CANADIAN FORCES COLLEGE / COLLÈGE DES FORCES CANADIENNES

JCSP 34 / PCEMI N° 34

MDS RESEARCH PROJECT / PROJET DE RECHERChE MED

NETWORK CENTRIC WARFARE AND CHALLENGES FOR SMALL NATIONS.

By /par CDR Ståle Kasin, RNoN

This page intentionally left blank.

Abstract

Since the term Network Centric Warfare (NCW) was introduced by Cebrowski and Gartska in 1998, NCW has been explained to be one of our time's Revolution in Military Affairs (RMA). NCW brings along new technology and also a new way of organising warfighting by introducing separation of sensor, shooter and decision maker and connecting those three entities together in networks. NCW brings advantages and challenges for military use in addition to other challenges that comes when NCW technology is implemented within military organisations. A major advantage identified is shared situational awareness which there is both positive and negative experiences about based on the use of NCW technology today. A successful implementation of NCW requires that NCW is introduced from a top level and throughout the organisation.

The U.S. has been the leading nation both regarding development and use of NCW technology, while other nations are coming on using different kinds of approaches. This paper focuses on the challenges smaller nations face when implementing NCW. Norway is used as a typical example of a small nation, both when it comes to size of the military and the defence budget. Norway has expressed its ambition for implementation of NCW both when it comes to levels and timing for when it should be implemented. The challenges smaller nations meet when implementing NCW indicates that it will be a problem for Norway to meet its ambitions.

This page intentionally left blank.

This page intentionally left blank.

1 Introduction

A 'Google-search' on 'Network Centric Warfare (NCW)' gives 148.000 results, mainly articles and documents describing NCW, and a search at the Information Resource Centre at the Canadian Forces College reveals 79 books, reports and student papers. Most of the written material about the topic is strongly linked to what is going on about NCW in an American context, which is not a surprise since the idea of NCW was American, most of the theory about NCW is American and it is the U.S. Forces who so far has implemented and been the major user of NCW technology.[1] Without doubt the U.S. is the leading nation when it comes to development and implementation of NCW. However, several other countries are coming on, but none of them seems to be in the same 'league' as the leading nation. Other nations as the United Kingdom (UK), France, Germany and Australia have a more reluctant approach both to NCW itself and how it should be implemented in the armed forces.[2] Compared to the U.S., most other nations are 'small' in this context. This paper will focus on the challenges smaller nations face when implementing NCW and Norway will be used as an example of a typical small nation.

The term NCW is widely known, but other related terms is coming along. The UK names it Network Enabled Capability (NEC), NATO uses Network Centric Capability (NCC), France Info Centric Warfare (ICW), Australia Network Enabled Warfare, and

---

[1] Tim Fish, "NCW Development in Small Countries." *Asia - Pacific Defence Reporter* 32, no. 7 (Sep, 2006): 32.

[2] Fish, "NCW Development in Small Countries," 32.

Sweden calls it Network Based Defence (NBD).[3] The Netherlands uses the term Network Centric Operations (NCO) [4] which also has been introduced in other countries where NCO can be said to be a term describing use of NCW in military operations. Although the alternative terms show different perspectives of the approach to, the implementation of, and the use of NCW technology this paper will use NCW as a common term.

All the written material about NCW indicates that there is a big interest in this topic. Several nations have plans for implementation of NCW, even though they also struggle to get it done.[5] There may be several reasons for why countries are pursuing NCW as an answer to solving future challenges. One thing is to 'hang out with the U.S.' and be interoperable with the worlds largest military power in an alliance or coalition, but there are several other more rational reasons as well. Some of those reasons will be identified and put into the context of smaller countries challenges.

However, there are not only advantages, but also critical issues and challenges when introducing NCW technology. The most important challenges will be described followed by recent experience from use of NCW technology today. To give an example of the level of implementation in a small country the Norwegian inventory of NCW technology will be briefly described. NCW cannot be taken out of its context, but has to be seen within the user countries overall defence policy. How NCW is beginning to impact a nation's defence policy will be described using Norway as an example. Specific

---

[3] Yu E. Gorbachev, "Network Centric War: Myth Or Reality?" *Military Thought* 15, no. 1 (2006): 145.

