autonomy in system security, instead of having to rely on external government agencies for guidance and expertise.

As explained earlier in this chapter, attracting the right people to join any army or armed forces for a NCW environment will have to see the defence force take a different approach. The New Zealand situation could be enhanced with closer ties to the commercial sector that run and manage LAN gatherings and online communities such as Microsoft New Zealand. The possibility of the NZDF sponsoring a competition or having a booth at gaming conventions showing off what they have and can do, would be of immense benefit to the recruitment and retention of digitally competent people. Both the US and UK are taking this approach with promising results.

Chapter Five
Effects of NCW on Policy and Doctrine.

"Doctrinal inadequacy is no less often the cause of defeat, or of unnecessary reverses, than is technological backwardness".

— Colin S. Gray

After many years of low funding, the current Labour Government has decided to boost the funding levels to the three services. This has led to the NZDF being able to review the structure of the New Zealand Army so that it remains relevant and ready to face the issues of the early 21st century security environment. The NZ Army is currently going through the Army Configuration Review[53], which has concluded that military tasks are becoming more complex and diverse, with asymmetrical warfare becoming more prevalent. In response the Army needs to change into a more dynamic and flexible organization. The review also states that:

> *"A number of doctrinal and structural changes are presently under consideration, as are innovative training approaches and the utility of new technology."*[54]

This review is setting the way for the Army Transformation Program, which will be under review by the government in late 2006. This program has a 5 to 10 year time frame. In this time period the army should have implemented a large percentage of its NEA options[55].

---

[53] New Zealand Defence Force (2006.). New Zealand Defence Force: Statement of Intent. **Page** 47.
[54] Ibid.
[55] Ibid.

Currently the NZDF is focusing on a more joint approach to the structure and implementation of each of the Army, Navy and Air Forces IT solutions and C4. The often-quoted "Three Services, One Force" is an indication of the implied direction the NZDF wants to take. Current NZDF doctrine as documented in the "*Foundations of New Zealand Military Doctrine: NZDDP-D 2004*" is looking towards a more integrated form. Chapter 10, called "Future NZDF Capability Concepts", focuses on four strategic concepts:

- **The concept of a Tailored Joint Force**
- **The concept of a Multi-Mission Capable Joint Force**
- **The concept of a Knowledge Edge Force**
- **The concept of a Network Force**.

The last two entries are of great concern for the implementation of both digital technologies and the NEA/NCW concept, yet they are the most interesting.

The concept of a ***Knowledge Edge Force*** is the realisation of focusing on the right people and technology, with the right knowledge, being in the right place. In short, it is the concept of using the human capital in the best ways, to achieve a great result with minimal waste or expenditure. Current NZDF doctrine states that the Army needs to incorporate this concept into its future service doctrine if it wants to keep pace with the constant change in IT and communication technologies.[56] This concept also provides the foundation doctrine for the future structure of the NZDF.

The other area is the concept of a ***Network Force.*** This is the parent doctrine and concept for the NZ Army's NEA program. This concept articulates how the services will interact with each other in both Joint and Coalition operations, the use of networks, and how they will interact with other government organisations.

---

[56] Ibid.

These concepts have laid a good foundation for the future doctrinal developments that are needed to introduce NCW to the NZDF. But these would need to be kept in check so that they can guide the development and capability of the future NZDF. It must make sure that it remains relevant and within a correct context. Without this there is the possibility off going of track or causing major disruptions to the introduction of NCW and its associated concepts.

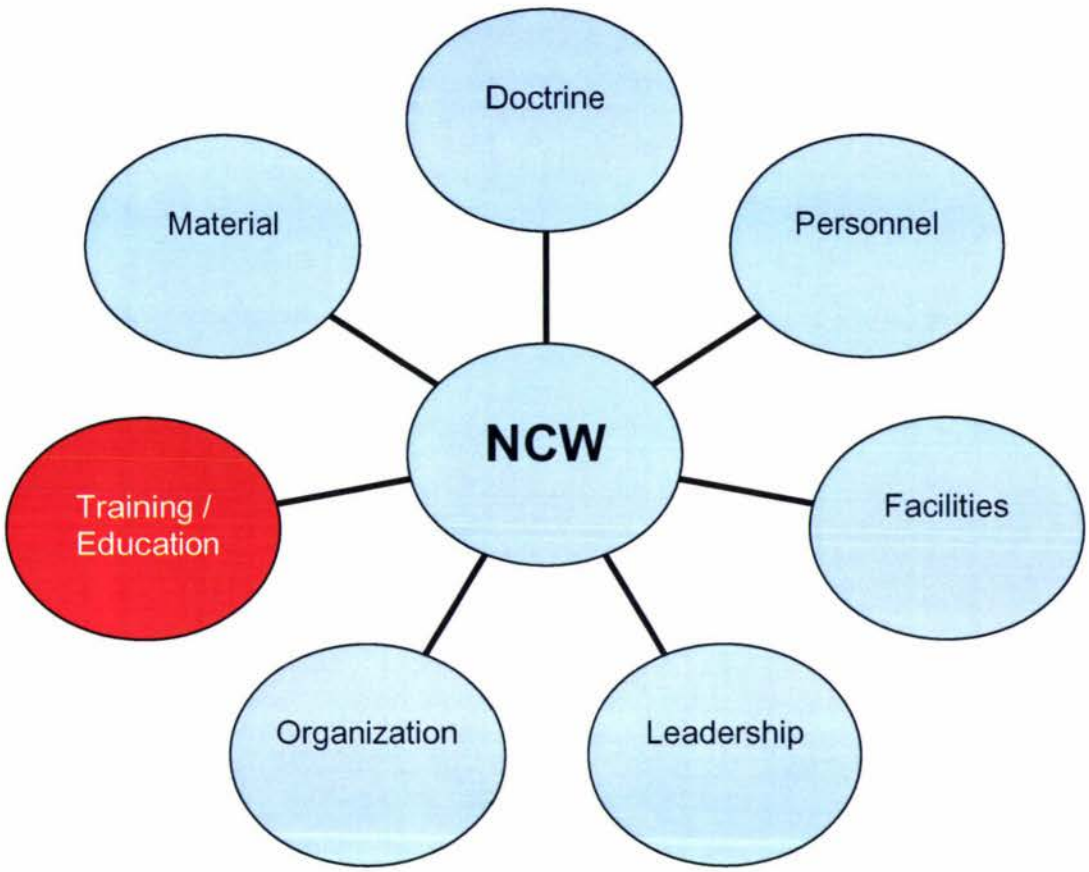
These concepts have the possibility of affecting how the services run and implement their projects both operationally and tactically including a change to battlefield tactics and minor capital expenditure. These issues have been faced by all countries trying to implement NCW at any level.

But it is currently unclear if it will affect strategic and national policies since comprehensive policies are in place for procurement and sales of military technology between countries. This includes Information Systems and services, and involves exchanges in technology provided by the CWID and intelligence community. The issue arises through the possibility of the NZDF and Ministry of Defence needing to invest in solutions that are already NCW capable to coalition standards or invest in systems that can be modified internally to reach these standards. It will come down to "Time versus Cost"

With the Army proceeding into its transitional phase it creates the right time to start the implementation of changes to the way the army is set up if it wants to follow the NCW trend. The army must look at seven key areas. These areas have been agreed upon by all of New Zealand major partners, and help to guide smaller nations in their attempts at NCW conversion. These recommendations come about from the lesson learned by the ABCA partners, and are designed to show the possible issues and solutions for the NZDF and NZ Army.

Figure 2[57]

The 7 Pillars of Successful Development



1. **Organisation and Structure:** This area is currently being reviewed in general by the ACR and ATP. However the problem of implementing digital technology efficiently highlights certain special issues to keep in mind. These issues are: What type of structure will be used in the front line branches, since frontlines and combat zones are much more integrated into a digital environment? Will the Army follow the same formula that the United States Army is using in setting up its LAVs into Stryker Brigade Combat Teams, for easy integration in a digital environment? Will the Signal Corps be in charge of the NEA/NCW plan

[57] Office of Force Transformation, Department of Defence: Transformation Trends: Implementation of NCW, Retrieved from www.oft.osd.mil 28/01/2006.

or will a new branch or section be created for the new and developing technology?

2. **Army Service Doctrine and Law:** With the NZDF focus on creating a Joint Force / Networked Force as one of its main future concepts, there will be a requirement for a review of current service doctrine and law. The reason for this is that there will be a new battle space created. In the near future Air, Land Space and sea will be joined by a new zone encompassing cyberspace and network warfare. New Rules Of Engagement (ROE) and Standard Operating Procedures (SOP) will therefore have to be designed and integrated into the current military law and regulations. An investigation of the possibility and consequences of making civilians who support the digital technology and infrastructure valid military target will have to be completed by both the NZDF, the UN and the international law community

3. **"Info-Structure[58]":** The Army will need to look at enhancing its current stocks of IT technology parts and spares. With more systems coming online the need for more bandwidth and the technology to keep it operational will have to be available, this is true for both the private and public sectors. New suppliers will most likely be needed across the country to service the equipment until the NZ army has enough trained personnel to take over the troubleshooting and repairs for a large integrated network system. Since IT is fast paced and ubiquitous in the modern digital world, there is a real question whether the army will ever again be able to be autonomous here. The implications will need to be investigated due to the consequences attached to the issue.

4. The NZ Army will need to consider looking at going to the new Internet Protocol version 6,[59] which will give the NZ Army the ability to expand

---

[58] Alberts, D. S., J. J. Garstka, et al. (2000). Network Centric Warfare: Developing and Leveraging Information Superiority. **Page** 287.
[59] Latham, R. (2003). Bombs and Bandwidth: The emerging relationship between Information technology and security. **Page** 52

its networks and remain compatible with both Australia[60] and the United States in the pacific region; who plan to transition from the current IP v4 to IPv6 by 2015.
As an explanation, IP is the language that is used on the network, and it is a way of finding resources on a network by using an individually unique number to identify a resource. But the current system IPv4 is running out of number combinations to identify resources on the net. The range in use by IPv4 is from 000.000.000.000 to 255.255.255.255.

This seems a lot of numbers, but when one considers that every bit of technology that connects to the network or Internet needs a unique number plus the amount of items there are globally, it is easy to understand how it is possible to run out of numbers. By adding every rifle, GPS system, soldier, radio, tank, plane, ship, etc, that will be on the future NCW network and the Global Information Grid (GIG), there is not enough numbers for this under the current IPv4 system. That is why most governments are going to the IPv6 system. This system has the ability to work with the current IPv4 systems during the transition but it provides the enhanced ability with 6 to the power of 48 combinations of unique network numbers.

As with both business and commercial network systems, the military will need to consider looking at the addition of redundant system to its networks. The military is the highest profile system for hackers to attempt to get into, according to the United States Department of Defence. Not every system will be hacker proof and very infrequently a system could go down due to malicious use or intent. There needs to be the consideration of built in redundancy in the network for just such a situation; a backup system if the main one is corrupted. Computer viruses have been known to lay dormant for a pre-arranged amount of time and become active when attention is no longer focused on the

---

[60] Warne, L., I. Ali, et al. (2004). The Network Centric Warrior: The Human Dimension of Network Centric Warfare. **Page** 108.

area. Left unchecked the virus could destroy or manipulate critical information.

But this need of security is not only for the individual computer systems themselves. It is also about protecting vital and critical infrastructure and hardware, for example fibre optic backbones, wireless towers and sender system as well as satellite receiver stations. Systems that transport the information are just as important as the information itself.

5. **Facilities:** Using the US quadrennial defence review as a guideline, new buildings will need to be built to support the increase of IT services. Specialist areas will need to be designed and built, where repairs and modifications can be done. Also new locations for servers and network components will need to be built to support the data increases on existing bases. These facilities will require a mobile or deployable aspect to them, for the support of long-term peacekeeping or long deployments overseas. This will help shorten turnaround times for components which can be changed quickly, if damaged, instead of sending the whole unit back to be replaced back at the main logistics facility.

6. **Personnel:** This has been covered in the opening of chapter 4.

7. **Leadership:** This area was viewed by the ABCA research as one of the most critically important areas. Leadership could make or break the introduction of digital technologies to the NZ Army and NZDF. If leaders show that they are willing to embrace the benefits that digital technology and the Network Centric concept, will bring to the realm of war-fighting, then its acceptance by those being led will be made easier. This is important at all levels, not just the tactical one, but the operational and strategic levels as well.

   As a counter point, if the leaders are not informed at the beginning of the program as to what the potential benefits are to them and the

troops they command, then how are they to convince the people that they lead? Indeed why should they. If there are some members of the army who don't like or don't want to take up the opportunities that are provided by the digital technology on offer, then there must be a way of minimising their impact on the other members around them. At the same time, if an experienced leader believes that such "opportunities" are suspect or not accurate there must be a way of letting them get a fair hearing to discuss their issues and concerns. In IT especially, inflation of the benefits is the rule, and leaders with experience have a reliable gut feeling as to what will and what will not actually help in a combat situation. Finding ways to assist the "Nay-Sayers" is just as important to the efficient implementation of digital technology as finding ways to assist the enthusiast.

Perhaps according to the literature, the hardest part will be convincing the non-technical branches of the benefits to them that digital technology will provide, while it is still in the development or theoretical phase. Sections such as infantry must be shown that digital technology won't be just something extra for them to carry around, adding to their weight, but a valuable tool. This will depend on getting the Senior NCOs onboard early. Branches such as signals already know of the benefits that the technology will bring, and can be used as an example and as a leadership demonstration.

8. **Training and Education:** This will be covered in detail in chapters 6-8.

With all of the focusing on the assets that have to be brought in or introduced there can be the tendency by nations to over look the influence that policies can have on the implementation of the NCW concept. From reviewing the available literature, four policies become potentially important:

1. ***Clearly defined goals:*** The NZDF needs to clearly define what it wants to achieve in its use of digital and network technologies. Clear goals need to be established at the outset of the development process.

The possibility of going away from the intended direction is much easier with digital technology than with any other technologies with which the NZDF is familiar with.

The need for clear goals is especially important for another reason: digital technology is essentially commercial rather than military restricted. Most military IT solutions come from the commercial sector first.

Every year new technology is developed by the commercial sector for use in business and technology environments, which would be of benefit to the NZDF, but with the constant change of technology the NZDF cannot afford to always have the latest and greatest technology in stock, or in its operational environment.

The process of getting and implementing the latest technology constantly would become cost inefficient quite quickly. Also the wants of the three services could put more pressure on the NZDF to provide the latest technology specific to one service, over another. This could lead to competition between the three services to the detriment of the Joint Forces focus.

A clear and defined plan needs to be made available to all three services, with each of them having input. Not just the IT sections of all three services but for all branches that would be affected by the introduction of advance digital technology. Consultation across the board is the only way to identify which components are needed by all the services and which ones are service specific.

2. ***Prioritisation:*** All of the members of the ABCA agreed that priority needs to be given to the elements or modules that are deployed in operations overseas, as these elements would be the ones actually putting the technology to its intended purpose. This would serve a dual purpose as it would identify early what technology would be of benefit

for future use and development and what technology does not actually provide the needed (though perhaps presumed) benefits.

Due to the nature of asymmetrical warfare and reinforced by the literature, the New Zealand Special Forces (SF) group of the Special Air Service (SAS) will need to have the highest training levels and standards, as it deploys with other Special Forces teams in operational environments. The technology being applied by the Special Forces is in constant use. It is the best available and is supplemented with the most recent developments. According to both doctrine and available policies, the nature of the SF job is to be the best solution for unconventional warfare, but the soldiers must be able to be trained and to practice with the most current gear to remain operationally ready for deployment. This means that priority must be given to the technology which the SF will need in order to be able to remain competitive and efficient.

3. ***Rules of engagement with the commercial sector:*** Using the United States as a template, policies and guidelines must also be in place to give guidance as to how the NZDF will interact with both the business and commercial sectors in the IT environment. The NZDF cannot achieve this by itself. Because businesses and commercial interests essentially drive digital technology, military ones do not. The digital technology provided to the NZDF – as well as to the worlds other military forces- is for the most part, digital technology developed by companies outside of the military. For example a computer firewall systems was picked up by the military after the commercial sector had employed them. This situation is unique in military history. Usually weapon systems used by the military have been built by companies outside the military to military specifications through bidding and tenders for the contracts.

This issue is particularly relevant for New Zealand. New Zealand has one of the highest rates of technology pickup in the world. Some of New Zealand's small businesses are leaders in the development of IT

services, such as Taite Electronics, and need to be tapped to help support and develop solutions for the NZDF. Just as Norway armed forces has taped into the resources and expertise of Microsoft for its command and control system services.

As an analysis from this research, the cost of critical infrastructure that is needed to support the IT change could be partially offset by going into agreements with local providers. This has benefits of supporting New Zealand businesses and communities but also providing the NZDF with a cheaper alternative than trying to finance and support critical infrastructure alone. These agreements could also give the NZDF access to highly trained personnel, which it could use to bring its own personnel up to acceptable skill and proficiency levels, on technological developments. The cost reduction could then be used to fund research into new technology to benefit the NZDF Joint vision, through the Defence Technology Agency. But there needs to be methods and processes in place so that a high level of security can be maintained during its development and deployment.

4. ***Policies for the protection of civilians:*** As was stated earlier, civilian employees have been shown to be able to fill gaps in operational capability, by both the United States and the United Kingdom. This could free service personnel to do their main jobs, without the risk of impairing the operational capability of a force. But as both doctrine and military law states a force commander must assess the risk factor to civilians and civilian assets involved. As they have a limited ability to protect all civilians and civilian assets that are engaged or used in military operations. The commander(s) must ensure that an acceptable level of security is in place, either through physical security, security response or effective prevention because in Asymmetrical Warfare as it is in Conventional Warfare, it is the enemy who selects the targets to attack. NCW is a good force enable, but it also opens up more valid targets for enemy forces.

As an example of this, a new grey area has developed with the progress of warfare. It is the impact of the media. Media journalists are now being embedded into forces and units on the battlefield. According to modern military law, it is the responsibility of the commanding officer to protect journalists or offer a reasonable level of protection to them. This raises the question of do they need to be tracked like conventional forces, using either a blue force tracker type of system? Or should journalists have access to low level NCW data feeds to help with the military media campaigns?

More questions will need answering. For example with the predominance of non state actors use of Asymmetrical Warfare and a basic NCW, will the military need to track civilian satellites, which have onboard cameras with sophisticated lenses to stop the media spying. As an even greater risk is the possibility of the enemy using programs such as Google Earth to spy on military build-ups and installations? Do commanders have the right to shut down or destroy the people who run or maintain programs such as Google Earth, if the enemy is using it as part of their NCW campaign? Where is the line drawn? Is it an issue of protecting civilians and civilian assets? The definition of these needs to be reassessed for the NCW environment.

These issues are only going to develop more with the advent of the open battlefield and the shift to urban warfare in the current Asymmetrical Warfare and developing NCW environments.

Chapter Six

Effects of NCW on Training and Education.

With the current focus on infrastructure, doctrine and policies, it would be easy to overlook what is in fact the most critical aspect to the successful implementation of digital technology. This critical aspect involves the people who need to be trained and employed to use this warfare enabler. According to the research and available literature, many of the issues in NCW stem from the Human Dimension[61]; which is why the NZDF need to ensure that its methods and procedures of training and continued education, are correct and to the best standards possible. Not for just the soldiers coming into the armed forces but also the soldiers, NCO's and Officers who already serve.

NCW and the NEA are tools developed to help win the next engagement that NZDF forces are deployed on. As with any tool – only more so-, if the operator does not know how to use the tool effectively, they run the chance of doing more harm than good, even to the extent of killing themselves or others.

The introduction of advanced digital technology has to be accepted as an inevitable fact for the NZDF, due to the pressures from the NZDF's allies and coalition partners. To remain interoperable with our allies and coalition partners, we must remain aware of the technology employed by them. The NZDF's soldiers and service personnel must be able to interact and employ that same technology in their operations. The issue of implementing digital technology and NCW, is not just about how such technology will fit into present and future Command and Control systems, but about how the soldiers will initially train and continue to train. According to the United States

---

[61] Warne, L., I. Ali, et al. (2004). The Network Centric Warrior: The Human Dimension of Network Centric Warfare. **Page** 108.

(USARI) and Australia (DSTO), digital technology has the ability to be able to help educate soldiers faster. It provides greater focus on information and techniques that will be constantly up-dated. This will come from the practical experiences and lessons learned from soldiers out in the field on operations[62].

This ability to assimilate new information quickly into training material and methods makes trainees more aligned with their unit's methods and procedures. It also helps to overcome the learning requirements they need to become competent in their jobs[63], not just in their new tasks of handling new technology but also in their standard mission tasks.

For the NZ Army, as an example, this will means that its Infantry personnel can be proficient in the latest techniques and methods used by an opposition, straight from training[64]. As well, it means that trainees, for instance, can now run through a training exercise with accurate data that has been updated in real time by intelligence assets such as observations by reconnaissance forces, UAVs or space based assets. This also means that trainees can have a better situational awareness before they even have started the training mission or leave the classroom. This method is also usable by the soldiers already on the ground who can run through a virtual mock up of the terrain ahead of them and find key terrain points and features to hep them navigate and reach objectives.

The issue that comes from these methods is the potential impact on mission planning and mission training. The images and intelligence provided to the planners could and can lead to misrepresentation of the true terrain. Assumptions on height of terrain features have the ability impact on the missions due to impassable terrain being assumed to be passable.

---

[62] Dressel, D. J. and Schaab, B. B. (2003). Training the Troops: What Today's Soldiers Tell Us About Training for Information-Age **Page** 30.
[63] Dyer, J. L. and Wampler, R. L. (2006). Training Lessons Learned and Confirmed From Military Training Research, **Page** 62.
[64] Ibid.

As an example, this issue has been proven by the hedgerows of France during World War Two, which were assumed to be small and passable by aerial photos and reconnaissance. These hedgerows were in fact three to four times larger than the estimates provided.

Also during the Bosnian-Kosovo war, space based satellite units and aerial recon units, were fooled into reporting fake targeting data back to higher command. Tractors with telephone poles were assumed to be tanks and were targeted for destruction, while the real tanks were safely hidden from view. Missions were assigned and rehearsed to engage these targets, which were not true targets.

According to some issues reported in a minority of research reports, Soldiers could be trained to have an over reliance on what is presented onscreen. Taking what is shown as true fact, or in near real time.

So the introduction of digital training becomes a key moment in the development of the future soldier. The skills that are introduced will provide the framework in which the soldiers will be able to adapt to new technological development, to remain competitive with our allies, and use information technologies to help win operations in the field. Digital skills and the use of digital training technology is not a skill set that must be introduced at a set time, unlike drill and ethos development, which need to be done at the very beginning of a soldier's career.

Nonetheless, as most of the NCW literature suggests, the earlier the soldier is exposed to the digital technology the more likely it will be that they will be able to come to understand and use it efficiently in their day to day needs[65]. The most efficient time according to both American and Australian research[66], to introduce these skills would be after basic training, where the soldier is still in

---

[65] Hess, K. P. (2003). Training Adaptability in Digital Skills: The Learning Skills Bridge (LSB) Learning Accelerator, **Page** 52.

[66] This was shown in the DTSO report on the human factors of NCW and in the training requirements report of the US Army Stryker Brigade.

a learning frame of mind and has the support network from his basic training group. This peer support and learning has been found to be the most efficient way of introducing new military IT technology to trained soldiers. There should be enough guidance to help out with complex tasks, but a set framework with goals and achievements should be sufficient to make soldiers proficient in basic computer and IT skills[67].

As a counter point to the previous argument, if the ability to have large groups sit down to a formal IT training session is not possible, then new methods may need to be applied in conjunction with other lessons. This may mean using overlapping classroom events to teach basic IT skills. Demonstrations by ABCA partners have shown that this could be done with soldiers learning how to strip and reassemble a rifle via an interactive CD-Rom. At first glance the soldier is learning the skill of assembly and disassembly of their rifle. But to reach this stage the soldier will have to learn how to use the computer to access the CD-Rom. This will allow a form of passive learning, while the active learning is the rifle lesson. Another solution would be a selection of self-paced IT packages either online or downloadable, such as the lessons available on Massey University's online WebCT classes, for different courses or skill sets.

As it has been suggested before, soldiers are the most important factor of the modern and future combat force. **Appendix B,** shows the skill sets that are currently developed during basic training plus skills identified by ABCA NCW research that could be introduced either at the very end of basic or as a separate component after basic training. According to the experiences from the United States, these skills should be the minimums that are introduced, as they cover the vital information for most IT systems. Both the Australians and the Americans believe that the soldiers need to be shown how the system will benefit them and their chosen field. This helps the soldiers see that IT and ICT systems are there to help and not make their tasks harder. Reinforcement

---

[67] Schaab, B. B. and Dressel, D. J. (2001). Training for Adaptability and Transfer on Digital Systems, **Page** 51.

of the importance of these skills and technology will help with the future transition to more advance systems as well as software and hardware updates.

The United States Army found in its research report 1774: Six myths about digital skills training[68], that:

> *"Systems will become easier to use, but training needs will grow as system capability increases. Digital systems should be accessible and used for work routines whenever possible to support adaptation to system changes."*

There is a common myth that technology will become able to solve most future problems. This misconception is dangerous as it gives people the false view that the training in such technology will become easier also. This is not so according to *Brooke B Schaab* research work called Six Myths about Digital Skills Training (2001). According to Schaab, training for a digital environment will never be an easy process to introduce, as many people currently in the services have a mistrust of technology and see it as a way of increasing their work load. This is known by psychologist as "negative experience transfer". This is where older more experienced soldiers have difficulty transferring their methods and skills over to a new system. A prime example is when older pilots have to transfer over from analogue controls and instruments to new digital controls and displays.

The need for the systems that are used in operations to be available for training is not always cost effective, if the units are expensive to get and maintain such as the Javelin Anti-tank missile system[69]. A solution to this is simulation. This will be covered later in more detail.

Basic keyboard skills such as touch-typing are becoming more important in everyday life and the armed forces are no exception to that rule. From emails

---

[68] Schaab, B. B. and Moses, F. L. (2001). Six Myths about Digital Skills Training. **Page** 34.
[69] The Javelin Anti tank system cost is found in the ammunition, each missile is worth in excess of $25,000. So live fire training is not cost efficient.

to presentations in Power Point accurate keyboard skills are a requirement to produce quality documents and displays, as well as orders and instructions from commanders. With technology developing at a high rate the possibility of a soldier-to-soldier messaging system is becoming more of a possibility. Such systems could be in the form of the Blackberry system [70] by Vodafone international or a Personal Data Assistant (PDA)[71] which each squad could carry. It would be used to be kept informed of changes to the commander's intent or updates of tactical maps from the company headquarters or tactical command post.[72].

The ability to be able to format and present information quickly and efficiently get it out to troops, or to the right people, is critical as the OODA (Observe, Orientate, Decide, Act) loop begins to shrink due to information technology. With the increase of information flow, soldiers will need to learn how to put it into a usable context. This is where the skill of data management could come in useful to the soldiers, including front line units, who could have vital tactical information on enemy units or of enemy movement which could affect a whole battle plan. Just as all soldiers on their All Arms Recruit Course (AARC) learn how to use communication equipment and the right way of passing information over the communications network, soldiers will need to know how to transmit digital information in digital format over the same networks.

This requirement was clearly demonstrated during the war in Afghanistan, where SF forces used laser target designators to spot and fix targets and to send the data directly to an air asset in the area for their destruction. Due to the loss of the RNZAF strike wing soldiers will have to interact with coalition aircraft through digital communications or digital networks. This is one application of "sensor to shooter" technology, and New Zealand forces must

---

[70] Vodafone Blackberry, an integrated, phone, email and Personal Data Assistant: http://www.vodafone.co.nz/blackberry/blackberry.jsp?st=ourservices&ss=mobile_email&item=blackberry retrieved 26/05/06

[71] The Command Data Assistant has just entered operational service with the latest rotation of troops to Iraq.

[72] Wendt, L. A. (2004). The Developmental Gap in Army Officer's Education and Training for the Future Force. **Page** 75.

know how to be proficient in this if the want to remain interoperable with coalition allies.

The table in **Appendix C** shows the current digital skills levels in each career option. It shows that a majority of the career options either need to enhance their current skills or to develop the basics in order to be able to work efficiently in a NEA environment. These were defined and refined by operational research done by the United States, from their experiences from OIF and OEF.

It also shows some options which will not need to develop high-end skill sets. Careers such as stewards, bandsman and fire fighters do not need to have the IT skill levels of people in ICT or IO combat careers. But since however, everyone is a soldier they would need to posses enough skills to be able to temporarily work in the front line, or combat careers.

This is not about learning mouse and keyboard skills but also the ability to use and manage data and information to the best possible level. All members of the ABCA research organizations show that, the force that can manage and use its raw and processed data fastest can end up controlling and manipulation the battle space to their advantage through increased situational awareness both of themselves and the enemy. So soldiers with digital skills will be of more benefit to the future battlefield and operations[73] through the developed ability to redefine tactics and techniques faster, such as swarm tactics. The digital soldier will also be able to increase the operational tempo to such a high level that individual operations could flow into each other or change as the circumstances dictated.

As an example of this is a company from the 172nd Stryker battalion in Iraq who had the ability and flexibility to change its mission quickly, when a suspected terrorist cell was intercepted accidentally at a checkpoint. It could

---

[73] Graves, C. R., and Pratt, D. M. (1999). Force XXI Training Program-Digital Project: Report on Development and Lessons Learned, **Page** 124.

access the data network and co-ordinate with other local units (both air and ground) to track and trace the vehicle back to its base, then have the Stryker unit successfully assault the hideout within an hour of the check point being breeched. All the time having C2 support and enhanced situational awareness.

According to the United States Army Research Institutes findings, the future battlefield that soldiers face will be dynamic, with a higher operational tempo. The awareness, views and data that the soldiers have access to, will allow them to adapt quicker to the changing surroundings and adapt mission requirements and end states in an effective timeframe[74].

As seen in the previous sections, the need to bring digital training into a phase near the completion of the All Arms Recruit Course, either through passive or active techniques, will become increasingly important. The advantage of digital technology is its flexibility. The systems are available nearly 24 hours a day except for time for maintenance and updates, seven days a week. This could provide the opportunity for training systems to be set up at short notice, such as a rapid deployment of troops to protect or extract embassy personnel. If an unforeseen event takes place such as snow or bad weather the time could be used to introduce or use digital training. This would not be a matter of just sitting the soldiers down in front of a computer with business applications. More crucially it encompasses the use of simulators to replicate environments to train in, with weapon systems which have been integrated into simulation software and hardware. Fortunately simulations are available constantly. This idea and concept will be discussed later on in more detail.

According to most of the available NCW research, expanding the AARC to an extra two weeks or following the US Army's approach of a New Equipment Training (NET) phase after basic training, could give instructors and trainers enough time to bring the soldiers up to a sufficient skill level to be handed over to command NCOs, in units for in-house training. This has been

---

[74] Moses, F. L. (2005). Training Challenges for Digitization. **Page** 34.

identified as having a two fold advantage:

1. The NCOs will get to bring the new recruit into his unit and spend some time showing how the system they have been trained on works in a active operational context;

2. The soldier forms a closer bond with the senior NCO and knows who has the required skills set and knowledge to help out if the soldier has an issue with the system.

   The initial problem identified by all major NCW research is getting the Senior NCOs up to the level where they can teach others under their command to an effective level on constant hardware and software updates. New versions of software will add or modify the way the system works. The adding of a new menu item will need the trainers and command NCO's kept up to date on the modifications. This comes back once again to time available for training the NCOs. The outlay can be expensive in time and resources but the benefit in having people readily available to help train can pay a big dividend later on down the developmental process and can speed up a digital training program as a whole.

3. Officers will need to start focusing on the benefits and issues a networked army will have and the way future operations will run. Using digital technology Officers will need to be able to lead the way so that the people under their command will follow them and have trust in the concept, making it beneficial to the NZ Army and Joint Service. Junior Officers (2nd Lieutenants, Lieutenants, and Captains) have been identified as the ones who will have the most need for digital skills. They will be the ones actually leading the troops who have the digital equipment into combat. They will be in charge of the future command posts, which will be collecting, analyzing and distributing the critical

data both up and down the command system, and across to other command post in a process call 'Horizontal Fusion"[75]. Such Officers will need to know how to interpret the raw data into usable information and how to distribute it to the people who can turn it to the best tactical advantage[76].

This is demonstrated clearly with the application of intelligence from other sources and services[77]. Most strategic intelligence is being managed in electronic form for ease of transport, use and storage by the intelligence community. This means that its integration into the NZDF systems will be predominantly in electronic form. According to the United States Army's Future Combat System (FCS) project, operational Intelligence updates and amendments will soon be digital, instead of flags and tags on a map or whiteboard. Many forms of digital Intelligence will not just be in a textual format. They may be images, Excel or Access databases, or even to the extent of stored digital communications.

With the addition of digital encryption to coalition Command, control and communications (C3) networks, the need to be able to understand the use and maintenance of the encryption keys is becoming more critical to success. Therefore minimisation the risk of interceptions and cracking of secure data networks. New keys and encryption protocols are transmitted digitally or through secure channels to commanders and they must know how to use, enter and securely destroy the keys.

Without these digital management skills there is the high possibility that soldiers or whole units could be locked out of intelligence networks, or access to up-to-date information, would see the removal of the situational awareness advantage that the network provides to the War Fighters.

---

[75] Dressel, D. J. and B. B. Schaab (2005). Training Requirements of Digital System Operators in a Stryker Brigade Combat Team, **Page** 37.
[76] Wendt, L. A. (2004). The Developmental Gap in Army Officer's Education and Training for the Future Force. **Page** 75.
[77] Government Communication Security Bureau, Defence Directorate of Intelligence and Security, Security Intelligence Service, External Assessment Bureau

So as a consequence of this, there will be a special challenge in managing staff in digital technology units, experienced in combat. In particular the junior officers will need to develop the skills and intuition that senior officers may have developed over their careers. They must learn to be able to separate the critical information away from the non-critical information but within the increasingly high speed environment of digital technology and the NCW context.

Under traditional means, the relevant experience used to be obtained by overseas deployment for selected officers and then propagated upon their return to New Zealand. But the situation is becoming more complex than it has been at any time in the past. The security environment is increasingly unstable New Zealand is being asked to contribute more troops at short notice, to more fragmented peace keeping missions. These missions require increasing inter-operability with the personnel and equipment with different standards to New Zealand. There is a critical need for Officers and Senior NCOs, of any nation, to work efficiently straight away in an environment which is attempting to gain information superiority over its enemies.

So as a consequence of this issue of getting soldiers and Officers the needed experience, many nations are starting to use embedded technology that is in their systems. This doesn't mean that classroom time should be minimised and all of the information put to a digital medium of course[78]. The need for classroom time is still a basic necessity of any training environment. The hands on approach are still worth much more than a Power Point presentation or a text document on a screen. This comes about due to people's aversion to staring at a static screen for long periods of time without mental stimulation or physical interaction. Nonetheless digital technology has its uses as a support tool for teachers in most learning environments. If students have the ability to access supplemental information while they are learning, this will help to reinforce the lessons learnt.

---

[78] Gentry, J. A. (2002). "Doomed to Fail: America's Blind Faith in Military Technology.". **Page** 101

Here are some examples derived from both the literature and research,

- If a Personal Data Assistant has the correct sequence on how to assemble and disassemble a rifle in a short video, or interactive demonstration, it gives the soldier a quick reference guide to help trouble shoot an issue they have. This is better than a manual as the components are able to be manipulated or rotated by the trainee. The manual will still be available to the soldier when needed but they will have quicker access to the information if they have an electronic means to access it. Either the teacher or soldier can add additional notes or personalised notes to an entry on the PDA.

- Updates to regulations and orders can be sent to soldiers instantaneously. New lessons can be applied to doctrine and policies which are kept by the soldier. Currently the United States Army has a unit called the CDA (Commanders Data Assistant. It is a militarised version of a PDA which works with tactical radios, it has the built in ability to interact with Blue Force Tracker (BFT) which can work in a networked environment)[79]. Financially, such PDA's and CDA's would have to be restricted to Officers and senior NCOs during training but with the price of information systems constantly coming down expansion into the other ranks use could be closer than expected.

- The current NZDF intranet and internet could be configured to act as a teaching resource, to the extent that it could act as a distance learning portal for troops who are deployed overseas to keep up with their training and promotional requirements. This

[79] The CDA: http://www.defense-update.com/products/c/cda.htm Reviewed 17/06/06

has been proven with the US Army's Army Knowledge Online (AKO) and EArmyU programs[80].

- Digital technology can also teach not only cognitive skills but motor skills. The New Zealand Army's Simulation Centre has a training facility and resources to teach rifle and weapon systems skills to soldiers. These can range from the standard Steyr rifle to the Javelin anti-armour missile system, as well as the Mistral anti air system. There will be more on this topic in the simulation section[81].

As a counter balance argument to these issues, Information and communication technology is only a tool set to the soldiers. It is a means to an end for most operational needs. But it is proving to be more and more critical to today's high tech battlefields. The possibility of the Army relying too much on technology could pose a problem and an inherent flaw to any future military campaign. This is based on the following reasons and flaws found in the review of the NCW literature and research.

Reason One: For every technological development its counter has been discovered and employed. During the 1990-1991 Persian Gulf War, the reliance on GPS became a critical factor due to the featureless desert environment that dominated the battlefield. However, because of the heavy reliance on battery powered objects and the stalled logistics lines, some operators lost the use of their GPS systems and had to rely on traditional navigational and orienteering skills to be able to manoeuvre away from the enemy. This dangerous situation had the potential for large fratricidal (Own Force) casualties[82].

---

[80] Lorenzo, G. (2002). "eArmyU and the Future of Distance Education." The Technology Source, http://www.thetechnologysource.com Retrieved 13/02/2006.
[81] New Zealand Defence Force (2006.). New Zealand Defence Force: Statement of Intent. **Page** 61.
[82] Talbot, D. (2004). "How Technology Failed in Iraq, " Technology Review: Emerging Technologies and Their Impact, retrieved from http:/TechnologyReview.com/Infotech/13893/page1.on 18/03/2005

A constant theme through out all of the available research was that basic military skills cannot be neglected in the information age. The ability to map read should not disappear because of the introduction of GPS units that can be integrated into many items[83]. Basic live fire training should not be totally replaced with virtual environments or simulated fire, or visual stock takes minimised due to inventory control systems and barcode scanners. ICT and IT are enablers but cannot and should not replace all aspects of traditional training.