[4] Doug Richardson, "Network-Centric Warfare: Revolution of Passing Fad?" *Armada International* 28, no. 5 (Oct/Nov 2004): 66.

[5] Fish, "NCW Development in Small Countries,"32.

NCW challenges for small nations will be discussed and finally the Norwegian level of ambition for NCW implementation will be analysed to see if a small nation like Norway will be able to reach its ambition for NCW implementation.

1.1 Thesis statement

Network Centric Warfare as a concept is adopted by several nations, such as the UK, Australia, France, Germany, Singapore, and Sweden among others.[6] Due to resources, the U.S. is leading the development, both technologically and operationally. Smaller nations like Norway have stated that NCW will be the basis for their future operations,[7] but there are many obstacles associated with the implementation of NCW which might have a more serious impact on smaller nations than larger nations.

This paper will give a description of NCW status today with focus on advantages and challenges related both to NCW itself, and the implementation of NCW. The main emphasis will be on the challenges faced by smaller nations in the implementation of NCW using Norway as an example. The purpose of this paper is to prove that Norway's ambition for implementation of NCW will be difficult to achieve within the given timeframe.

---

[6] Richardson, "Network-Centric Warfare . . .," 66.

[7] Forsvarsstaben, *Forsvarets Fellesoperative Doktrine* (Oslo: *FST Norge*, June 2007), 3.

2 What is Network Centric Warfare?

NCW is a topic that most people with a relationship to the defence or the armed forces has an opinion about. Whether it is officers, Non-Commissioned Officers, civilians working in the armed forces, defence politicians, or people working in the defence industry they will most probably be able to give their explanation about what NCW is. However, there are several misunderstandings of what NCW actually is and what kind of impact it will have on the armed forces around the world. In general it seems that most people have an optimistic view and that NCW will be able to solve a lot of problems and make war easier for those who have implemented NCW. Based on this, this chapter will give an introduction into the development of NCW, what it is and the intention behind NCW.

2.1 Origin of NCW

The article "Network-Centric Warfare - Its Origin and Future" by Vice Admiral Arthur K. Cebrowski and John J. Gartska is the foundation for understanding NCW. The two gentlemen have been called 'the fathers of NCW' and are referred to in most literature written about NCW. The article was published in January 1998, which gives a good indication of when the development of NCW started. According to Cebrowski and Gartska, the idea of NCW came in the middle of a Revolution in Military Affairs (RMA) ". . . *unlike any seen since the Napoleonic Age*."[8] They further state that NCW grow out of ongoing changes related to evolution of economics, information technology and business processes and organisations in the American society and that the changes are mainly linked to three themes:

---

[8] Cebrowski and Gartska, "Network-centric Warfare. . .," 29.

- The shift in focus from the platform to the network.
- The shift from viewing actors as independent to viewing them as part of a continuously adapting ecosystem.
- The importance of making strategic choices to adapt or even survive in such changing ecosystems.[9]

NCW principles has its origin in Information Technology (IT) used in modern commercial systems and Cebrowski and Gartska use Wal-Mart as an example of how network-centric operations are used as a retailing system.[10] Wal-Mart outperformed its competitors based on the use of information technology to keep track of the transactions within the stores and share this information directly with their suppliers in near real time. This made the central purchasing department superfluous and gave in addition better control of the transaction information.[11] To make such a system work efficiently there is a need for high-quality networks to enable the change from platform to network, and to increase speed and profitability in both sales and production partners have to be a part of the network instead of viewed as independent.[12]

Based on the use of network-centric operations within the retail industry, Cebrowski and Gartska argue that network-centric operations can deliver the same powerful dynamics to the military and in order to achieve this, the network requires:

> . . . an operational architecture with three critical elements: sensor grids and transaction (or engagement) grids hosted by a high-quality information backplane.[13]

---

[9] James F. Moore, T*he Death of Competition: Leadership and Strategy in the Age of Business Ecosystems*, Harperbusiness, 1996, quoted in Cebrowski and Gartska, "Network-centric Warfare. . .," 29.