Without these core skills, soldiers could be rendered ineffective if the technology fails or if counters are introduced. And with stock levels being represented on computer systems, there is the possibility of stock and weapons going missing due to the fact that the system isn't presenting the actual available stock levels, only the data that has been put into the system. This flaw has been shown recently with military weapon systems and grenades being found on private property by New Zealand Police raids.

Reason Two: Each individual soldier will react differently to different training methods. Some soldiers learn faster with visual learning styles and digital based training is designed for these people[84]. Other soldiers will need practical experiences to be able to firmly reinforce lessons into their memories. Using digital training methods requires that the verification and validation of the acquired skills in real world situations will need to be done to a high standard as with any training. Digital learning can accelerate the uptake of skills but it can also accelerate mistakes and skill shortcomings. Mistakes can be trained out by digital training methods for example rifle accuracy. As long as the initial digital training process is not flawed, for example, the simulation misrepresents the distance on a rifle range or the trajectory of a shot, soldiers should be able to modify their reflex skills and remove identified bad habits on a digital range before a reassessment on a live firing range.

---

[83] Gentry, J. A. (2002). "Doomed to Fail: America's Blind Faith in Military Technology.". **Page** 97
[84] Nanda, S. (2005). Applying Technology to Train Visualization Skills. I. **Page** 206.

Reason Three: The reliance on technology could possibly lead to a form of lethargy by instructors and trainers, where they get into a routine of presenting the same material the same way. Instructors and trainers need to be able to learn how to create and sustain real life scenarios for their training resources. This provides them with continued education and also with a form of vetting and validation for the training data, so that trends and methods can be identified and integrated into the training system and lessons. Instructors and trainers who have taught and seen the results of the material they have used can be the best moderators of the quality of the training.

With digital training there needs to be a form of feedback that the soldiers can follow which is independent of the training system. After Action Reports and interviews need to be set up to provide feedback as to how the digital training and the real world experiences match-up. There is no point in soldiers waiting until they are updating their skill sets to point out a discrepancy between what instructors are teaching and how the employment of the digital technology such as the Joint Command and Control System (JCCS) is used in operations. Soldiers may know of a shorter way of doing a task that they learnt on operational deployment, which would be of benefit to the instructors to know, then the instructor could modify or amend their training to incorporate this new method.

Reason Four: Overconfidence in digital technology in training also causes the danger that instructors will tend to go towards thinking that the skill they must be teaching for the digital environment is "why the system works as it does", rather than "how the system works for the soldiers". To counteract this, there needs to be a clear understanding that not every menu option or every system detail needs to be explained to the soldiers. What needs to be explained is how it all works together and interacts with other digital systems. Soldiers need to know how the data that they put into the system is managed and how to read and use the outcome from the system and from linked systems that feed theirs. The United States Army found that most of its soldiers on operational deployment did not know how their system interacted with the rest of the systems in use; this led them to not knowing how to send

the correct data between systems[85]. If the New Zealand Army can get its embedded digital training systems[86] set up correctly at the beginning of its deployment of digital technology and give its soldiers a complete overview of how their digital systems interact with the other systems, showing them how their system works in the context of the "System of Systems", many of the problems faced by the United States Army can be avoided[87],[88].

The most important point is to try and differentiate between what is an acceptable use of digital technology in training and what methods are used to teach digital training. How much reliance on technology should be given so that soldiers remain interoperable? While not forsaking techniques and methods that have proven successful without technology. These questions will need to be looked at by trainers and instructors if New Zealand is to venture into the NCW environment.

So with the military needing to be aware of its responsibilities to ensuring a quality education to its soldiers and service personnel, the focus then starts to shift to the issue of what is happening to the potential recruits in regards to their skill sets before they join the armed services. Research publications such as Marc Perenskys *"Has "Growing Up Digital" and Extensive Video Game Playing Affected Younger Military Personnel's Skill Sets?"* or Roy C. Campbell's *"Future Soldiers: Analysis of Entry-Level Performance Requirements and their Predictors"* have started to look at what IT skills are being brought to the armed forces.

With the availability of personal computers in both home and schools the level of information technology awareness is increasing every year. Most schools are introducing computers early in a child's development from at least

---

[85] Warne, L., and Ali, I. (2004). The Network Centric Warrior: The Human Dimension of Network Centric Warfare. **Page** 108.
[86] Training events or capabilities that are embedded into systems that are used on operations.
[87] Dressel, D. J. and Schaab, B. B. (2003). Training the Troops: What Today's Soldiers Tell Us About Training for Information-Age Digital Competency. **Page** 30.
[88] The number one issue stated by surveyed soldiers, was that they did not know how their system worked in relation to the other systems in use around them in an operational context.

standard one. The children are being exposed to keyboard skills, mouse skills via interactive games and to some extent the Internet. These skills are being developed throughout the school years in classes such as computer science, IT classes and general lessons. It has also led to the adult population becoming more IT literate as IT services become more integrated with daily tasks, such as Automatic Teller Machines (ATM), online shopping and ordering of products from E-commerce sites etc.

More and more homework for children is being researched online, while businesses are using Internet based software so that some employees can work from home to minimise cost overheads. People are setting up home networks in order to be able to share Internet connections and printers to play networked games. Some of these people are as young as nine or ten. With IT skills being introduced at such a young age, the army has the potential to identify the people joining it ranks that possess high IT skills or aptitude and divert them away from the traditional career paths into IT and advance IT areas.

This can lead to a misdirected policy, where the NZDF could assume that the people entering the armed services have enough skills, from prior exposure, to be able to implement the network force policy without additional training. With the introduction of the NEA more IT skilled people will be needed to make the process work effectively. This is true for all of the New Zealand services; both Navy and Air Force need to be doing the same as the army, or at least have access to a combined advance IT service pool.

Therefore, according to the experiences of the United States, career paths such as Information Operations (IO) and Information Warfare (IW),[89] need to be made more visible to prospective recruits early on so they can make an informed choice. Even if they are focused on choosing a combat career, the benefits of going to either IO or IW specialities needs to be made very clear to them.

---

[89] Denning, D. (1999). Information Warfare and Security. **Page** 66.

This appears true of people who want the army experience, but not a front line career path. The need for IT aware people to service systems, by adding updates to software, repair networks as well as infrastructure is as important as the need for people who use digital technology to engage the enemy. People who know about database management and integration or data mining can be of as much benefit for the intelligence section as the people out in the field doing surveillance and target acquisition. Therefore the need for IT specialist is there. A policy of identifying the already advance IT aware recruits and documenting them is the most effective way to meet this need, but as a second recommendation derived from the research, would be a lowered entry standard, that could be used for potential soldiers who could be restricted to the IT services. As it has been stated before, it is easier to train someone who already has IT skills than it is to teach an IT novice.

With this, the stereotypical image of a "geek" or "nerd" behind a computer screen or inside a computer system needs to be removed or modified for the military context. The required image of all soldiers using digital technology needs to be accepted and integrated into the NZ Army's cultural identity. People who join the NZ Army, who are identified as having high IT skills, need to understand that they will not be sitting in front of a computer screen away from any action, but could be deployed to an observation post, command centre or even an operations planning cell[90].

Here are some possible career paths for such IT aware recruits that have been identified by international research:

- Predominantly the Special Forces units employ the most advance IT solutions. The macho image of a soldier out in the wilderness with just his gun and knife made popular by Hollywood and Rambo type of films, no longer applies to the

---

[90] Koucheravy, R. J. (2001). Whence the Soldier of the Future? Recruiting and Training for the Objective Force. **Page** 56.

NCW concept. These forces are made up of highly trained and educated people.

- The combat position of sniper/scout also use high levels of technology from laser range finders, laser target designators, digital optical scopes, thermal and infrared scopes. These soldiers must know how their systems work and keep them working, plus how to interact with coalition technology.

- Some of the people identified with high level skills, but not up to the physical fitness levels of the Special Forces could be placed in a command post directing Special Forces units and support services. They could provide up-to-date intelligence; send reports out to the troops and using the data provided by the forces to plan additional or new missions for these forces.

- If New Zealand decides to follow the United States lead and attempt to turn the Light Armoured Vehicles into a Stryker brigade, the high level skills identified could be put to use inside the battalion, not only in the headquarters but also in frontline sub-units[91]. Digital operators are a key component of the brigade combat team.
  Their skills must be of a high level to provide quick and accurate responses to raw and processed data, which is coming in from multiple sources, both organic to a unit and attached. The digital systems operator in a Stryker unit has the potential to become part of the sensor, decider, and shooter cycle in a networked environment[92] above their traditional role in the unit, such as commander, driver or gunner. Therefore their skills and training must be to such a high level that they can perform effectively in both needed roles.

---

[91] Dressel, D. J. and Schaab, B. B. (2005). Training Requirements of Digital System Operators in a Stryker Brigade Combat Team, **Page** 37.
[92] Ibid.

- Whether or not the New Zealand Army or New Zealand Joint Force follows the United States model for the digital brigade, it must have advance IT trained people ready to adapt New Zealand's IT technology to the proposed military Global Information Grid (G.I.G)[93]. This network will be a global data network, where all allies and coalition partners will be connected to one large interoperable network.

The G.I.G is the culmination of many of the United States programs, and it will be using the IPv6 infrastructure to provide all of its soldiers, platforms and allies a presence on the network. New Zealand needs to have the skill sets and people available to adapt to its proposed methods and standards, so that the NZDF and its resources can be present on the network.

If New Zealand wants to be an active partner in future coalition operations it needs to be able to deploy, manage and sustain its presence on the G.I.G and not put the rest of its allies at risk with bad digital methods and practices. New Zealand needs to know how to work in a Common Relevant Operating Picture (CROP) with digital forces. Those in the NZDF specialist IT groups will be the soldiers who posses and implement such knowledge, but it will be the average service person who will use the services and resources provided by the G.I.G.

With the introduction of IT services and technology, the need for soldiers to be more aware of the potential for such digital events as hacking and digital attacks, becomes more important to operational success.

It is at the most fundamental level, that the security of a network is only as strong as the weakest password. A simple easily remembered password could compromise a secure network and allow malicious entities into not only

---

[93] MacMillan, K. (2005). Evolving Command & Control: The Challenge for Smaller Defence Forces. **Page** 6.

local inter and intra networks, but also attached allied networks. This could cause New Zealand's allies to detach their resources and assets away from the NZDF's Command and Control (C2) assets, technically blinding them to the events on the battlefield. By denying access to support services and combat assets there could be a loss of service personnel lives. Again, correct implementation of secure services and servers needs to be in the minds of all people who could interact with the internal digital operations network or the G.I.G.

Other examples of security breaches could be:

- A hidden virus on a disk brought from a home or unsecured network causing damage to data, change data or drop a network at a critical time.
- Storing confidential or top secret information on a wireless device such as an unencrypted Vodafone Blackberry[94], PDA, or cell phone,

This basic security needs must be shown and explained to all soldiers so that they are aware of the consequences of bad practices. Special Forces troops must have the highest awareness as they have access to the most secure information on a network and also provided some of the most critical information to the network. Special Forces personnel need to be held to the highest standards, but also have the access to personnel who can help and advise on the best course of action for them and their data.

In detail, according to the available research, all soldiers will need to be aware of how the classification system works for digital information and hardware. How to dispose of digital material will need to be shown to soldiers so that no trace of data can be found on a disposed media item such as a disk, data tape, hard drives or computer RAM. Too many times the media has had news

---

[94] GCSB Security Notice– Blackberry PDA Use, 30 June 2005

articles about computers that were disposed of by military units, with secret or secure data still on the drives or stored in the RAM.

The storage techniques and methods of securing data must be shown to soldiers and kept up to date with government standards and policies, either provided by NZDF or the Government Communications Security Bureau (GCSB). These sources have the technical expertise to manage the correct policies for data disposal.

Both the Australian and American research shows that data transmission techniques, methods and policies must be introduced to soldiers so that they can be educated to a high standard, just as they are for voice communications over the communications network. Interception of unsecured data transmissions has been shown to be just as dangerous as unsecured radio traffic to soldiers in a combat environment. This becomes even more important when the data being sent by soldiers is a transmission package with location coordinates for a platoon or larger force element. With some communications and data equipment a constant signal can be sent out to establish its position with the GPS system. This signal can be fixed to a location and tracked by an opposition force with the right equipment[95].

Soldiers need to be educated about the potential for security breaches from digital IT systems otherwise the cost could be heavy in loss of service personnel. The benefits to soldiers who are trained and proficient in IT services and equipment security comes from the capability to exploit the same digital weaknesses in an opposition force which can provide a tactical advantage to their force.

---

[95] Venzke, B. (2003). Al-Qaeda's Advice for Mujahideen in Iraq: Lessons Learned in Afghanistan, retrieved from http://www.intelcenter.com. Retrieved 03/05/2006

With the introduction of the JCCS system[96] in to joint use, the need to have soldiers who can manipulate and understand the joint data coming into the system will become more critical to successful operations, both single service and joint. The JCCS system, according to its tender, will be designed to give the soldier at the front the ability to direct relevant unit assets which are either in the Rear Areas or in deployed formation in the support area, such as organic artillery which is linked to the frontline soldiers through the JCCS system. This is where concepts such as the idea of the "strategic corporal" can come into play. Where a common soldier can influence and redirect the overall picture and strategic context.

The skills that can be applied to the Joint environment will also benefit the single services as well. The Command and Control systems that are employed by the individual services internally will be able to interact with the JCCS system, providing a training environment which is unified and has good information flow between all of the components.

When working digitally, information can be passed along at a faster rate than if the services were acting independently. But this is only possible if the format that the data is being sent in is uniform across all of the services. This issue has been a large problem for the United States military. Even down to the individual services the systems are not set to a uniformed data format.

For instance systems which make up the Army Battle Command System (ABCS) such as the much respected Force XXI Battle Command Brigade and Below (FBCB2)[97] battle command system and Blue Force Tracker (BFT)[98]. According to USARI reports, these systems have had issues with the other

---

[96] "The JCCS will provide the means by which commanders at strategic, operational, and tactical levels execute command and control (C2) of the NZDF forces singly, jointly, within a combined force, and within a coalition environment. It will ensure a sustainable C2 interoperability framework, including relevant non-defence organisations."
http://www.Defence.govt.nz/industry/jccs.shtml

[97] These systems form the basis of the US Army's Battle Management System (BMS). BFT shows digitally when units are located on the battlefield, in near real time to help offset fratricide.
[98] United States. Navy Dept., Institute of Land Warfare (Association of the United States Army), et al. (1994). U.S. Army field manual 100-5: Fighting Future Wars. Washington, Brassey's (US).

systems in the group due to different data formats being used in the individual systems. Even systems which are located next to each other, cannot communicate unless the soldiers running those systems actually talk with each other and decide on a common data format with agreed policy and standards. This is an issue that comes about from the attempt to integrate new digital technology systems with old legacy systems between services. Some of the new digital systems are not compatible with the legacy data formats of other joint service systems. In a Joint environment, service personnel will need to know or be aware of the resources that are available from the other military services and how their systems produce data and in which format.

As a recommendation from this research, the issue of mismatched data formats between services assets must be avoided with the introduction of the JCCS system into military use. The Joint system will only be as good as the people sending and encoding the data. The JCCS system must be compatible with all of the platforms and data types in use by all three armed services. This is especially needed for the Army's LAV platforms. These platforms could be acting as the main data and information point for the soldiers on the ground when they are deployed. The information from the soldiers on the ground must be fed into the systems onboard the LAV's correctly and in the right format, so that commanders in the joint HQ can use it quickly and also between service assets.

As an example of a possible future system, a LAV unit could need the support of a naval unit which is sitting off shore. A fire mission could be set up quickly by the LAV digital operator, by placing a naval Target Reference Point (TRP) onto a digital map display. This display system instantly sends the TRP to the naval ship with the data tags that would be embedded into the TRP icon which would send correct authorisation, round type and number of rounds. The data would be sent in a short data burst which would be hard to detect by enemy forces instead of a long voice communication. This is dependent on the data being able to travel from the Army's C2 along the JCCS and onto the

Naval C2.

This advantage will only come about if all the service personnel are trained or made aware to send data in the right formats and standards for a joint environment. Currently such training can be made available to specialists, such as Forward Observers, Naval Fire Support or those in command of units. But with the continuing development of IT and NCW, the data paths between the services will become closer, to the point where all Joint assets could be integrated and work as if they are organic to a unit. This is where a single data system is in use, for all three services for their C2. This has the possibility to lead in the future to where individual units are able to use assets that are maintained by a separate service, as if they were organic to them without the currently needed specialist knowledge. The NCW network would take care of the specialist knowledge required, via an integrated combat AI (Artificial Intelligence)

Currently there is a need to cross train some but not all of the personnel from the services for a NCW joint operations environment, but this will lessen as the development of technology progresses. Joint systems with standardised data formats will help lessen the need to train service personnel to work with the current setup: Service Ones C2 onto the JCCS then out to Service Twos C2 and back.

With the issues of ***why*** there is a need to train for and with digital technology in a NCW context being shown in this chapter, the next issue to be looked at is ***how*** this could be achieved. Both chapter Seven and Eight will be looking at this issue.

Chapter Seven

The Use of Digital Technologies for Training in NCW

With the advent of the digital revolution, many new types of training have become available. The physical distance between resources and assets is no longer a major issue to commanders who want to train with multiple units, which could be spread out between different bases or locations.

The types of digital training can be put into three main categories[99]:

- Live
- Virtual
- Constructed

These will be discussed in more detail later on. But a brief description is required here to make the point that immediately follows

Live training: It is where the soldier is in the field with his equipment firing real ammunition at targets, and using real operating systems such as command, control and communications. The equipment, systems, and tactics they employ are exactly the same as those they will use out on operations and deployments.

Virtual Training: This is where soldiers are using a mock up of the systems and equipment that they use in real combat situations. This can be in the form of a driving simulator, a weapons range, or a re-creation of a weapons'

[99] Sieberg, D. (2001). "War games: Military training goes high-tech". CNN.com. New York. Viewed on November 23, 2001

system that is too expensive to fire in a training environment, such as the Javelin anti-tank system.

Constructed Training: This is where a system is used to display units or resources in icon form to show a technique or tactic which is too large to be replicated by either live or virtual means. This can be a diagram of a deployed battalion over a wide area of terrain which would be impossible to display on the ground. Constructed environments are the best way of showing a bird's eye view of a battle space. All three elements can interact and exchange data or they can be used independently of each other.

Digital networks are becoming stronger and more reliable. This has given military planners the ability to plan training operations and joint exercises which don't have to be in the same country. As a prime example the Australian Defence Force (ADF) has just recently finalised a joint training infrastructure agreement with the United States Department of Defense. This agreement allows the linking of digital training methods between the two countries at their respective combat training centres. This will allow the services to train together with their respective equipment in a joint environment and to better allow themselves to work more efficiently together. According to available research, even though the physical distance between the units could be many thousands of kilometres away; they can train as if they are working side by side.

An example of this could be a Headquarters unit that would be using a replicated command, control and communication system to provide directions for a second group of troops who are either in another virtual C3 environment such as a tactical operation centre or who are on a digital firing range. It can also be a unit who is engaged in a live field exercise as well which is being fed targeting data from a simulated event. Real time information can be sent to the Command, Control, Communications, Computers and Intelligence (C4I) system(s) which can interact with simulated information to provide a realistic training environment.