[10] Cebrowski and Gartska, "Network-centric Warfare. . .," 29.

[11] *Ibid*., 30.

[12] *Ibid*., 31.

[13] Cebrowski and Gartska, "Network-centric Warfare. . .," 32.

IT has been used by the military all over the world for ages,[14] but it is the change in the use of the technology within the economical business and the ". . . *economics of information and the implication of these changes*" that have been the main motive power behind the development we see today.[15]

2.2 Definition of NCW

Alberts, Gartska and Stein defines in 'Network Centric Warfare: Developing and Leveraging Information Superiority' NCW as:

> … an information superiority-enabled concept of operation that generates increased combat power by networking sensors, decision makers, and shooters to achieve shared awareness, increased speed of command, higher tempo of operations, greater lethality, increased survivability, and a degree of self-synchronization. In essence, NCW translates information superiority into combat power by effectively linking knowledgeable entities in the battlespace.[16]

The authors further explain that:

> … the power of NCW is derived from the effective linking or networking of knowledgeable entities that are geographically or hierarchically dispersed. The networking of knowledgeable entities enables them to share information and collaborate to develop shared awareness, and also to collaborate with one another to achieve a degree of self-synchronisation.[17]

---

[14] Examples of such Information Technology are link systems for information exchange between units, e.g. Link 1 within the NATO Air Defence Ground Environment (NADGE) and Link 11 for maritime and air units, computerized message handling systems and computerized plotting systems for situational awareness. In addition several stand alone systems with applications for military use have been in service since the introduction of computers.

[15] David S Alberts and Richard E. Hayes. *Power to the Edge : Command, Control in the Information Age*, (Washington DC: CCRP Publication Series, 2004), 72.

[16] David S Alberts, John Garstka, and Frederick P. Stein, *Network Centric Warfare: Developing and Leveraging Information Superiority*, (Washington DC: CCRP Publication Series. 2nd (Rev.), 2000), 2.

[17] Alberts et al, *Network Centric Warfare . . .,* 6.

One of the most important differences from the traditional platform centric way of doing warfare is the separation of the combat power from the physical location of the battlespace assets by the concept of separating sensors, shooters and the command and control process. This again introduce the opportunity to focus on the 'massing of effects' instead of the traditional 'massing of forces'.[18] The traditional focus of militaries have been ". . . *manoeuvre, mass, surprise, firepower and logistics*" together with surprise, while in the 'Information Age' the focus is on the level of information.[19]

2.3 Separation of Sensor, C2, and Shooters

NCW introduces the concept of linking separate sensors with shooters, and move away from the traditional way that the shooter had its own sensor to give target data.[20] In addition is the decision making part, in military terms called command and control, is introduced as the third major part in the network. The sensors contribute to battlespace awareness and the shooters constitute the 'combat power', which can include both non-lethal and lethal means. The decision makers utilise the battlespace awareness provided by the sensors and other sources to command and coordinate the effects provided by the actors.[21]

The separation of sensor, command and control, and shooters introduces the need to link those functions in a network to be able to communicate and share information. Sharing battlespace awareness also requires the sensor entities to be linked together, not

---

[18] Alberts et al, *Network Centric Warfare . . .,* 90.

[19] David S Alberts. *Information Age Transformation* : *Getting to a 21st Century Military*, (Washington D.C.: CCRP Publication Series, 2002), 18.

[20] Alberts et al, *Network Centric Warfare . . .,* 92.

[21] *Ibid.,* 116.

necessarily linked to each other or in a single network but the information provided by the sensors must be provided in a manner so it is useful for other entities.[22] The shooters will not be linked together in the same way as the sensors, but will in general be linked to more battlespace entities than in traditional platform-centric operations. They will be linked to each other, to sensors or indirectly to sensors to have the possibility to get the necessary information and increase overall effectiveness.[23] Based on how the sensors and the shooters are linked implies that the decision makers have to be linked to both the sensors, shooters, and other decision makers, in order to be able to command and control the forces.[24]

In traditional platform-centric operations the platform has its own sensors and weapons. In NCW the shooters do not necessarily have their own sensors and decision makers not have their own shooters.[25] This leads to a more flexible approach to decision making where decisions are taken in support of command intent *". . . by a greater degree of freedom than normally associated with a traditional approach to command and control"*.[26]

2.4 Infostructure

To separate sensor, shooter and decision maker in NCW they have to be connected together in some sort of a communication network. Similarly ". . . *as in the*

---

[22] Alberts et al, *Network Centric Warfare . . .,* 118.