With the flexibility of digital training methods available, soldiers have the ability to be step trained. According to the Australian DSTO work entitled "*The Network Centric Warrior: The Human Dimension of Network Centric Warfare*" This process takes soldiers who are commencing their initial unit training and have their individual needs meet through skills development such as live fire exercises (rifle range) and field deployments. The same soldier is then feed into squad based training which can be either live or virtual with his squad mates. This can be done on digital firing ranges where more weapon system can be introduced which would be cost ineffective in a real live fire exercise. The squad can then go through squad tactics in a virtual environment or PC scenarios to get the group cohesion working before being sent out on a validating and certifying exercise. Once the squad is working cohesively then the platoon level training can be entered into by either live or synthetic (Virtual or Constructive) training. These steps can be taken all the way up the unit formation.

The difference to current methods is the speed at which this process can take. Multiple training and evaluation cycles could be taken in a short time and any additional training, which may be needed to modify errors or issues, can be taken quickly while the lessons are fresh, and before they become habit.

This type of approach has already been displayed internationally by Special Forces units who can act as individuals or as part of a squad to achieve mission objectives and the Live, Virtual and Constructed training that enhances the abilities of the troops involved through speed and repetition. This process of using digital training methods also helps to offset unforeseen issues or incidents.

When a commander is planning the training for a selected unit, they have to make the assumption that the weather will be favourable or to a lesser extent the minimum required standard to achieve the selected training.

According to publicly available doctrine and policy manuals, the designing of a training program is done many weeks to months in advance, this is to allow

resources and finance to be arranged as well as time in the field to be organised and slotted into other Army tasks.

Therefore if an unforeseen severe weather system such as rogue snow or continual heavy rain transpires, many months of planning can be disrupted or delayed until resources cannot be used. Resources may have to be moved or abandoned. This scenario can end up costing a lot of money, which could have been spent on the core requirement of training soldiers to be effective War Fighters.

This issue is even more important with the Territorial Forces (TF) who have a very limited training time available compared to the Regular Forces (RF), but are can be asked to deploy on RF tasks and missions.

As a consequence, Territorial Forces do not have the same access to the same digital training resources due to their civilian work commitments that the RF has. Digital technology allows there to be a process in place that let the TF to get the required training time needed plus access to RF digital training resources even if it is after traditional working hours. The use of digital training could be the best way for the TF to keep their skills up to required operational standards.

With the possible advent of tri-service use of digital training, training events could have a usable back up which could be employed 24 hours a day no matter the weather type. Digital training methods have the potential to be available around the clock to soldiers and commanders, such as the Multiple Integrated Laser Engagement System (MILES) (Laser tag for adults). These systems can be used on short notice to train soldiers on most aspects of war fighting. They are adaptable and flexible enough to let commanders refine them to achieve set training agendas[100].

---

[100] Campbell, C. H. and R. C. Campbell (2006). Approaches to Managing Future Training, **Page** 52.

If the exercise was going to use more than one unit or use units which aren't based near each other physically, the ability to bridge that gap with digital means is possible and the combined training could go ahead. This is possible with the digital training networks that can be set up either short term or long term even to the extent that they become a permanent fixture. As the American and Australian example showed, these networks can be extended to include intra service training assets in a wider area network. This would lead to digital training assets from different services being able to work together in a combined training event.

With the availability of digital training methods short notice deployments can have the opportunity to refine tactics and techniques needed before being shipped out, such as "shoot-don't-shoot" refresher training, for peacekeeping operations or terrain over flights, for search and rescue planners.

In the final chapter of this research a closer look will be taken at simulations and simulation technology. This chapter will look at the issues associated with using simulation technology, from both a psychological and technological approach.

Chapter Eight
The Use of Simulation Technologies for Training

To understand where simulation technology is going, there needs to be an understanding of where it came from. This will help to show the underlying trends and patterns present in simulation technology. So a brief history of simulation is given here.

Military forces have used simulation technology since the development of the moving picture. The first military simulator was designed to teach pilots how to fly during the 1930's[101]. It was a very basic set up with the simple flight controls and a simple display. This was first shown at the Chicago World's Fair in 1933 to help recruit people into the newly formed United States Army Air Force. The initial results were mixed as people were not used to the moving pictures approach and many people suffered from motion sickness.

In the late 1970's a small electronic device would forever change the way military simulators be used. The first personal computer was developed and sold to the general public. It had a very basic monochrome screen and limited processing power. But this led to the introduction of the first commercially available video games, such as "Pong" and then to "Space Invaders", but the United States Army was investigating a small program called "Battle-Zone". This program recreated a very basic wire frame 3 dimensional (3D) environment in which a person could control a basic wire frame tank and engage similar enemy tanks. The US Army decided to develop a control

---

101 Link Trainer, From Wikipedia, http://en.wikipedia.org/wiki/Link_Trainer Reviewed on 9/08/06

interface which would allow tank drivers to use the controls that were present in the tanks of the time and fight against basic 3D enemies.

During the late 80's and early 90's the development of simulator technology was left to the US Army who produced some video games, with emerging developers which went on to commercial success, such as "M1 Tank Platoon" and "LHX". Both were commercially distributed through the Microprose label.

The technology was put to the test during the Persian Gulf War of 1990-91 where simulators planned out missions and pilots could fly rough facsimiles of the terrain that they would encounter. Tank commanders could put their troops through *procedural simulations* where the tank would respond as if a live round was fired. Loading and firing times were reduced due to the use of the simulators. The Gulf War was the first war that people referred to it as the "Video Game War". This came about due to the precision guided munitions that sent back video footage which made it look like a video game, and the M1 Abram tank controls which looked like a games controller[102].

During the late 1990's the US Army was reducing its operating capital. Defence budgets were being cut to make way for the "peace dividend" and simulation technology was being toned down due to the increasing costs of keeping up with the latest technology. During this time the gaming industry started to take off at an incredible rate. The introduction of consoles like the "Sega Saturn", "Play Station One", and the "Nintendo 64" had created an industry from scratch that would start to out strip the entertainment industry within seven years for revenue produced. Due to this phenomenal growth, the defence industry saw an opportunity to get the latest simulation software at a reduced price and without the large research and development cost associated with internal development[103].

---

[102] Prensky, M. (2001). "True Believers: Digital Game Based Learning in the Military". Digital Game Based Learning. **Page** 6.
[103] Institute for Creative Technologies http://www.ict.usc.edu/ Reviewed on 30/05/06

The American armed forces started to allow access to military hardware and people for games developers in return for a slightly modified game system to be used in training by the armed forces[104].

One of the most successful games to come out of this agreement was the title called Full Spectrum Warrior (FSW). This game came out of the United States Army's own development of a constructed environment simulator called Full Spectrum Commander (FSC) which trained commanders in the use of battle command software. FSW was a squad based; third person perspective (you see your character in front of you instead of first person where you see through your characters eyes). This game teaches squad Non Commissioned Officers (NCO) and their troops correct techniques for engaging and suppressing enemy troops and correct tactics for urban operations. The game is a teaching platform where techniques can be demonstrated and results shown without risking troops in the process.

The commercially available game has had some components disabled to make it more player friendly, but with an unlock code the military functionality becomes available. This product has been picked up by some NATO (North Atlantic Treaty Organization) countries to teach urban tactic and American doctrine and techniques to it troops. The Swedish armed forces found that its troops were remembering scenarios that were shown in the game and applying them to the live training exercises[105].

With the gaming industry investing large amounts of money and resources into newer technology and markets, the United States Army decided to invest in new tools to help recruit new members. The medium that they decided on was the video game, to entice the computer orientated and technologically aware people. The game, which was designed internally, was called

---

[104] Prensky, M. (2004). "The Seven Games of Highly Effective People." Microsoft Games for Windows, 2005. Reviewed on 4/06/06

[105] Boyd, C. (2005). "US army cuts teeth on video game". BBC News.com. London. Retrieved 27/01/06

"Americas Army"[106]. This product was available online or from a local recruiter. It demonstrated the basic boot camp that a soldier goes through to be a trained infantryman. It also picked up on the online multiplayer environment by having the ability to play against others in a team versus team game. This had the benefit of propagating the software to others and getting it distributed quickly.

The US Army, at little cost to themselves hosted the online servers, the data that was recovered by them led to developments, which helped to produce better versions of the game.

In the beginning of this campaign the product was only available to the Personal Computer (PC) community due to the fact that the army was using it on their PC's for soldier training. But with the introduction of home entertainment consoles such as the "Microsoft Xbox" and the "Play Station 2", a new Market was opened up to the recruiters. A new version of the Americas army product was developed, called "Americas Army: Rise of a Soldier". This was a commercially available product which took the participant through basic boot camp, with rifle and other weapons' training. They had to become proficient with the sighting systems used by the army before they could progress to other military occupation speciality (MOS), such as the Special Forces career paths.

The army found that the people who were coming into basic training who had had the exposure to the "Americas Army" software were quicker and more accurate in the initial rifle training. The conditioning and responses they had developed from the game exposure helped to minimise the retrain time needed in a live fire environment[107].

---

[106] Americas Army, Frequently Asked Questions, http://www.americasarmy.com/intel/ Reviewed 15/07/07

[107] Prensky, M. (2003). Has "Growing Up Digital" and Extensive Video Game Playing Affected Younger Military Personnel's Skill Sets?" . **Page** 4

Other software packages have been adapted to suit individual armed forces needs. New Zealand is no exception. The NZ Army has invested in modifying the program "Operation Flashpoint" which is a first person shooter, which has had the New Zealand weapons integrated into the scenarios making them more relevant to the training. The traditional M-16 rifle was replaced by the New Zealand Steyr rifle to make it more relevant to the troops who are using it[108].

From this knowledge of the history of simulation technology and its influences and effects on progressive developments, a solid framework can be set, to show how this technology can be used for the introduction of the NCW concept and digital training but also the potential consequences.

The major question that is posed by most international research in simulation technology is "What is needed to make a simulation militarily relevant?" First and foremost is ***context***[109], which means that the information that is being simulated is relevant to the training which is required. There is no reason in having a virtual simulation which is showing a battlefield that will never be encountered, such as downtown New York, which is an urban operation but the context is incorrect. The context must be relevant to the service personnel who are using it.

Different context must be catered for when designing and implementing simulation equipment software for the New Zealand defence environment. The ability for Regular Forces (RF) and Territorial Forces (TF) to work with the same simulation software is important, as the defence budget appears to be unable to cover two different simulation systems. But the same systems must be able to cater for the Special Forces group who have a different context to the RF and TF troops. Context is helped by the other elements of a successful military simulator[110].

---

[108] Demonstrated at the seventh form orientation event at Massey University in October 2003.
[109] Page, E. H. (1998). Introduction to Military Training Simulation: A Guide for Discrete Event Simulationists.. **Page** 3
[110] Ibid.

Fidelity: Fidelity is the ability to represent a realistic form of information, which is not at odds with the solders internal reasoning skills. This element is a primary source of context; it is the visual representation of the information. It is the aspect, which allows a soldier to absorb the training information and be able to apply it at a later date. It is an acceptable form of realism to which the soldier is accustomed and would not subconsciously fight. As an example of incorrect fidelity, if a soldier knows that if they shoot accurately at a target, that target will go down as it is a logical sequence, which is backed up by reason. But if the simulations fidelity is wrong and the target does not respond as predicted then the fidelity is broken the learning will cease and a resistance to that training method would ensue.

Presence / Immersion: This element is based around the simulation user, in the military's case the soldier in the simulation. The soldier must feel they are part of the whole process and has an impact or can make a difference to the simulation. The simulation must draw its participants into the realm that it is trying to portray without breaking the fidelity that it has set up. The weapons that are used in a rifle range simulation must feel and act like the real world counterpart, the weight and reaction must fit the real world processes. If this core element is not implemented then the soldier will not take on board the designated lessons. This would set back the complete process and minimise the potential benefits the system could offer, the sound and texture of the environment must also help to draw the soldier into the simulated world. With the digital rifle range example, the need for the targets to reflect what would be seen in the real world becomes more critical for cross training. Being able to take the lessons and skills out of the digital simulation and onto a real rifle range or field exercise is the goal of all simulations.

Buy-In: The final element to a successful simulation. This is the ability for the soldier to "buy-in" to the simulation. The simulation must be able to fool the human senses into believing that they are real events playing out in front of the soldier participant. The surrounding visual and auditory elements of a simulator must work in conjunction with the total approach. With the rifle range

example, the use of sandbags and other materials that are found on a real range would add to the complete experience.

Sound plays an important role in the acceptance of the virtual reality simulation. The sound must match up to the real world equivalence. On the rifle range the sound a shot makes must be replicated to best simulate the real world. The recoil must be the same as well to reinforce correct practice and techniques. Many new simulation ranges such as the EST 2000 system provide a total emersion experience. Due to the presence of gas powered recoil mechanics in the weapon systems, the soldier gets the true feel of how the weapon will react. But also with the integrate technology inside the weapon systems the instructor can induce scenarios such as the weapon system jamming or failing.

Using the New Zealand environment as an example, the possibility of "buy in" can be increased by setting the simulations on the rifle range to reflect the local real life range. This can be achieved by using digital photos of the surrounding real world range and incorporating them into the simulation. This would provide the soldier with visual feedback, which would help with the crossover needed to go from the simulation to the real world. The soldier would get the experience of seeing the targets, as they would appear in the real world equivalent.

Both USARI and DSTO research[111] show that the instructors would play a crucial role in the immersion and "buy in". Correct rifle range procedures and techniques should also be used in the virtual simulation for the process to work. The need to train as the soldier will fight is still relevant in the virtual world. Soldiers need to understand that the behaviour learnt in the simulations is just as important as it is in the real world. If this illusion is shattered the soldier will only see the simulation as a video game and the wrong messages will get reinforced. This could lead to fatal results in real world situations.

---

[111] Warne, L., I. Ali, et al. (2004). The Network Centric Warrior: The Human Dimension of Network Centric Warfare. **Page** 108.

These four key points are also used by commercial video game developers; many modern video games are trying to replicate the combat environment for the entertainment market. These games use all of the psychological indicators that are needed to immerse the player into believing that they are in the simulated battle. Military simulators are trying to achieve the same thing, but the difference between commercial and military simulations is very important, from both a technological and psychological standpoint.

Commercial games are designed to be of entertainment value, giving the player a challenge while not actually putting the player in any real danger. The player has a vested interest in how his *avatar* (Digital representation of a person in a cyber environment) or character progresses through the game to reach the end and finish the game. Many of these games give the player multiple lives, save points and no real punishment if they kill innocent bystanders such as civilians. Modern games give the player the chance to experience situations and events which they would usually not attempt or try[112].

Many of the best seller's provide the ability to handle weapons in a Rambo style, the so-called "point-and-shoot" approach or the "spray-and-pray" mentality. There is a psychological cost associated with these types of games as only the destructive nature is rewarded, the more you kill the better your score or the more you can brag to other players in the same game. As explained before, Multi player games are increasing in popularity due to the competitive nature of user versus user game play.

The techniques that are used in many commercial video games would not be out of place in a modern battlefield. Pincer movements, fire and manoeuvre and suppressing fire can be found in many modern games including the use of certain types of shots from weapon systems. Most video game players believe that the best shot to get is a headshot, as it will kill their opponent in

---

[112] Gee, J. P. (2003). What Video Games Have to Teach Us About Learning and Literacy. . **Page** 28

one move, compared to body shots which disable people or incapacitate them. More points are given to a player who has a better kill ratio and hit count. The ability to kill is reduced to who can hit the best with the least amount of wasted ammunition. No thought is given to the consequences of their actions or restraint to techniques or methods used to win. Only that they will be rewarded with more points the more they kill[113].

Military simulations are also there to give soldiers skills. The competitive drive can be instilled in them with challenges against other units and team members. This competitive aspect fosters team cohesion, which is critical for the battlefield environment. Without this cohesion soldiers would not work as a team and could risk their own lives and the lives of others in their unit. According to USARI research, the military simulator is trying to get the body to remember certain actions that should become second nature, or what is referred to as "muscle memory". This is the ability for a soldier to react quickly and correctly to a situation without the need for conscious thought, as quick reactions can mean the difference between life and death on the battlefield.

Therefore a soldier must also learn restraint because the ability to open fire and hope that the soldier hits something is not longer applicable. With more and more operations moving into urban environments and the ability for an action to be displayed, in high definition all over the world in a matter of minutes, the need for control is becoming more important. This is where simulations start to become of more use.

Modern military combat simulations are now equipped with a "Shoot- don't-shoot" scenario to teach soldiers when it is acceptable to open fire and when restraint should be shown. These digital scenarios have digital actors who can act as an enemy force or as civilians mixed up in the presence of the enemy

---

[113] Orvis, K. A. and K. L. Orvis (2005). The Influence of Trainee Gaming Experience and Computer Self-Efficacy on Learner Outcomes of Videogame-Based Learning Environments. **Page** 43.

forces. This provides a situation, which cannot be replicated with such ease in a live fire exercise[114].

Military simulations also have Rules Of Engagement and Laws of Armed Conflict built into them so that soldiers can get use to acting within the legal framework. Military simulations can provide instant feedback to the user to help reinforce correct behaviour. This is done to remove unwanted traits before they become ingrained into the soldier's memory and reflex. Military simulators can be adjusted to accommodate all aspects of the spectrum of warfare. They are not like commercial games where the task is to win to progress.

Military Simulations act on real world logic. If a soldier is hit with a shot that would kill him in real life then that soldier is taken out of the scenario. There are no extra lives on the battlefield, medical packs will not instantly heal all of the wounds, and a stray bullet will have an effect. Military simulations try and teach that all actions will have a consequence and the soldier must be able to handle the situations provided.

Military simulations are also more flexible than their commercially available counterparts. The military can add scenarios to the simulations as the need arises or as new threats become more prevalent. Commercial games don't have that ability unless the manufacturer provides an add-on pack or a new version of the game.

As the military experiences new tactics or techniques from the enemy combatants they can be integrated into training scenarios to let the next rotation of soldiers be able to cope with the new methods. This has been shown with the United States Army and its Improvised Explosive Devices (I.E.D) trainer for the infantry[115]. The lessons that have been learnt in both Iraq and Afghanistan have been integrated into the latest rendition of the

---

[114] Ibid.

[115] Army News Service, July 26, 2005, http://www.globalsecurity.org/military/library/news/2005/07/mil-050726-arnews01.htm Reviewed on 7/08/06

simulation. As more After Action Reports/Reviews (AAR) are filed, more changes are implemented to keep the trainer's knowledge current with the operational progress. From these situations, new techniques and modifications to procedures have been created due to the experience gained through the simulations[116].

As a recommendation from this research, New Zealand needs to ensure that its simulations and digital training devices have the ability to adapt to new situations and scenarios. Digital technology can give that freedom but the infrastructure must be in place to do it.

With the current rate of technological development and high-speed communications becoming more available, the New Zealand forces may need to make sure that they stay up with the current trends in international military development. Digital technology in the New Zealand public and private sector is taking on a new phase with the unbundling of the local loop network, and higher speeds of digital broadband coming online[117]. This may have provided the best time for the New Zealand forces to set up a dedicated digital training network. The possibility of using technology such as Voice over Internet Protocol (VoIP) or internet telephone to link all of the forces training assets into one unified approach over one digital network instead of two that has one for data and one for communications.