[23] *Ibid*., 119.

[24] *Ibid*., 119.

[25] *Ibid*., 120.

[26] Alberts, *Information Age Transformation . . .,* 9.

commercial sector, it [NCW] all begins with infostructure."[27] This infostructure must be able to give all the three roles access to the necessary information. [28] Alberts et al. defines 'infostructure' as:

> . . . a high-performance, communications, and computational capability providing access to appropriate information sources, and allowing seamless interactions among battlespace entities in a "plug and play" fashion. This is called the "infostructure."[29]

As implied in this definition, the infostructure is more than the communication network itself. It also includes a computational capability to compile the information and also the capability for a seamless interaction between the battlespace entities (sensor, shooter and decision maker. Based on how 'easy' 'Plug and play' function on personal computers, it will probably not be easier when it comes to 'plug and play' of battlespace entities. Challenges related to this, e.g. interoperability, will be described later.

The network itself can be organised in different ways, e.g. common networks or separate networks based on what kind of information they provide. Separate network is using separate protocols especially suited for that network's purpose and are able to provide more near real-time data and a higher quality of service, i.e. they are used to speed up the information exchange process.[30] Common networks using the Transmission Control Protocol/Internet Protocol (TCP/IP) networking technology have traditionally not given the necessary quality of transaction for military purposes. However, technology to

---

[27] Alberts et al, *Network Centric Warfare . . .,* 88.

[28] *Ibid*., 187.

[29] *Ibid*., 116.

[30] *Ibid*., 190.

solve the TCP/IP network issue is now available and such networks are becoming more common. Even though technology has evolved to solve these problems there will still be a need for separate networks when there are security requirements and technological limitations hampering the use of common TCP/IP based networks.[31]

2.5 The different domains

In its full mature form NCW consist of three domains of warfare: physical domain, information domain and cognitive domain. There are interactions between the domains, and networking is involved within all the domains.[32] When looking at NCW from a domain perspective it becomes clear that it is important that the force must be able to exchange information between and across the three domains to be able to ". . . *achieve synchronized effects in each of these domains."*[33]

The physical domain is where the influence and effects of military power takes place within the environments of land, air, sea and space.[34] Within the physical domain the elements of the force are ". . . *robustly networked achieving secure and seamless connectivity and interoperability."* [35]

As indicated by the name the information domain is where the information is created, processed and distributed. Within the information domain the information is communicated among the entities, i.e. information among warfighters, command and

---

[31] Alberts et al, *Network Centric Warfare . . .,* 190-191.

[32] David S Alberts, *Understanding Information Age Warfare*, (Washington DC: CCRP Publication Series, 2001, 57.

[33] Alberts, *Understanding Information Age Warfare*, 58.

[34] *Ibid*., 12.

[35] *Ibid*., 57.

control information and communication of higher commands intend.[36] A simple way to understand the information domain is just to say that this is where we communicate with others.[37] And since information is the major issue within NCW the information domain must be protected and defended. [38]

Compared to the two other domains the cognitive domain is more abstract as it is in the minds of the 'players' within the networks. Within the cognitive domain the 'players' ". . . *perceptions, awareness, understanding, beliefs, and values reside"* [39] and consequently it is in this domain that decisions are made. According to Alberts, this domain is made of human aspects:

> . . . leadership, morale, unit cohesion, level of training and experience, situational awareness, and public opinion. This is the domain where an understanding of commander's intent, doctrine, tactics, techniques, and procedures reside.[40]

In addition to these three domains, Alberts et al later introduced the 'social domain' in 'Power To The Edge' and defined it as a ". . . *set of interactions between and among force entities*." [41] The social domain is where processes and interactions between individuals and entities defining organisations and doctrines exist.[42] Simplified, the social domain contains the processes and interactions that do not fit into the other domains.