Most international research in NCW suggests that the investment in new broadband technology could open the way up for distance learning and combined unit training. Simulations technology could be designed to work together over large distances as if they were located at the same complex. Both Wide Area Networks (WAN) and Local Area Networks (LAN), could interact with each other meaning troops on deployment could interact with their home units and be kept up to required standards on courses, and unit

---

[116] Trinquand, B. D. (2004). "Lessons learnt from Multinational Operations". Future Armies, Future Challenges: Land warfare in the Information age: **Pages** 282.
[117] Government moves fast to improve broadband, speech by the honourable David Cunliffe. http://www.beehive.govt.nz/ViewDocument.aspx?DocumentID=25636 June 2006

progressions. Online courses could become available to deployed soldiers to help keep them in line with promotional requirements instead of waiting to attend a local promotional course at the end of an operational tour.

The JCCS may provide the catalyst to start an effective digital update program within the NZDF. The digital hardware will need to be provided if the system is going to reach its full potential. Data streams must be able to get to and from the system in a reasonable timeframe to be of any operational use to troops both deployed and in training. This issue is not only relevant to New Zealand due to its geographic isolation, but to any force that is investing in the transition to the NCW concept and the benefits of simulation and digital training. Both the United States and Britain are investing in technology that will expand their bandwidth size and speed within their current physical infrastructure.

With the introduction of new digital training methods and techniques a unified approach is needed so that all the simulations can work together to provide the best training environment for the soldiers involved. Lessons from the experiences from the other members of the ABCA can be applied to the current situation within the NZDF.

For example, a decision will be needed by each individual service, to determine if each base will have its own independent digital training system or if there will be a service wide digital training system where all bases are interlinked. If this first approach (Individual base networks) is taken then the need for the information and statistics for each individual soldier to be available to all of the command staff and personnel departments service wide, has to be considered.

From the United States Army's experience, Information on what skills and training is needed should be made available easily so that the individual soldiers can get access to information and resources that will help in their career development. Also the NCOs need to be able to see which one of their

soldiers needs more attention on certain skill sets and how that help can be given.

As another example derived from the experiences of the ABCA, a unified training system could be designed and managed to provide a storage point for soldier's information which will help in the design and implementation of correct training solutions for individual soldiers. This database could be accessible by both NCOs and unit commanders who could see what skills shortages there were in their units and how or when an opportunity to rectify the situation became available. This same database could also be used by individual soldiers to see what skill sets they have and when an appropriate promotion course (either online or in class) is available to them. It could act as an informal promotional checklist to help guide soldiers and give them more control over their personal direction within the Army's needs and direction.

This digital training network would also be the repository of a digital library, which could be access to help soldiers with issues or problems with weapon, or information systems, a location with both manuals and Defence Force Orders[118]. Access to restricted material could be secured against malicious attack using modern information security techniques.

This program could also help in the joint approach that the New Zealand Defence Force is taking. The training network could host all of the services tactics, techniques and procedures (TTP) information giving officers and NCO's the ability to see how the other services work, thus giving them a more joint view. This also works in reverse with the other services seeing what the Army can do in a training context. This would not replace the current intranet but be a learning extension.

Currently the New Zealand Army is in the process of implementing a data network between its army bases to help with large unit and formation training.

---

[118] Lorenzo, G. (2002). "eArmyU and the Future of Distance Education." The Technology Source, 2005. www.thetechnologysource.com Reviewed on 15/4/06

This network will help with the implementation of the new Weapons Training System (WTS). This system is the New Zealand equivalent of the United States training system the EST 2000. This system helps to train and familiarise soldiers with the correct use and methods of weapon systems, before they are put out to a live fire environment. This system has force feedback through the selected weapon which can simulate the recoil that is provided by a live weapon. But with the system being digital, there is the ability to mould the training solution to the needs of the individual soldier. Elements such as the location of fired rounds on a target or the pressure applied to the weapon as it is pulled into the correct firing position can be analysed and recorded to help in the training.

The New Zealand Army has found that more of its recruits are coming from urban environments. These recruits have had little or no exposure to firearms. There has been more need to have new personnel work with firearms to get them up to an acceptable level.

The networked WTS system will give the trainers and managers the ability to create and manage training scenarios and provide them to all of the training centres so that there is a unified training method being employed across the whole service. But this system is dependent on the implementation of the data network backbone and supporting infrastructure. With this in place the online learning environment can take shape and develop.

The United States and British forces have already started a deployment of this type of concept. Their online knowledge centres are accessible by the soldiers all around the world[119]. The best example of this anywhere is the United Stated Army's Army Knowledge Online (AKO) program and its digital library system with all of their field manuals and pamphlets available for down load and printing[120].

---

[119] EArmyU, Frequently Asked Questions, http://www.earmyu.com/Public/public_resources_faqs.asp Reviewed 3/04/06

[120] Prensky, M. (2001). Digital Game Based Learning.. Chapter 10

These developments are all based on one major issue, the use of a single data architecture. As it has been stated before, both the Australian forces and the United States forces have combined to create a global digital training network between their respective combat centres. This would not have been possible if they had not discussed simulation architecture first. Both of these countries are transitioning to IPv6 protocols for their defence networks, but they are also introducing common simulation architecture to their systems.

This system is known as High Level Architecture or HLA. The Australians are transitioning from their current simulation standard, Distributed Interactive System (DIS) to the new HLA standard. From the available research a clear point has emerged, New Zealand needs to decide which standard it wants for its simulation system if it wants an integrated simulation network.

With this, New Zealand is in the good position of being able to decide which simulation format it wants to follow. Currently there are two main types in use by New Zealand's coalition allies, the standard DIS system and the newly introduced HLA system. According to ABCA research, both of these data architectures have their advantages and disadvantages.

The new FBCB2 embedded training system that is being introduced into general service with the United States forces uses the new HLA standard. This allows the Battlefield Operating System (BOS)[121] to interact and act like a single active system the "System of Systems" approach, with real world outputs but in a simulated controlled environment. The hardware is the same as the items used in the real world counterparts but the data being fed into the system is simulated. The hardware has the ability to adapt between simulated information (training) and live information (real world).

---

[121] There are seven Battlefield Operating Systems. The BOS provide the Army a common taxonomy of critical tactical activities. They provide the commander and staff a means of assessing the planning, preparation, and execution of an operation in discrete subsets. The Battlefield Operating Systems

Manoeuvre, Command and Control, Intelligence, Fire Support, Air Defence, Mobility, Counter-mobility, Survivability, Combat service support

From *Field Manual 3-90, Tactics.*

Scenarios can be feed into the system such as FBCB2, so that it will act as if it is under real world conditions while new users train on it. This simulated data can be fed to the other system to make them respond as if they are in a real world scenario and their users get the training experience as well.

This ability only comes about due to the common data architecture that has been introduced. There are still issues trying to integrate legacy systems, which have not been designed to use or understand, the new HLA[122]. These are usually old legacy devices, such as tape drives, or early generation Inter vehicle information systems. DARPA research and experimentation has shown that translation programs can be used to change the data from one form to another, HLA to DIS, DIS to HLA but this can add a large time factor. Information can be lost or translated incorrectly in the initial setup of the transition servers.

This is where New Zealand could have an advantage. Its introduction of new systems service wide gives the opportunity for a common programming architecture to be introduced across the services so that a more joint integration can be achieved. Deciding which of the architecture types to adapt is paramount.

With HLA each simulation or system is called a "federate", and a group of federates is called a federation. A federate has its own Simulation Object Model (SOM). This is a list of the objects that it can accept from other systems and what it can produce for other systems. For example a LAV will have an onboard training simulation system that can be linked to other systems. The system will have the ability to receive and send out information about itself; such as where it is located, where it is going, and when it fires and what it fires. This data is then sent out to units that can use or accept that data type, such as other LAVs.

---

[122] Ping, I. C. K. (2000). HLA performance measurement. **Page** 91.

For example, each LAV is a federate but combined together they are a federation and the information exchanged is formatted to the standard set by the SOM. Now each federation has a Federation Object Model (FOM), which is a combination of all of the SOMs. When multiple federations join together they will know what type of data each one can produce or receive.

This method is being accepted globally as the new standard over the more traditional Distributed Interactive System (DIS), which was created in the early 1990's. The DIS system has some advantages over the more modern HLA system which was created in the late 1990's. In the DIS system the data is formatted to a universal standard where as the HLA system is decided on by the participants. The DIS has all of the data values set across the board. Data value fields such as system type, location and weapon systems in use are presented and transmitted in full. Even if the data isn't changed it is sent across the network. This process was acceptable when the systems were not very complex and the data wasn't detailed to such a complex level[123].

But the DIS system is currently experiencing a data crush[124]. With the data levels increasing, the amount of bandwidth needed to send all of the data values even if the data value hasn't changed, is getting beyond the capacity of most systems or is causing a data delay to the simulation. The HLA system only sends the data that has changed to the other simulation systems on the network. This frees up the bandwidth to allow better communication between the systems and produces clearer simulations. Data can be sent in more frequent packages due to the free bandwidth. This can increase the refresh rate of the simulation and give the user the ability to react quickly to changing circumstances. This ability also allows the opposition force to introduce new elements to the scenario without the risk of the new data and elements stalling the simulation system[125].

---

[123] Defense Simulation and Modelling Office (1995). Modelling and Simulation (M&S) Master Plan.,. www.dsmo.mil Reviewed 15/05/06

[124] Where the data being sent is greater than the available bandwidth, forcing a system slow down

[125] Page, E. H. (1998). Introduction to Military Training Simulation: A Guide for Discrete Event Simulationists. 1998 Winter Simulation Conference, Washington, DC, the MITRE Corporation.

The smaller data packages that come with the HLA system allows the simulations to be located over a larger area. This ability allows international simulation co-operation to take place without putting much stress on the national bandwidth network. The systems have the ability to exchange information over long distances without a loss in simulation fidelity. The ability for soldiers to work in a coalition environment without the need for expensive field exercises or transporting personnel and equipment to foreign locations will offset the initial expenses in establishing the network.

With the simulation system having a flexible architecture to it the ability to introduce other agencies to the network could be made easier with a complete and accurate defence simulation policy. Under the New Zealand Defence Force Statement of Intent 2006, one of the Key Points that was discussed was:[126]

"Developing a Defence Simulation Policy, Architecture and Analysis Tools to inform NZDF's future capability."[127]

This need for clearer policies on simulation systems is becoming more crucial as the three services start to take advantage of the benefits that simulation systems can provide. Each of the services is starting to introduce simulation systems into their core training rotations. This could provide the best time to bring in a unified standard for the NZDF. This unification could provide a cost saving benefit to all of the services. If a single architecture is introduced to the NZDF simulation environment then the possibilities of having a true joint training environment will start to come to pass. This could be through the establishment of a joint simulation centre for the three services where a unified terrain database could be set up so that all simulations draw from a single location for easy updating and use. This would follow the United States

---

[126] New Zealand Defence Force (2006.). New Zealand Defence Force: Statement of Intent. **Page** 21.
[127] Ibid.

example in their establishment of the Defense Modelling and simulation Office (DMSO)

The single joint simulation centre could focus the concepts and paths, needed by the services and provide a centralised location for overlaps in service needs. As was mentioned earlier, and as an example, a single terrain database could help the joint environment by storing and maintaining an up to date repository of terrain information. This allows soldiers trained in simulation environments to be able to transition between services and not have to learn a new approach and methods. The result would be a speeding up of the training sector and provide inbuilt interoperability between the services.

Currently the three services of the NZDF are in initial discussions on the development of a unified data architecture, for both NCW and the training support simulations, with establish developments being introduced during 2007 and 2008.[128]

With the possibility of digital training methods being used to train service personnel for the NCW environment, there needs to be an understanding of what simulations can realistically provide to the NZ Army and other services. A commonly accepted view from the members of the ABCA is that, the tangible training benefits must help the soldier and service personnel, who will be using and relying on IT Systems in combat operations to achieve greater results than current training methods. It is their lives and the lives of the soldiers and service people around them that are on the line with these systems. If they aren't trained to use them effectively and to apply the benefits an NCW environment provides, then the cost will be high, both in the loss of life and the misspent financial capital[129].

As an example, the WTS system is designed to help soldiers enhance their shooting capability, and refine shooting methods on a digital firing range. But

---

[128] Ibid.
[129] Archer, R. and Warwick, W. (2003). Training Future Force Leaders to Make Decisions Using Digital Information, **Page** 51.

if the soldier is only using the range to get proficient or to reach the minimum standard then the enhanced benefits that the system provides is being wasted, as well as training the soldier to their full potential.

Simulation systems and digital training methods can be a benefit to the services. The following point from the research literature, will demonstrate how this is possible.

First and foremost is the ability of simulators to provide a safe training environment for soldiers. There are high levels of control and safety built into the simulation systems so that soldiers do not have to worry as much about their own personal safety. There are some small risks with any system but these can be minimised with correct procedures and methods in place. For example the WTS system has high-powered lasers in use to trigger the system. These can lead to blindness if directed to uncovered eyes due to the strength of the system. But it is about common sense practices to stop this type of accident[130].Such as using the same methods employed on a live fire rifle range.

Also in a simulation environment, soldier's responses to certain stimuli can be monitored for deviation or issues before they become a problem out in the field. This has been used to monitor soldiers for when they are in a "shoot-don't-shoot" situation, where a minor number of people have the psychological persuasion to become overly aggressive and uncontrollable. In David Grossman's book "On Killing"[131] he discovered that a 2% minority of people have a psychological disorder to accelerated aggression in combat environments. These people also display anti-social behaviour when in combat. They can put their unit and civilian lives at risk.

But the reverse has also been found to be true. Soldiers, who cannot or will not pull the trigger in a combat environment and to a lesser extent, purposely

---

[130] Moses, F. L. (2005). Training Challenges for Digitization. **Page** 34.
[131] Grossman, C. D. (1998). On KIlling, Penquin.

aim off and miss target have been found to have a psychological disposition to not killing. These soldiers become a risk to their units and can have a devastating effect on morale within the unit. This division can rip a cohesive group apart. Simulation training can help find these people before they become a factor in missions and combat groups.

With the changing nature of warfare the asymmetrical warfare approach has provided the psychological situation of unnatural killing - the killing of children and women. This situation provides both an ethical and moral dilemma for soldiers when out in a combat environment. The basic human male instinct derived from millennia of human evolution, is to protect young lives and females from harm due to procreation needs and survival instinct. But the asymmetrical nature of current warfare methods has put these elements into combat situations[132], either as combatants or as fellow soldiers.

As an example, soldiers have had to face children coming up to them with hand grenades and other Improvised Explosive Devices (IED). The issue then becomes, do the soldiers engage the target to protect themselves and their unit, at the cost of their morals and ethics, or lose their lives through the attack. Woman combatants also provide issues to this dilemma, as most combat soldiers would take issue at having to open fire on women in combat. A variant on these themes has been the use of women and children as human shields for armed insurgents to hide behind. The soldiers are then faced with the dilemma of shooting into the crowd or being shot at themselves by the forces in the crowd. But with the choice comes the possibility of the images being used against the forces to provide propaganda for the enemy forces.

These issues can be faced by the use of shoot don't shoot scenarios in a simulated environment. Or the use of images of the aggressors used as targets to try and minimise the impact of unfamiliar opponents on soldiers. But as will be discussed in the section that follows, the possibility of desensitising

---

[132] Ibid.

soldiers to fire at target without moral and ethical consideration can become an issue when using simulation systems.

Another benefit of using digital training and simulation is in the treatment of Post Traumatic Stress Disorder (PTSD) in combat soldiers. Currently the United States Armed forces are developing a method of recreating a traumatic event experience by a soldier in virtual reality. This traumatic event is then played out so that the soldier can experience the sights and sounds of the conflict, so that the soldier can work through the associated stresses with a psychologist or councillor who is with them in the VR experience.

As has been discussed before, simulation systems can provide the ability for trainers and instructors to change training scenarios quickly and to be able to modify the learning objectives as operational lessons come to light. The rapid ability to change and adapt to the fluid combat environment helps to provide troops who can adapt rapidly and take up lessons quickly which could save lives. Lessons that have been learnt by other military forces can be adapted by local forces to provided access to larger training and learning objectives. Close allies can move, change or modify lessons from allied partners to help with joint and coalition training. The ability for a foreign unit or formation to work effectively and efficiently with the NZDF helps to provide a more effective combat force for joint forces and coalition commanders.

Network Centric Warfare provides the tools for commanders to interact and control larger forces than could be available locally to them. NCW simulation systems can give the prospective commander the needed experience and exposure to the high intensity environment that comes with a multi nation or coalition arena. This means that soldiers and commanders will not be forced to adapt quickly to new methods or procedures or be replaced. Commanders can develop the needed skills to adapt and manage the high intensity environment before it becomes mission critical. Stress management, strategies and methods can be introduced gradually or as needed in a simulated environment. Soldiers will learn on the system they will use instead of on systems that will not be relevant to a soldiers or commanders job. The

closer to reality that a simulation can get the more benefit it will provide to the soldier or commander.

Another identified benefit of a digital simulation system, is the ability to introduce errors and mistakes in a controlled way. The human factor in any digital system can provide errors and issues to the system and the results can be disastrous to a combat unit or supply element. Soldiers and commanders need to experience and work through errors so that their troubleshooting skills get developed.

As an example the Australian Defence Force deployed to Iraq had the experience of a supply element inputting the wrong data into the digital supply system. The results were that a combat element was issued 10 rounds of ammunition instead of the 100 that were ordered. The soldiers had faith in the system, but the data was not put in correctly, so the result was not correct. The Information Assurance (IA) was not there. This was a lapse on the user's side of the system. This is why the digital simulation system can provide the opportunity to let soldiers make the mistakes and learn the lessons from them without the risk to operational success. They can also be exposed to the mistakes that others have made so that they can learn from them[133].

With digital simulation technology, new concepts can be introduced faster. New methods, techniques or tactics can be implemented into the training system, so that the next rotation can be as up-to-date on the new methods as possible. If a new weapon system is introduced or a current system is removed then the scenarios and training events can be updated or modified instead of the need to write or develop all the information again. If a working concept has been accepted from a foreign force, for example, the use of the Stryker brigades concept into the New Zealand Army, their methods can be adapted to our own. This is due to the fact that the Stryker brigades use digital

---

[133] Graves, C. R., D. M. Pratt, et al. (1999). Force XXI Training Program-Digital Project: Report on Development and Lessons Learned, **Page** 124.

training methods[134] which can be sent to the Army's training establishments for integration in to current methods. This process also works in reverse. If a foreign nation wants to accept our methods of training, development or digital learning then the NZ Army's training provider will send them out the relevant data files for them to use in their systems. This efficient data exchange is what is provided with correct digital architecture and set-up.

This provides the ability to have a unified training standard between allied countries while allowing nations to develop individual identities with in these methods. Interoperability can be enhanced by standardisation between forces allowing the services culture to adapt to the global environment. Unified digital training standard allows forces to interact and interchange troops, units and formations without much disruption.

An integrated, flexible simulation network will provide an enhanced training environment for current and future soldiers, and can work in conjunction with a modern command and control system. This allows soldiers to work on systems and processes which will be an accurate representation of live real world systems[135].

With every positive gain by the use of a simulation and simulation network there have been identified negatives and draw backs to their use. It must be remembered that a simulation system is only a tool for the trainers and instructors. As with any tool the opportunities to abuse it and misuse it are always present[136]. If it is not managed and focused to the training needs, then all of its benefits become redundant, as the negative aspects will offset them[137].

---

[134] Dressel, D. J. and B. B. Schaab (2005). Training Requirements of Digital System Operators in a Stryker Brigade Combat Team, **Page** 37.
[135] Roland, R. (1998). Panel: The Futue of Military Simulation. Proceedings from the Winter Simulation Conference, Monterey, CA, Rolands & Associates Corporation.
[136] Wesensten, N. J. and Belenky, G. (2005). "Cognitive Readiness in Network-Centric Operations." : **Page** 12.
[137] Zipperer, E., G. Klein, et al. (2003). Training and Training Technology Issues for the Objective Force Warrior. **Page** 53.

With the positive aspect of being able to train soldiers how to think dynamically in stressful environments, the ability to corrupt correct thinking processes is a real risk that must be guarded against. If a scenario is repeated often without change or challenge, the possibility of thinking process becoming static and non-dynamic becomes a greater issue[138]. Live human factors in a battlefield can change the total dynamics quickly. This is made evident by the soldiers who risk their lives to do heroic acts to save their fellow soldiers; events such as one soldier taking out a machine gun nest alone have been recorded in many major battles. The simulation system, due to its use of statistical probability would not reflect this factor. It would misrepresent it as a perceived computer glitch, where one icon takes out a disproportionate amount of enemy icons due to miscalculation or user intervention. It is currently impossible to factor in and program for all of the possible events a soldier is capable of doing.

This leads onto another current issue with simulation technology, the ineffectiveness of current Artificial Intelligence (AI) enemies. This issue has an impact on the self-autonomous aspect of simulation training. In a NCW environment the opposition would be another human force, but for training either another human force must be provided to represent the opposition force or there is reliance on in-built AI. This AI is restrained by key programming factors and a set of rules it must follow. This does not allow for flexibility in its approaches to scenarios and situations, so the risk increases in the possibility of predictable outcomes. With the outcomes or tactics being predictable from a baseline AI the learning objectives start to lose their effectiveness.

Non-relevant content is also a negative aspect that can have a detrimental effect on using simulations and digital technology to train for a NCW environment. The context of a scenario and of the lesson elements, are critical to successful learning objectives. If the context is not set correctly then the soldiers will not take away the lessons needed. An example would be the use of foreign military units in a simulation to represent NZDF forces instead

---

[138] Sanders, W. R. (2001). Cognitive Psychology Principles for Digital Systems Training, **Page** 38.

of accurate representations. This can be done with the Janus simulation systems LAV units, which have simulated weapon systems available to its mounted crews which are unavailable to real LAV crews such as the Mk 19 grenade launcher. These discrepancies can affect the tactic and techniques employed by the soldiers in the simulation which could lead to an unrealistic view of NZ Army mounted LAV capabilities. But if these systems are going to be invested in, then a precursor learning experience could provide benefits later on in soldier development. But these rely on the early exposure and the right processes being invested in early.

With the global investment in NCW, relevant training technologies taking place and the need for coalition forces the possibility of having a standard pushed onto the NZDF by larger coalition forces could become a factor in the successful implementation of the NZDF's NCW approach and its training needs. International standards for HLA, which have been defined by the Institute of Electrical and Electronics Engineers (IEEE) community, could impact on the way that New Zealand develops its NCW strategy. This could affect the quality of simulations that the NZDF and the New Zealand Army could implement as well as the ability to recruit and retain people with the right skills to manage and maintain the simulations up to an international standard. There maybe a need for secondment from the Australian Defence Force (ADF) to help maintain skill levels until NZDF staff can be trained to take over. But the longer there is a delay in a simulation strategy for the NZDF the longer it will take to get the staff skill levels and numbers up to an effective level for the NCW training environment. The establishment of better relationships between Coalitions and Allies simulation services need to be established early, so that the staff can be exposed to up coming ideas and concepts sooner rather than later, before they are implemented.

With the NZDF starting to see the cost benefits of using simulations to train soldiers and service personnel, the NZDF must keep in mind a joint approach so that it can maintain its doctrinal approach and goals. Simulations cannot totally replace live exercises, joint or single service. Even though a joint headquarters can be simulated and replicated in a digital environment the

need is still there to be able to go out into a combat environment and put the skills to the test in a live combat exercise. Soldiers still need to fire live rounds on open training terrain and facilities. Live fire exercises with units supported by organic and attached assets need to take place. No simulation currently can replicate the blast wave effect on the human body from an artillery shellfire or from a battery of field artillery. These need to be experiences in a controlled live fire exercise, so that soldiers who then move back into a simulated environment know first hand the effects of organic and attached units. Instead of seeing them as a simulated replication on a screen, they can apply what they felt and experienced from the live fire exercise to that scenario making the context and fidelity more complete for the learning experience[139].

According to the US Army's behavioural and social sciences research, the ability to accurately replicate the screens needed for a NCW environment digitally; can lead to a rise of what psychologist call disassociation, the inability to distinguish between real and unreal[140]. This is the goal of many software and game developers but for a military environment the risk factor has higher consequences. With NCW units and soldiers are represented by icons on a screen. This disassociation between what is real and what is projected can lead to substantial ethical and moral conflicts or to a lesser extent the lack of these. The operant conditioning[141] provided by simulations which represent live firing conditions such as the Weapon Training System (WTS) can have a deep psychological impact on soldiers if it is not managed and controlled[142].

This situation has been represented by events where teenagers have gone onto shooting rampages after playing First Person Shooters (FPS) with high hits and kills in the correct target area, being the torso and head. These skills

---

[139] Paterson, R. (2005). "Capturing Live Combat in Network Centric Warfare". DARPATech 2005, Advanced Technology Office. www.darpa.mil Reviewed on 27/08/2006

[140] Sanchez, L. M. (2002). Violent Video games and Operant Conditionin **Page** 20.

[141] The stimulus-response conditioning process, exemplified by Pavlov and his dogs, the dogs drooled (Response) on the command of a bell ringing (Stimulus)

[142] Sanchez, L. M. (2002). Violent Video games and Operant Conditioning **Page** 20.

have been developed and maintained in a simulated environment without the moral and ethical constraints or considerations[143]. This being coupled with the need for higher scores and game progression through kill ratios and accuracy can provide the breeding ground for sociopath tendencies even after psychological screening for entrance to the military.

This pre-screening can stop the majority of people who have the inherent mental deficiency but with the combination of peer reinforcement coupled with the intensity provided by a high fidelity interactive simulation system the possibility of triggering anti social behaviour is present[144].

An accepted fact of combat is that a soldier is trained to take life if need be. But that is coupled with moral and ethical standards that have been explained and trained into the soldier's behaviour. Even Special Forces soldiers and units reinforce the correct use of weapons and hold fire situations.

The possibility of the Special Forces soldiers going in with "guns blazing" is diminished through the use of "shoot-don't-shoot" scenarios and live fire exercises in what is called "Kill Houses". Live participants are spread amongst cut out enemies to force the soldiers to think before shooting and to identify a target before engaging.

But with the use of simulations this inbuilt hesitation due to the presence of innocent lives is removed. According to behavioural research, a moral and ethical consideration needs to be in place with the use of virtual reality fire simulators, so that the correct psychological constraints can be implemented into the training sequence.

An uncontrolled simulation experience could create a soldier who will revert to shooting at any target approach, when stressed in a combat environment.

---

[143] Grossman, C. D. (1998). Psychological Effects of Combat, www.killology.com. Retrieved 30/06/2006

[144] Prensky, M. (2001). "The Games Generations: How Learners Have Changed". Digital Game Based Learning. Chapter 2.

This could be in the form of a friendly unit or civilians and this becomes especially important in urban operations where the intermixing of civilians with combatants can take place. Soldiers and instructors need to be aware of the possible warning signs that can be displayed by someone who is creating negative responses to simulation training. Quick and early identification is critical to successful management of possibly dangerous behaviour[145].

Soldiers in a simulation system will continuously get feedback from the system, in the form of sounds, lights or actions. The stimulus-response cycle is ongoing in a military simulation. It is there to teach soldiers how to react to a situation quickly and effectively with the ability to bypass a cognitive approach and engage the reflex skills directly. These stimuli reinforce the soldier's state of mind. The soldier will experience psychological arousal (either fear or pleasure) from the simulation. This will leave the soldier with the need to repeat, attain, or remove the same arousal instance from other situations unless self-correcting skills are built into the simulation training scenario[146].

These issues have been discovered and manipulated by most of the video game community and designers. These stimuli reinforce gamer's needs to attain better skills or to achieve higher states on a developer's game. Many gamers' loose track of vast amounts of time due to the immersion provided by a high fidelity game. The same could be done to the soldier in the simulation. "Bigger, brighter and better" is always the need for gamers. If the soldiers do not get the same reaction, a form of boredom could set in and training lessons could be lost[147].

With all advance technology the need to have the latest and greatest is always a concern for many people and nations. There is no difference for the NZDF. The ability to provide the best training environment for its soldiers is very important, and NCW is going to need to enhance this to a greater extent.

---

[145] Grossman, C. D. (1998). On Killing, Penguin. Chapter Two

[146] Grossman, C.D. "Physiological Arousal and Fear" Encyclopaedia of Violence, Peace, and Conflict, **Volume 3, Page** 159

[147] Macedonia, M. (2005). Entertainment Technology and Virtual Environments for Military Training and Education. **Page** 36

The latest upgrades to both hardware and software can provide an advantage to a soldier and force, but what about the constant need to train soldiers on these updates and revisions of software? A soldier cannot always be in class for the introduction of new revisions and updates. If a new version of a piece of software becomes available, whose responsibility is it to teach the others these new concepts and tools? Should a force stick to a constant level and only update when a major addition is created. Should it apply the needed updates as they develop? These issues need to be addressed as they will impact on the ability of a force to provide a constant learning environment.

With the constant development in IT and ICT a force will compare itself to its allies, and see what they are introducing or revising to better prepare their soldiers to fight with high technology levels. The United States is the leader in this regard as it has the commercial and technological basis to be able to implement major upgrades and revisions to its software and hardware when required. They have the manpower to be able to remove soldiers from their primary tasks and put them through a revision process, while another soldier takes over for them so that operational tempo is maintained. This is not possible for nations like New Zealand. It does not have the financial or manpower requirements to be able to remove an active soldier for revision training, without the loss of operational tempo. New Zealand needs to be able to find or invest in practical solutions to this update issue. This issue is only going to increase with time as the changes in software and hardware start to impact on the operational tempo of most nations.

This revision concern, when coupled with the interoperability of system with other nations, could see problems getting worse. If the United States implements a large scale update of their systems and remove the backwards capability from the system then all nations who want to join in or work with them will need to update as well or be forced to update. New Zealand cannot win this fight. The resources and skill are not there and the use of the Kiwi mentality could actually work against us, as our solutions could cause more problems than rectifying the initial dilemma.

Even without looking to other nations this issue of incompatible software or hardware could come to pass. This could be in the form of joint forces operations between the three services. If the NZ Army updates itself to the new HLA or even the IPv6 protocol before the other services do they could be left out of Joint operations or be unable to effectively work with the other services. A single stepped approach is needed for all of the services so that the updates and upgrades will take effect evenly around the three services. Training interoperability will also be a key task that will need to be taken in to consideration. NCW simulations will have to have a generic approach if it is to be taken up by all three services. A strong joint foundation will need to be set so that there is no internal or inter-service issue.

This integration of both simulation system and operational systems calls for the need to ensure that correct operational procedures are introduced or in effect. The United States Army found during its NCW training and experiments that soldiers were being faced with simple error issues such as systems either being disconnected or being switched off. The training systems that they were using were expecting to either send or receive information from other units and the systems and soldiers were not getting the results they were expecting. Training was stalled because of this. Their basic troubleshooting skills had not been developed as they had an inbuilt reliability on the technical support available to them. New Zealand cannot afford this reliance as it would not be cost effective to have the massive amounts of technical support needed to be able to identify and solve all of the minor issues. For this reason it is critical that all soldiers should get basic trouble shooting skills for the operational NCW systems.

As an interesting side point to training issues, the New Zealand Army Simulation Centre (NZASC) has found an ingenious way of offsetting the training time required for their constructive simulation system Janus. Instead of having to train every officer in its use and means they have decided to put an intermediate step into the process. They have developed a group of people who act as the interface between the Officer and the simulation system. These people are known as Interactors. It is their responsibility to interpret the

officer's orders in to the outcomes needed in the simulation system. These people are trained on the updates and modifications done to the system instead of the individual officers. This is a good solution to the limited resource and time that the NZ Army can invest in operational constructive simulation training.

The following images are of the training systems that are used by the Interactors to help with Officer training in the NZDF. They are constructed based simulations, with icons representing multiple units.

Figure Three: Janus constructed simulation[148]

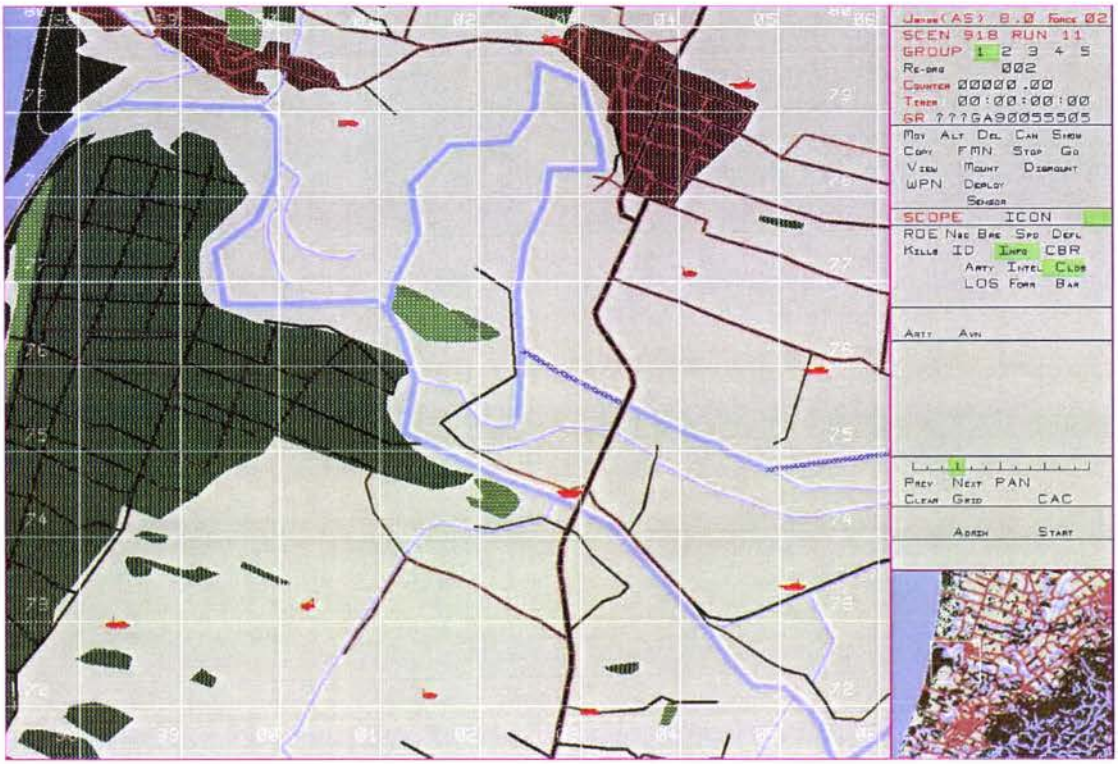
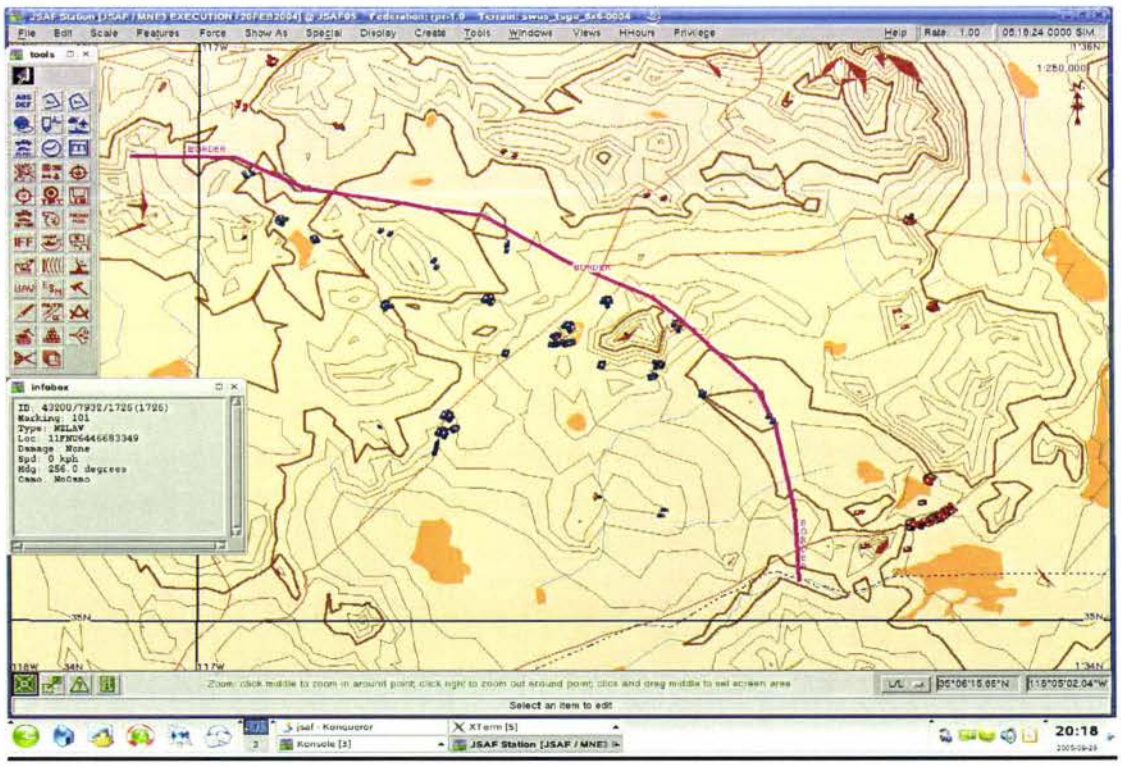


Figure Four: J-SAF (Joint Semi Autonomous Force) Constructed Sim



[148] Screen captures of the software from the NZASC presentation: **Simulation: Use of Technology,** Major Thomas Bielenberg, Mr Andy Hatt, Massey University 30 May 06

And finally according to international research, is the major issue of information overload. When the amount of processed and raw data is coming in at a high rate that the soldier or operator who is in charge or using the information starts to have performance degradation. This comes about, due to human physiology as the human mind can only deal with a limited amount of information at a time. But current NCW has an unfiltered approach to information. This can overwhelm many people quickly if correct methods of coping have not been introduced in a controlled manner. This issue is one of the core stumbling blocks to the implementation of NCW. This has to be changed so that future soldiers can work in peak condition[149].

As an example of this, the United States Army war-fighters are being introduced and exposed to multiple IT systems for both NCW and conventional warfare, such as satellites, the Joint Surveillance/Target Attack Radar System (JSTARS) and UAVs which are providing real time information to the All Source Analysis System (ASAS), Advanced Field Artillery Tactical Data System (AFTADS) and the Manoeuvre Control System (MCS) at the same time. These systems produce over one hundred individual messages of unfiltered information per minute[150]. The war-fighter has to be able to process and categorise this information so that the best tactical and operational advantage can be made from it, while receiving constant updates to those systems.