---

[36] Alberts, *Understanding Information Age Warfare*, 12.

[37] *Ibid*., 12.

[38] *Ibid*., 12.

[39] *Ibid*., 13.

[40] *Ibid*., 13.

[41] Alberts and Hayes, *Power to the Edge . . .,* 113.

[42] *Ibid*., 15.

2.6 Network Grids

The network grids are composed of nodes consisting of sensors, shooters or decision makers connected together. There are three separate grids; the information grid, sensor grid and shooter grid.

The information grid is an important part to make NCW effective as it provides a mean to get target information to the shooter.[43] In other words, the information grid is the infrastructure for communication and computing and is the ". . . *means to receive, process, transport, store, and protect information for the Joint and combined forces*." [44] It is a ". . . *physical permanent grid*" present in all elements taking part in the network while it also should provide the possibility to 'plug and play' sensors and shooters.[45] A well functioning information grid is important to achieve good situational awareness.[46]

As the name indicates the sensor grid consists of sensors. All types of sensors can be included, regardless of environment[47] or type of sensor.[48] The aim of the sensor grid is to generate information on the battlespace. The sensors are physical, but the sensor grid is not permanent. It is established for the task and then makes the sensors interrelated.[49] Alberts et al summarize this as follows: *"Sensor networks provide the warfighting force*

---

[43] Walt L. Perry, *Network-Based Operations for the Swedish Defence Forces : An Assessment Methodology*, (Santa Monica, CA: Rand Corporation, 2004), 14.

[44] Fred P. Stein, "*Observations on the Emergence of Network Centric Warfare"*, http://www.dodccrp.org/files/stein_observations/steinncw.htm; Internet; accessed 2 March 2008.

[45] Stein, "*Observations on the Emergence of Network Centric Warfare."*

[46] Perry, *Network-Based Operations for the Swedish Defence Forces . . .,* 13.

[47] Air, sea, land, or space.

[48] For example dedicated sensors, sensors based on a weapon platform, sensors carried by individual soldiers etc.

[49] Stein, "*Observations on the Emergence of Network Centric Warfare*."

with the operational capability to synchronize battlespace awareness with military operations."[50]

The shooter grid is similar to the sensor grid because the shooters themselves are physical but the grid is virtual, dynamic and in place for a task. The main purpose of the shooter grid is to enable the decision maker to plan and execute operations to achieve the necessary effect on the battlefield and then retask the shooters as necessary.[51] The shooter grid is also called 'The Engagement-Decision-Shooter-Grid' because it involves both the decision maker and the shooter. The sensors are also included in this grid because the shooter needs sensor data.[52]

2.7 Tenets of NCW

There are four basic tenets of NCW that provides the foundation for a value chain describing the different levels and complexity of NCW.[53] A prerequisite for the tenets involves that information is available at all levels within the organisation and that there is a change in the relationships among participants and the traditional military hierarchy.[54] The tenets of NCW can also be used to explain and define the cause-effect relationships:[55]

- A robustly networked force improves information sharing
- Information sharing and collaboration enhances quality of information and shared situational awareness.

---

[50] Alberts et al, *Network Centric Warfare . . .,* 152.

[51] Stein, "*Observations on the Emergence of Network Centric Warfare*."

[52] Perry, *Network-Based Operations for the Swedish Defence Forces . . .,* 13.

[53] Alberts and Hayes, *Power to the Edge . . .,* 99.

[54] Alberts, *Information Age Transformation . . .,* 8.

[55] *Ibid*., 97.