Simulation technology can help with this issue while solutions are found to help filter the raw and processed information. Simulations can replicate the complex operational environment that is present in a NCW area. This gives the operators or soldier's time to create managing techniques that will help them cope with the demands in a controlled environment.[151]

---

[149] Cotton, A. J. (2005). Information Technology – Information Overload for Strategic Leaders. **Page** 33.
[150] Moses, F. L. (2005). Training Challenges for Digitization. **Page** 34
[151] Freeman, J. T. and M. S. Cohen (2005). Information Overload in the Digital Army: Simulator-based Training for Prevention, Detection & Cure ,**Page** 5.

Chapter Nine
Conclusion

Network Centric Warfare and digitisation are the next steps in the evolving warfare cycle. This is a global phenomenon that the NZDF needs to make a conscious effort to understand and to implement to some degree. The transition from platform centric to network centric warfare will have a lasting impression on both the makeup and cultural identity of the NZDF and the New Zealand Army. This change in methods and approach will change they way warfare is managed and implemented for the rest of the 21st century.

Many hard lessons from other countries attempts at introducing NCW and digital technology to their armed forces; needs to be taken onboard, before the mistakes are repeated in the NZDF's attempt. The NZDF cannot afford both financially and in human resources to go down non-productive paths in the implementation of NCW and its digital integration.

New Zealand will need to create its own NCW identity in the global realm. No other country's solutions will fit the unique cultural identity that the NZDF has. The need for the right people in the right positions will have to be maintained if the NZDF's transformation to a NCW enabled force will succeed.

As a conclusion derived from this research, both policy and doctrine will need to change to adapt to the fluid and dynamic environment that NCW and digitisation will provide. Old methods and techniques will need to be enhanced and/or modified to truly utilise the capability and force multiplier that NCW provides.

The New Zealand Government will need to implement new standards for the organisations who wish to be part of interagency agreements with the NZDF Issues such as the transition to the new IPv6 protocol and split level security will need to be addressed. But the advantages provided by the inter agency co-operation will provide greater benefits to all of the participating members.

Inter agency training on digital training devices will also help to save limited operating resources. Interactions between the NZ Police and the NZ Army, as a usable example, will help both to create closer working skills and methods that will benefit both sides. Digital weapons training could become one of those core foundations between the two agencies.

The correct implementation of NCW and digitisation will save lives but it is depended on the skill of the people running the systems and using the end results. If a good foundation with clear goals is established at the beginning of the NZDF's and Army's transformation, then the follow-on will be of great benefit, both in available resources and training ability, to the service personnel under their influence.

The road to a successful implementation of NCW and digital training will be difficult with many technical and cultural aspects needing to be taken into account. But if the NZDF follows its own guidelines of getting and retaining the right people for the right positions then the NZDF will be able to continue to be a valuable member of any coalition.

Interoperability with our allies and friends has always been a key consideration for any purchase or investment, and NCW and digitisation are no exception. But this time there is more than just the financial aspect under consideration. The NZDF will need to set its own guidelines as to how much external influence will be accepted in the development of the NCW capability. It will have to decide on information architecture and structure which will influence all future capabilities and hardware selections. The choice between HLA and DIS simulation architecture is one example of these decisions. This should not be an individual service decision because the benefits of a joint

interactive simulation network among the three services is unmatched. The timeframe for these decisions and others, such as the transition to IPv6, is getting closer with all of the services starting to invest in simulation and new IT technology. The IT and NCW standards need to be set and agreed upon by all involved parties, or the possibility of joint interaction could be lost, or at the least hindered, as a viable solution is created.

There also needs to be a unified research approach for both digitisation and NCW. A single defence research entity needs to take control of the fractured research nature that is currently present in the NZDF. Each service needs to participate in joint and combined research for the betterment of the whole NZDF. Interactions between the operational and research sides of defence need to be established so that clear boundaries can be set. There is no point having the NZDF pay twice for the same research from different organisations. This approach will also help with interactions between Defence Force organisations globally, with a single research point. This does not mean that the services will lose their research capability but it means that they will have an awareness of other services research so that they can focus on the operational research aspects of their force.

With all of the strategic and operational changes that will be brought about by the introduction of NCW and digitisation, there needs to be an increased focus on the average service member. These people will be the backbone of any change to the NZDF or the New Zealand Army. If these people do not accept or have hesitation about the introduction of digital technology to both their service environment and their career path, then the whole process could stall or get delayed to a point where it is ineffective and the benefits lost.

Soldiers coming into the services now will be at the forefront of the changes. These people will lay the developmental framework down for the implementation of this change. These people will be reliant on the skill and technology that is introduced. As this research has shown, the greatest asset and resource that any service has in the implementation of NCW, is its people. These resources cannot be easily replaced if lost or harmed. People

must be treated with the up most care and the training they get must help them become better soldiers for both the NZDF and the coalition forces that they could be attached to.

With the introduction of NCW and digitisation, new issues are going to be created which have not been encountered before and yet will have a large impact on the operational tempo and organisational make up of the present and future NZDF. The issues, such as that of Information Overload (IO)[152] or that of Information Assurance (IA), will become more prominent. As has been suggested, early intervention or early introduction of coping skills needs to be implemented before soldiers are exposed to operational environments where these issues could cost lives. Correct prevention and management may end up saving lives in the future.

There must also be an awareness that the techniques and methods that are introduced into the Army and NZDF, in relation to NCW, could have a longer impact than first expected, in comparison to the introduction of a weapons platform. Some of the methods and techniques that have been looked at through the entire research project will have unknown side effects. This is one of the consequences of using such rapidly evolving technology. The operant conditioning that is use in reflex training, such as target shooting, can remain imprinted on the soldier long after the training has ended. Awareness has to be maintained that these soldiers have been programmed to respond by reflex to certain stimuli, some of this is done down to a subconscious level. The stimulus that is present in some digital training solutions such as the WTS system can reinforce some of the hidden behavioural issue some people can have. Ethical and moral considerations need to be integrated into the training environment especially with the rise in Asymmetrical Warfare.

This research has tried to show that there is a strong case for the implementation of NCW and digital training by both the NZDF and the New Zealand Army. It has shown that there is a need for strong standards to be set

---

[152] Ibid.

early and adhered to[153]. Science and technology will continue to progress and it is up to the leadership of both the NZDF and the NZ Army to decide where they want to go and how they are going to get there. NCW is a force enabler and multiplier, but it can be an Achilles heel as well. This research has shown that if a greater reliance is put onto technology as the solution to everything then the possibility of failing starts to increase. There will always need to be well-rounded soldiers to fight for New Zealand who have the basic skills to be good soldiers even when they don't have all of the latest technology their allies may have. That has been the strength of the New Zealand service personnel. They have the ability to adapt to the changing environment without the loss of their unique identity. The NZDF culture will change with the implementation of NCW and digitisation but the core elements which make the NZDF unique in the international community will not change as these are at the heart of the three services.

The NZDF and the New Zealand Army are on the brink of a new era in warfare. The need to have high skilled, digital soldiers and equipment is no longer a fantasy. With correct implementation the NZDF could have some of the most advance and effective soldiers in the world with high quality training to support them. These soldiers could have highly sound and adaptable skills which would make them deadly in combat but also well rounded with high morals and ethics to be superb peacekeepers and peacemakers. The choices that are made now will have long-term consequences which will either hurt or enhance the global reputation of both the NZDF and the New Zealand Army.

---

[153] Cotton, A. J. (2005). Information Technology – Information Overload for Strategic Leaders. **Page** 33.

Appendix A[154]

The Next Soldier:	
Traditional Soldier Qualities:	**Additional qualities for NEA:**
Mana	
Discipline	
Fitness	
Decisiveness	
Leadership	
Obedience	
Patriotism	
Sacrifice	
Loyalty	
Courage and Compassion	
Teamwork	
Morality and Ethics	
	Versatility
	Flexibility
	Adaptability
	Confidence
	Independence
	Initiative
	Intercultural Competence
	System Thinking
	Relationship Management
	Cognitive Skills
	High Emotional Intelligence (EQ)
	Skills to innovate and to improvise.

Appendix B: Soldiers Skills

Traditional Soldier:	**NEA Soldier:** Basic / Advanced
Drill	
Marksmanship	
First Aid	
Field craft/ Map Reading	
Basic LoAC knowledge	
	Basic Keyboard and Mouse Skills
	Basic Technology Troubleshooting
	Basic Business Applications (MS office)
	Data Management
	Information Management
	Database Manipulation

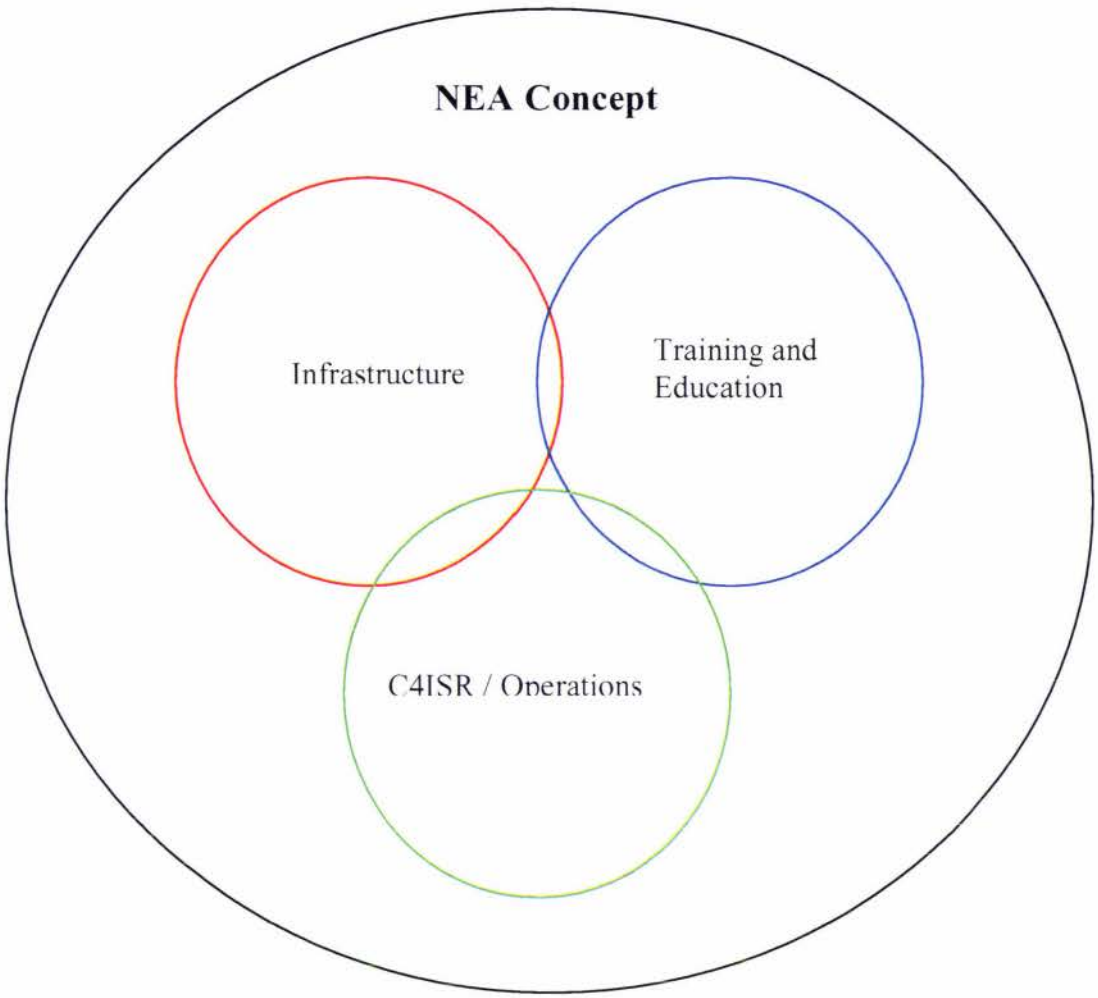
[154] Appendixes derived from current NZDF doctrine and recommendations from Defence Advance Research Projects Agency, Defence Science and Technology Office and US Army Research Institute.

Appendix C

Current Levels vs. NCW (NEA) needs:

Position:	*Has needed skills:*		*N.E.A. Ready:*	*Needs NEA Skills:*	
	Basic /Advance			Basic / Advance	
Army Combat Careers:					
Rifleman:	X	X	X	√	√
Crewman:	√	X	X	√	√
Field Engineer	√	X	X	√	√
Gunner	√	X	X	√	√
Plant Operator	X	X	X	√	X
Army Apprenticeship Careers:					
Armourer	X	X	X	√	X
Carpenter	X	X	X	√	X
Electrician	√	X	X	√	X
Electrical Fitters	√	X	X	√	X
Electronic Technicians	√	√	X	√	√
Maintenance Fitter	√	X	X	√	X
Position:	*Has needed skills:*		*N.E.A. Ready:*	*Needs NEA Skills:*	
	Basic /Advance			Basic /Advance	
Plumber	X	X	X	√	X
Systems Engineer	√	√	√	X	X
Vehicle Mechanic	X	X	X	√	X
Army Support Careers:					
Administrators	√	X	X	X	X
Ammunition Technician	X	X	X	√	X
Chef	X	X	X	X	X
Comm Sys Op	√	√	√	X	X
Driver	X	X	X	√	√
Info Sys Op	√	√	√	X	X
Movement Operator	√	X	X	√	X
PTI	X	X	X	X	X
Steward	X	X	X	X	X
Supply/Quartermaster	√	X	X	√	X
Specialist Positions:					
Bandsman	X	X	X	X	X
Dental Hygienist	X	X	X	X	X
Educators	√	X	X	√	√
Fire Fighter	X	X	X	X	X
Medic	X	X	X	√	X
Needed Positions:					
Simulation Operator	√	√	√	√	√
Info Ops Operators	√	√	√	√	√

Appendix D
The NEA Environment



NEA Concepts focus at the levels of war:			
Level / Component	Training and Education	C4ISR / OPS	Infrastructure
Tactical	High	Medium	Low
Operational	Medium	Medium	Medium
Strategic	Low	Medium	High

Possible participants needed in an NEA Steering Group:

- Communication and Information Systems branch (CIS).
- Directorate of Joint Command, Control, Communications and Information Systems
- J8 Development Branch and the Defence Technology Agency
- J7 Training
- HQNZDF.
- Army Training Group
- Army Simulation centre

Appendix E

NEA Considerations and Recommendations:

1. **High Level Architecture:**
   - *a.* Single programming standard for all applications. Both operational and simulated.
   - *b.* Unified data types across all databases for easy information exchange
   - *c.* Unified Operating System for ease of change and standardisation. (Such as Linux, OS X or MS Windows).
   - *d.* Interactive simulations, Sims that work together, live, virtual, and constructed for increased fidelity.
2. **Oversight:**
   - *a.* A unified approach must be taken to maximise its potential.
   - *b.* Representatives from all braches must be involved to remove the possibility of one branch going in a different direction. (Dependent on policy directives)
   - *c.* A single research database must be created to keep track of all projects and to stop duplication in the NEA environment. (Dependent n policy directives)
   - *d.* NEA doctrine must match up to both Joint and Army specific doctrine and procedures.
3. **Training**:
   - *a.* Tri-service participation must be made available to keep inline with current military doctrine, in the areas of Network Force and Knowledge Edge Force.
   - *b.* A standing Opposition Force (OPFOR) must be available to train and implement new lessons learn from operational experience to help soldiers get up to speed quicker for deployment.
   - *c.* Soldiers must have access to training materials after hours to improve or reinforce lessons, such as websites and CD ROMs.
   - *d.* All ranks must be able to use digital equipment. Catch-up classes should be made available to all ranks, to keep them up to date on software and hardware updates.
   - *e.* A form of New Equipment Training (NET) must be created for new recruits so the most up to date information is being introduced to units.
   - *f.* A database of all NEA trained soldiers must be created, to track progression and location of troops so correct continued training could be given.
4. **Army Structure:**
   - *a.* New soldier careers should be created for the NEA environment, such as Simulation Officers, Data Management Officers, Information Operations officers, and should be advertised like standard careers.

b. A new NEA branch should be created which will take Comm Sys and Info Sys under its control to unify standards and protocols. This branch will also be responsible for IO, IW, NEO, and EW.

Bibliography

Abigail, M. G. P. (2004). "Preparing the Australian Army for 21st-Century Conflict: Problems and Perspectives," in Future Armies, Future Challenges: Land Warfare in the Information Age. Michael Evans, Russell Parkins and Alan Ryan (eds). Sydney, Allen and Unwin

Alberts, D. S., Garstka, J. J., et al. (2000). Network Centric Warfare: Developing and Leveraging Information Superiority. Office of Force Transformation, United States Department of Defense.

Alvarez, S. (2005). Army's Ongoing Transformation Was Decades in the Making, Washington DC, American Forces Press Service.

Alvarez, S. (2005). Gaming is More Than Just Play for Military Services, Washington DC, American Forces Press Service.

Antal, J. A. (1999). "Battle Shock XXI". in Digital War, R. L. Bateman (ed). Novato, CA, Presidio Press.

Antal, J. A. (1999). "The End of Manoeuvre," Digital War, R. L. Bateman (ed), Novato, CA, Presidio Press.

Archer, R. and W. Warwick (2003). Training Future Force Leaders to Make Decisions Using Digital Information, United States Army Research Institute for the Behavioural and Social Sciences.

Babcock, S. (2002). Canadian Network Enabled Operations Initiatives, Directorate Defence Analysis, National Defence Headquarters.

Banks, S. B. and M. R. Stytz (2005). Cyber Warfare Distributed Training: Considerations and Requirements for Operators in Network Centric Warfare.

Barbin-Smith, R. (1997). "The Challenge for Australia's Defence Science," in The Revolution in Military Affairs: Warfare in the Information Age.

Bateman, R. L. (1999). "Pandora's Box". Digital War. R. L. Bateman (ed). Novato, CA, Presidio Press.

Batiste, J. R. S. (2004). Soldier's Handbook to Iraq. US Army, 1st Infantry Division.

Battelle (2005). Future Terror Defences. http://www.battelle.org/forecasts/terror.stm, www.battelle.org.

Battelle (2005). Technological Forecast. http://www.battelle.org/forecasts/defense.stm, www.battelle.org.

Bellin, D. and G. Chapman (1987). Computers in Battle: Will they work? Florida, Harcourt Brace Jovanovich.

Biddle, S. (2003). "Afghanistan and the Future of Warfare," Foreign Affairs, vol. 82 (no. 2).

Bolger, D. P. (1999). "The Electric Pawn: Prospects for Light Forces on the Digitized Battlefield," Digital War. R. L. Bateman (ed). Novato, Ca, Presido Press.

Bowie, C. J. (2004). "Trends in Future Warfare," Joint Forces Quarterly (Issue 35).

Boyd, C. (2005). US army cuts teeth on video game. BBC News. London, BBC, Http://www.bbc.com/news.

Bracken, P. (2006). "Net Assessment: A Practical Guide," Parameters 2006 (Spring).

Branch, A. A. D. (2002). Land Warfare Doctrine 1: The Fundamentals of Land Warfare.

Brown, B. R. and L. Anderson (1999). Cognitive Requirements for Information Operations Training, United States Army.

Burgoon, J. K., S. Weisband, et al. (2005). Interactivity, Communication, and Trust: Further Studies of Leadership in the Electronic Age. University of Arizona, United States Army Research Institute for the Behavioural and Social Sciences.

Bushnell, D. M. (2004). Future Strategic Issues/Future Warfare. Future Threat for Global War Games Army War College, NASA Langley Research Centre.

Campbell, C. H. and R. C. Campbell (2006). Approaches to Managing Future Training, U.S. Army Research Institute for the Behavioural and Social Sciences.

Campbell, R. C., C. E. Sager, et al. (2005). Future Soldiers: Analysis of Entry-Level Performance Requirements and their Predictors, United States Army Research Institute for the Behavioural and Social Sciences.

Chatham, R. (2001). "A Tale of Training Superiority, Games, and People Stuff." DARPA DSO.

Cheeseman, G. (2004). "Defending the "other": military force(s) and the cosmopolitan project," in Future Armies, Future Challenges: Land Warfare in the Information Age. Michael Evans, Russell Parkins and Alan Ryan (eds). Sydney, Allen and Unwin

Coker, C. (2004). The Future of War Oxford, Blackwell Publishing.

Cotton, A. J. (2005). Information Technology – Information Overload for Strategic Leaders. U.S. Army War College.

Cousens, C. R. (2004). "Whiter the close battle - British Army operations: 2015 and beyond," in Future Armies, Future Challenges: Land Warfare in the Information Age. Michael Evans, Russell Parkins and Alan Ryan (eds), Sydney, Allen and Unwin.

Curnow, C. K. (2002). *Training on the Web: Identifying and Authenticating Learners,* United States Army Research Institute for the Behavioural and Social Sciences.

Department of Defense, (2006). Quadrennial Defense Review. DOD, Department of Defense.

Defence Simulation and Modelling Office (1995). Modelling and Simulation (M&S) Master Plan. Under Secretary of Defense for Acquisition and Technology. Http://www.dsmo.mil.

Denning, D. (1999). Information Warfare and Security. New York, ACM Press.

Dichairo, J. J. (1986). The Impacts of Digitization on the Army's Military Decision-Making Process: Modifications to the Estimate of the Situation. U.S. Army Command and General Staff College, Niagm University. Master of Military Art and Science.

Dressel, D. J. and B. B. Schaab (2003). Training the Troops: What Today's Soldiers Tell Us About Training for Information-Age Digital Competency, U.S. Army Research Institute.

Dressel, D. J. and B. B. Schaab (2005). Training Requirements of Digital System Operators in a Stryker Brigade Combat Team, U.S. Army Research Institute for the Behavioural and Social Sciences.

Dunn, P. J. (1997). "Time X Technology X Tactics = RMA," The Revolution in Military Affairs: Warfare in the Information Age.

Dyer, J. L. and R. L. Wampler (2006). Training Lessons Learned and Confirmed From Military Training Research, U.S. Army Research Institute for the Behavioural and Social Sciences.

Efflandt, S. and B. Reed (2001). "Developing the Warrior Scholar." Military Review (July-August 2001).

Enemo, G. (2005). Analysis of Command and Control (C2) in Network Enabled Operations (NEO), Norwegian Defence Research Establishment.

Erwin, S. I. (2000). "Videogames Gain Clout as Military Training Tools," National Defense Magazine November (2000).

Evans, K. L. (2003). Project train mod: modernizing soldier training through research, U.S. Army Research Institute.

Evans, M. (2004). "Clausewitz's chameleon: Military theory and practice in the early 21st century". in Future Armies, Future Challenges: Land Warfare in the Information Age. Michael Evans, Russell Parkins and Alan Ryan (eds). Sydney, Allen and Unwin

Felton, a. and B. B. Schaab (2003). Training Requirements for Battle NCOs in Digital Units, U.S. Army Research Institute.

Ferrell, R. S. (2002). Army Transformation and Digitization – Training and Resource Challenges, US Army War Collage Strategy Research Project.

Fontenot, G. (2005). "Seeing Red: Creating a Red-Team Capability for the Blue Force," Military Review 2005(September-October).

Fowler, S. (2005). Army medics train with patient simulators. Army News Service.

Freeman, J. T. and M. S. Cohen (2005). Information Overload in the Digital Army: Simulator-based Training for Prevention, Detection & Cure, U.S. Army Research Institute for the Behavioural and Social Sciences.

Gee, J. P. (2003). What Video Games Have to Teach Us About Learning and Literacy? Hamshire, England, Palgrave Macmillian.

Gentry, J. A. (2002). "Doomed to Fail: America's Blind Faith in Military Technology," Parameters 2003(Winter).

Graves, C. R., D. M. Pratt, et al. (1999). Force XXI Training Program-Digital Project: Report on Development and Lessons Learned, U.S. Army Research Institute.

Grossman, C. D. (1998). On Killing, Penguin Press.

Hess, K. P. (2003). Training Adaptability in Digital Skills: The Learning Skills Bridge (LSB) Learning Accelerator, U.S. Army Research Institute for the Behavioural and Social Sciences.

Hosek, J. H. (2003). "The Solider of the 21st Century," New Challenges, New Tools for Defence Decision-making.

Ignatieff, M. (2002). Virtual War. London, Chatto & Windus.

James. B. (2004). Instructional Characteristics and Motivational Features of a PC-based Game, U.S. Army Research Institute for the Behavioural and Social Sciences.

Kaplan, F. (2005). A Future the Army Can't Afford. http://slate.msn.com/id/2115867/.

Kegan, J. (2002). Intelligence in war: The value and limitations of what the military can learn about the enemy. New York, Random House.

Kirriemuir, J. (2002). "Video gaming, Education and Digital Learning Technologies," D-Lib Magazine Volume 8(NO. 2).

Koucheravy, R. J. (2001). Whence the Soldier of the Future? Recruiting and Training for the Objective Force. Fort Leavenworth, Kansas, School of Advanced Military Studies, United States Army Command and General Staff College.

Krepinevich, R. (2002). "The Army and Land Warfare: Transforming the Legions," Joint Forces Quarterly (Autumn 2002).

Latham, R. (2003). Bombs and Bandwidth: The emerging relationship between Information technology and security. New York, The New Press.

Lenoir, T. (2000). "All But War is Simulation: The Military Entertainment Complex," Configurations Fall.

Leonhard, L. C. R. (1999). "A Culture of Velocity". Digital War. R. L. Bateman. Novato, CA, Presidio Press.

Leonhard, L. C. R. (2004). "Creating a culture of velocity: The western military commander's mindset and the challenge of digitisation," in Future Armies, Future Challenges: Land Warfare in the Information Age. Michael Evans, Russell Parkins and Alan Ryan (eds). Sydney, Allen and Unwin

Leonhard, R. R. (1998). "The Principles of War for the Information Age," Digital War. R. L. Bateman (ed). Novato, CA, Presidio Press.

Lewis, M. G. D. (2004). "Lessons from East Timor," in Future Armies, Future Challenges: Land Warfare in the Information Age. Michael Evans, Russell Parkins and Alan Ryan (eds). Sydney, Allen and Unwin.

Livingstone, S. C. and J. T. Root (2005). Surrogates for Future Force Warrior (FFW) Training Research, United States Army Research Institute for the Behavioural and Social Sciences.

Lonsdale, D. J. (2004). The Nature of War in the Information Age. Great Britain, Frank Cass.

Lorenzo, G. (2002). "EArmyU and the Future of Distance Education," The Technology Source.
http://www.thetechnologysource.com

Luddy, J. (2005). The Challenge and Promise of Network-Centric Warfare, Lexington Institute.

Ministry of Defence. U.K. (2003). British Defence Doctrine, London, United Kingdom Ministry of Defence. (Joint War fighting Publication).

Ministry of Defence. U.K. (2004). Computing Technology for Defence. London, United Kingdom Ministry of Defence

Macedonia, M. (2005). Entertainment Technology and Virtual Environments for Military Training and Education. Orlando, Florida, U.S. Army Simulation, Training and Instrumentation Control.

MacFarling, G. C. I. (2004). "Asymmetrical warfare: myth or reality," in Future Armies, Future Challenges: Land Warfare in the Information Age. Michael Evans, Russell Parkins and Alan Ryan (eds). Sydney, Allen and Unwin.

Macgregor, C. D. (1999). "Command and Control for Strategic Action". Digital War. R. L. Bateman (Eds). Novato, CA, Presidio Press.

Macgregor, C. D. (2004). "Resurrecting Transformation for the post-industrial era". in Future Armies, Future Challenges: Land Warfare in the Information Age. Michael Evans, Russell Parkins and Alan Ryan (eds). Sydney, Allen and Unwin.

MacMillan, K. (2005). Evolving Command & Control: The Challenge for Smaller Defence Forces, Canberra, Booz Allen Hamilton, Defence and National Security Team., Australia,

Mayberry, P. W. (2005). "Transforming Training," Military Training Technology **Volume 8** (NO. 4).

Menon, R. A. (2004). "Maritime strategy, land warfare, and the revolution in naval affairs," in Future Armies, Future Challenges: Land Warfare in the Information Age. Michael Evans, Russell Parkins and Alan Ryan (eds). Sydney, Allen and Unwin

Moses, F. L. (2005). Training Challenges for Digitization. U.S. Army Research Institute for the Behavioural and Social Sciences.

Nanda, S. (2005). Applying Technology to Train Visualization Skills. I. SDS International, United States Army Research Institute for the Behavioural and Social Sciences.

New Zealand Defence Force, (2006). New Zealand Defence Force: Statement of Intent. NZDF. Wellington, NZDF.

New Zealand Ministry of Defence, (2000). The Government Defence Policy.

New Zealand Ministry of Defence (2000). The Government's defence policy framework. Wellington, New Zealand Government.

New Zealand Ministry of Defence (2001). A Modern, Sustainable Defence force Matched to New Zealand's Needs. Wellington, New Zealand Government.

New Zealand Ministry of Defence (2002). The Defence Portfolio. NZMOD

New Zealand Ministry of Defence (2002). Ministerial Briefings 2002 Legislation, NZMOD.
http://www.beehive.govt.nz/briefings/dta/defence/legislation.cfm

New Zealand Ministry of Defence (2002). Ministerial Briefings 2002 New Zealand Ministry of Defence policy,
http://www.beehive.govt.nz

New Zealand Ministry of Defence (2002). Ministerial Briefings 2002 New Zealand Ministry of Defence roles,
http://www.beehive.govt.nz

New Zealand Ministry of Defence (2004). Annual Report: for the year ended 30 June 2004, New Zealand Ministry of Defence.

New Zealand Ministry of Defence (2004). Defence long term Development plan, New Zealand Ministry of Defence.

New Zealand Ministry of Defence (2004). Ministry of Defence Statement of Intent. New Zealand Ministry of Defence.

New Zealand Ministry of Defence (2005). Ministry of Defence Statement of Intent. Wellington, New Zealand Ministry of Defence.

New Zealand Ministry of Defence (2002). Improving Joint Effectiveness in Defence. Cabinet Policy Committee, Minister of Defence.

Nieborg, D. (2005). Changing the Rules of Engagement -Tapping into the Popular Culture of America's Army, the Official U.S. Army Computer Game. Faculty of Arts. The Netherlands, Utrecht University.

Offley, E. (1999). "The Military-Media Relationship in the Digital Age," Digital War. R. L. Bateman (ed). Novato, CA, Presidio Press.

Orvis, K. A. and Orvis, K. L. (2005). The influence of trainee gaming experience and computer self-efficacy on learner outcomes of videogame-

based learning environments, United States Army Research Institute for the Behavioural And Social Sciences.

Page, E. H. (1998). Introduction to Military Training Simulation: A guide for discrete event simulationists. Proceedings of the 1998 Winter Simulation Conference, Washington, DC, the MITRE Corporation.

Paterson, R. (2005). "Capturing Live Combat in Network Centric Warfare". Proceedings of DARPATech 2005. Washington DC, Department of the Army Advanced Technology Office

Peters, L. C. R. (2004). "The West's Future Foes: Amplification and slaughter," in Future Armies, Future Challenges: Land Warfare in the Information Age. Michael Evans, Russell Parkins and Alan Ryan (eds). Sydney, Allen and Unwin.

Ping, I. C. K. (2000). High Level Architecture Performance Measurement. Master's Thesis in the Department of Modelling Virtual Environments and Simulation, Monterey,. CA, Naval Postgraduate School http://handle.dtic.mil/100.2/ADA376484

Prensky, M. (2001). "The Games Generations: How Learners Have Changed," Digital Game Based Learning. California, M. Prensky (Ed) McGraw- Hill

Prensky, M. (2001). "'Simulations': Are They Games?" Digital Game Based Learning. M. Prensky (Ed), McGraw Hill.

Prensky, M. (2001). "True Believers: Digital Game Based Learning in the Military," Digital Game Based Learning. M. Prensky (Ed), McGraw Hill:

Prensky, M. (2001). "Why Education and Training Have NOT Changed." Digital Game Based Learning. M. Prensky (Ed), McGraw Hill:

Prensky, M. (2002). "Evolving Instruction? Seven Challenges." On the Horizon **Volume 10** (no. 2).

Prensky, M. (2002). A Military Field and Training Game Developer Corps. http:/www.games2learn.org

Prensky, M. (2003). Has "Growing Up Digital" and Extensive Video Game Playing Affected Younger Military Personnel's Skill Sets? Inter-service /Industry Training, Simulation, and Education Conference (I/ITSEC) 2003.

Prensky, M. (2004). "Interactive Pretending: An overview of Pretending," 2005. http:/www.games2learn.org

Prensky, M. (2004). "The Seven Games of Highly Effective People," Microsoft Games for Windows.
http:/www.games2learn.org

Pryor, M. (1999). "Digitization, Simulation and the Future of the Army National Guard," Digital War. R. L. Bateman (Ed). Novato, CA, Presidio Press.

Randal, B. L. (2001). Sun Tzu: The Art of Network Centric Warfare. U. S. Air Force. Carlisle Barracks, Pennsylvania 17013, U.S. Army War College.

Richardson, J. G. (2002). War, Science and Terrorism. London, Frank Cass Publishers.

Roland, R. (1998). Panel: "The Future of Military Simulation," Proceedings of the Winter Simulation Conference, Monterey, CA, Rolands & Associates Corporation.

Raise, G. S. M. (2004). "Lessons from Bosnia: a British perspective," in Future Armies, Future Challenges: Land Warfare in the Information Age. Michael Evans, Russell Parkins and Alan Ryan (eds). Sydney, Allen and Unwin

Ryan, A. (2004). "Early 21st-century armies and the challenge of unrestricted warfare," in Future Armies, Future Challenges: Land Warfare in the Information Age. Michael Evans, Russell Parkins and Alan Ryan (eds). Sydney, Allen and Unwin

Ryan, A. (2004). "Land forces in the 21st century coalition operations: implications for the Asia pacific," in Future Armies, Future Challenges: Land Warfare in the Information Age. Michael Evans, Russell Parkins and Alan Ryan (eds). Sydney, Allen and Unwin

Sanchez, L. M. (2002). Violent Video games and Operant Conditioning. Maxwell School, International Peace Bureau. International Organizations.

Sanders, W. R. (2001). Cognitive Psychology Principles for Digital Systems Training, U.S. Army Research Institute for the Behavioural and Social Sciences.

Schaab, B. B. and Dressel, D. J. (2001). Training for Adaptability and Transfer on Digital Systems, U.S. Army Research Institute.

Schaab, B. B. and Dressel, D. J. (2004). Digital Skills Training for Net-Centric Operations. Alexandria, VA, U.S. Army Research Institute for the Behavioural and Social Sciences.

Schaab, B. B. and Moses, F. L. (2001). Six Myths about Digital Skills Training, U.S. Army Research Institute for the Behavioural and Social Sciences.

Shukman, D. (1995). Tomorrow's War. New York, Harcourt Brace and Company.

Sieberg, D. (2001). "War games: Military training goes high-tech," CNN Online, New York, CNN News Network.
http://www.CNN.com .

Singh, H. and Dyer, J. L. (2002). The Computer Backgrounds of Soldiers in Army Units, U.S. Army Research Institute.

Singh, H. and Dyer, J. L. (2005). Computer-based Approaches for Training Interactive Digital Map Displays, U.S. Army Research Institute.

Smith, H. (2004). "The military profession in Australia: Crossroads and cross-purposes?" in Future Armies, Future Challenges: Land Warfare in the Information Age. Michael Evans, Russell Parkins and Alan Ryan (eds). Sydney, Allen and Unwin

Spiller, R. (2004). "Sharp corners: Combat operations in urban areas," in Future Armies, Future Challenges: Land Warfare in the Information Age. Michael Evans, Russell Parkins and Alan Ryan (eds). Sydney, Allen and Unwin

Steele, R. D. (2006). Information Operations: Putting the "I" Back Into D.I.M.E, U.S. ARMY Strategic Studies Institute.

TACOM (2004). Future Combat Systems. Department of Defense, Boeing.

Talbot, D. (2004). "How Technology Failed in Iraq," Technology Review: Emerging Technologies and Their Impact
http://www.technologyreview.com/Infotech/13893/page1.

Thomas, J. A. (2005). Evaluating the Claims of Network Centric Warfare. Master of Science in Human Systems Integration
Monterey,. CA, Naval Postgraduate School

Trinquand, B. D. (2004). Lessons learnt from Multinational Operations. Future Armies, Future Challenges: Land warfare in the Information age.

United States Army (1984) Fighting Future Wars (Army Field Manual 100-5). Washington DC, Brassey's / / Department of the Army (US).

United States Army (2005). EArmyU. Department of the Army. US Army Online University
www.earmyu.com.

United States Army (2005). The Army Future Force: Decisive 21st century land power. Training and Doctrine Command (TRADOC).

Vandergriff, D. (1999). "The Culture Wars" in Digital War. R. L. Bateman (ed). Novato, CA, Presidio Press.

Venzke, B. (2003). "Al-Qaeda's Advice for Mujahideen in Iraq: Lessons Learned in Afghanistan," Intelcentre,
http://www.intelcenter.com

Warne, L., I. Ali, et al. (2004). The Network Centric Warrior: The Human Dimension of Network Centric Warfare. D. S. A. Division, Defence Science and Technology Organisation.

Welch, T. J. (1997). "Technology and Warfare," The Revolution in Military Affairs: Warfare in the Information Age.

Wendt, L. A. (2004). The Developmental Gap in Army Officer's Education and Training for the Future Force. U. S. Department of the Army. Fort Leavenworth, Kansas, School of Advanced Military Studies United States Army Command and General Staff College.

Wesensten, N. J. and G. Belenky (2005). "Cognitive Readiness in Network-Centric Operations," Parameters 2005(Spring).

White, A., S. O'hare, et al. (2005). "Digital Warrior: Blending Pedagogy and Game Technology," Proceedings of the Inter-service /Industry Training, Simulation, and Education Conference (I/ITSEC) 2004, University of Texas Institute for Advanced Technology.

Wisher, R. A. (2001). The Virtual Sand Table: Intelligent Tutoring for Field Artillery Training. Alexandria, VA, U.S. Army Research Institute for the Behavioural and Social Sciences.

Wisher, R. A. and T. M. Olsen (2003). The Effectiveness of Web-based Training, U.S. Army Research Institute for the Behavioural and Social Sciences.

Wisher, R. A., M. A. Sabol, et al. (2002). Distance Learning, the Soldiers Perspective, U.S. Army Research Institute.

Zipperer, E., G. Klein, et al. (2003). Training and Training Technology Issues for the Objective Force Warrior. T. W. G. International, U.S. Army Research Institute for the Behavioural and Social Sciences.