- Shared situational awareness enables collaboration and self-synchronisation.
- These, in turn, dramatically increase mission effectiveness.[56]

2.8 Increased tempo (speed of command)

One of the principles in military operation is to speed up the decision making process. This principle is an important foundation of John Boyd's theory which produced the 'observe, orient, decide, act (OODA) loop'.[57] One of the key elements to speed up the process is to get better access to information. Another way of looking at getting advantages is to ". . . *capitalize on one's own strengths while exploiting the weaknesses of adversaries."* [58] Information can be a strength and traditionally it has always been a challenge to get enough and good information for the decision maker to be able to make timely decisions. The introduction of NCW will make this easier as NCW introduces the ability to collect and process a lot of information that can be used by the decision makers to make decisions.[59]

One of the principles used to achieve increased tempo is self-synchronisation which is an interaction between two or more entities outside of the traditional hierarchy of command and control.[60] To be able to achieve self-synchronisation a rule set describing the desired outcome and the shared awareness is necessary.[61] Self-

---

[56] Alberts, *Information Age Transformation . . .,* 7-8.

[57] Forsvarsstaben, *Forsvarets Fellesoperative Doktrine*, 80.

[58] Alberts, *Understanding Information Age Warfare*, 208.

[59] Alberts et al, *Network Centric Warfare . . .,* 88.

[60] *Ibid.,* 175.

[61] *Ibid*., 175-176.

synchronisation will contribute to speed up the process so that effects may be utilised before the enemy can react.[62] Alberts and Hayes sum up the results as follows:

- Clear and consistent understanding of command intent;
- high quality information and shared situational awareness;
- competence at all levels of the force; and
- trust in the information, subordinates, superiors, peers, and equipment.[63]

Synchronisation occurs between entities within different places, layers, etc within the hierarchy. Alberts states that there are three types of self-synchronisation: First, in the physical domain because it involves human beings with ideas and concepts in their heads which has to be transformed and used in the real world together with available information. This requires "*. . . fusing the cognitive, information, and physical domains."*[64] Second, a command and control concept to provide the guidance and flexibility for the specific situation is required.[65] Third, it involves both horizontal and vertical harmonisation within an organisation. Vertical harmonisation within the organisation is necessary to achieve that decisions at the lower levels are consistent with higher levels goals. Horizontal harmonisation is required to synchronise the different actors at the same level within the organisation. [66] Finally, the application of the force elements should be synchronised to achieve a more synergistic type of operation.[67]

---

[62] Alberts, *Understanding Information Age Warfare*, 208-210.

[63] Alberts and Hayes, *Power to the Edge . . .,* 27.

[64] Alberts, *Understanding Information Age Warfare*, 206.

[65] *Ibid*, 206.

[66] Alberts, *Understanding Information Age Warfare*, 207.

[67] *Ibid*., 211.

However, it is important to notice as said by Alberts and Hayes that self-synchronisation is not the only way the forces in the Information Age will operate.[68]

2.9 Organisational behaviour

The introduction of NCW will impact all levels within the organisation as it contributes to all three levels of war; tactical, operational and strategic.[69] To be able to successfully implement and utilise NCW the focus within the military should not only be on the technological part, but also emphasise NCW's implication on organisational issues and how to utilise NCW within operations.[70] This was stressed by the U.S. Secretary of Defence Donald Rumsfeld in his speech to the National Defence University students 31 January 2002:

> A revolution in military affairs is about more than building new high-tech weapons, though that is certainly part of it. It's also about new ways of thinking, and new ways of fighting.[71]

This fact is also recognised in the latest Defence Study carried out by the Norwegian Chief of Defence (CHOD), which states that the major challenge with the increased focus on NCW will be the traditional hierarchical military organisation, traditional ways of leadership, established knowledge, culture, ways of communication, and tempo. A

---

[68] Alberts and Hayes, *Power to the Edge . . .,* 27.

[69] Alberts et al, *Network Centric Warfare . . .,* 88.

[70] *Ibid.,* 88.

[71] CNN.com, "Rumsfeld presses for more agile military," *CNN.com*, 31 January 2002, http://archives.cnn.com/2002/US/01/31/rumsfeld.speech; Internet ; Accessed 2 March 2008.

development of both the NAF and the leaders is required to be able to exploit the opportunities given by NCW.[72]

2.10 What is Network Centric Warfare? – Conclusion

This chapter has given a brief introduction and overview of NCW from its origin and definition as well as NCW characteristics such as separation of sensor, decision maker and shooter, the network grids and the domains. NCW technology and the intention behind makes the basis for understanding both the military advantages and the critical issues and challenges discussed later. The impact on the organisations has also been touched as this is an important issue when introducing new and even revolutionary technology into the military. The complexity of NCW is emphasised as this is an important issue when such technology is introduced in smaller countries with limited resources.

---

[72] Forsvarsstaben, *Forsvarssjefens Forsvarsstudie 2007 Sluttrapport* (Oslo: FST Norge, October 2007), 64.

3 Military advantages

NCW is basically about networking entities in the battlespace and distribute the information they collect, produce or may use.[73] From a military point of view the " . . . *increased content, quality, and timeliness of information"* within the network gives advantages for military use.[74] Some of the most important advantages will be discussed in this chapter. They are selected based on a mixture of both the theoretical approach to NCW and practical examples from case studies and experiences in use of NCW technology. The advantages will be discussed keeping the tenets of NCW presented in paragraph *2.7 Tenets of NCW* in mind as the tenets are describing the 'NCW value chain'. The advantages discussed are: situational awareness, reduced sensor-to-shooter time, tempo and responsiveness, command and control, developments of tactics, mission effectiveness, economy of force and logistics, and the relationship between them. The advantages discussed will give an understanding of why several countries are pursuing and implementing NCW technology in today's military.

3.1 Situational awareness

The networking of sensors, near real-time sharing of information and presentation of information gives a force the capability for an increased situational awareness including increased quality of the information.[75] Gonzales et al. defines situational awareness as:

---

[73] Alberts et al, *Network Centric Warfare . . .,* 94.

[74] *Ibid*., 100.

[75] John B Tisserand III, *Network Centric Warfare Case Study - U.S. V Corps and 3rd Infantry Division (mechanized) during operation Iraqi Freedom combat operations (mar-apr 2003) Volume III: Network Centric Warfare insights*, Report Prepared for the Office of Force Transformation in the Office of the Secretary of Defense, (Pennsylvania, Carlisle barracks: U.S. Army war college, August 2006), 1.

> A comprehensive view of the battlespace that includes mission constraints; environment; time-space relationships; the capabilities and intentions of Red, Blue, and neutral forces; and an assessment of the associated uncertainties.[76]

The U.S. Army Stryker brigade (SBCT) both utilises NCW technology and has an organisational structure designed to exploit the advantages of NCW technology.[77] The SBCT is networked using satellite communications and different other communication means and has their own combat system, the Stryker brigade battle command system (SBBCS) integrating several independent command and control and battle management systems.[78] A case study comparing the SBCT with a traditional infantry brigade concluded that the "*Quality of individual and shared information*"[79] for SBCT was 80% while it for a traditional infantry brigade was 10%.[80] In other words, the use of NCW led to an enormous enhancement in situational awareness. The SBCT was prepared for NCW both with regard to technology and organisation, but even use of relatively simple stand-alone systems like the Blue Force Tracker (BFT) tracking own forces contributes by its rapid information sharing and improved quality of information to increased situational awareness.[81]

---

[76] David Gonzales et al, *Network Centric Operations Case Study – The Stryker Brigade Combat Team*, Report Prepared for the Office of Force Transformation in the Office of the Secretary of Defense, (Santa Monica: RAND Corporation, 2005), 116.

[77] Gonzales et al, *Network Centric Operations Case Study – The Stryker . . .,* xiii.

[78] *Network-Centric Operations Case Study - The Stryker Brigade Combat Team ARBRIDGED REPORT Version 1.0*, Report Prepared for the Office of Force Transformation in the Office of the Secretary of Defense, August 2007, 5.

[79] "Quality of situational awareness information" is defined as the percentage of actual enemy, neutral, and friendly forces that are correctly identified and accurately located by the commanders and soldiers or by their information system in each unit.

[80] Gonzales et al, *Network Centric Operations Case Study – The Stryker . . .,* 105.

[81] Tisserand , *Network Centric Warfare Case Study - U.S. V Corps . . .,* 2.

Enhanced situational awareness is possible to achieve by the use of NCW technology, and it seems to be further enhanced if the organisation also is designed around the use of such technology. The enhanced situational awareness itself gives other advantages such as improved and quicker decision making, reduced sensor-to-shooter time, improved tactics and by this increased effectiveness.[82]

3.2 Reduced sensor-to-shooter time

There are units today that already have short sensor to shooter time, e.g. naval vessel tracking a target with a sensor and simultaneously engaging the target with the gun. In other situations the sensor and the shooter may be separated and one of the benefits by NCW is that it enables a reduction in the time used for information exchange when a sensor is giving target data to a shooter. This is especially true in situations where the sensor data needs to be interpreted and analysed before the target can be attacked. In such situations NCW provides the ability to let the shooters themselves do the analysis of sensor data before they carry out the attack.[83] Further, information from several sensors is available and possible to synthesise, which produce more accurate track information that again permits more accurate engagements.[84]

The advantage given by reduced sensor-to-shooter time is the key to time-sensitive-targeting (TST) because this targeting process is working with 'immediate' as

---

[82] Gonzales et al, *Network Centric Operations Case Study – The Stryker . . .,* xxx-xxxi.

[83] Alberts et al, *Network Centric Warfare . . .,* 184.

[84] *Ibid.,* 142.

opposed to 'deliberate' targets which normally permit longer planning time.[85] The US Joint Doctrine 3-60 defines time-sensitive target as:

> A joint force commander designated target requiring immediate response because it is a highly lucrative, fleeting target of opportunity or it poses (or will soon pose) a danger to friendly forces.[86]

TST needs to be an integral part of the planning process and is dependent on that the flow of data from sensor to shooter is streamlined.[87] NCW technology reduces this time and this is already tested out by the U.S. Navy using their Naval Fires Network (NFN) based on the Tactical Exploitation System (TES). TES was originally developed for the U.S. Army to get access to sensor data, but the Navy has extended it to do real-time targeting by further compressing the sensor-to-shooter time.[88] Another example of successful use of NCW technology to achieve TST is the attack on Saddam Hussein and his sons April 17, 2003 where the U.S. forces were able to drop four 2000-lb Joint Direct Attack Munitions (JDAMs) 12 minutes after the location of the Hussein family members was obtained.[89] The advantage of NCW for time-sensitive-targeting is also emphasised in the NCW case study of the U.S. V Corps and Third Infantry Division during Operation Iraqi Freedom (OIF) saying:

---

[85] Ted McKenna, "Right on Time." *Journal of Electronic Defense* 28, no. 4 (Apr 2005): 44.

[86] United States. Joint Chiefs of Staff. "*Joint Targeting. Jp 3-60*". Vol. 3-60. Washington, DC: Joint Chiefs of Staff, 2007, GL 14.

[87] Kernan Chaisson, "MNF Addresses Time-Critical Targeting." *Journal of Electronic Defense* 24, no. 5 (May 2001), 16.

[88] "Navy Adds Component to Network Centric Warfare Plan." *Defense Daily* 211, no. 3 (Jul 5, 2001), 1.

[89] McKenna, "Right on Time," 44.

> . . . the new information systems increased the level of situational awareness and were especially key in the rapid coordination and execution of strategically important time-sensitive targets.[90]

3.3 Tempo and responsiveness

Proponents of NCW often use increased tempo as an argument when they describe advantages of NCW and they are undoubtedly right in their assumptions. NCW is in its nature prepared for increased tempo simply because 'everybody' is supposed to be in the same network, get the same information and sensor data will be provided to those who need it. Self-synchronisation is one way to achieve increased tempo and is gained by ". . . *improved quality of information, information sharing, shared situational awareness, and collaboration.*"[91] However, even without self-synchronisation increased tempo and responsiveness are possible. Shared situational awareness by having a Common Operational Picture (COP) in itself contributes to increased tempo and responsiveness simply because everybody has a common understanding of the situation.[92] Improved sensors provide better and more reliable sensor data and contribute to increased responsiveness by reducing the time to analyse the sensor data and by providing more accurate target data.[93]

Even the time used for morning briefs can be reduced. The US Task Force 50 reduced the time spent on morning briefs from 1-2 hours to 30-45 minutes because ". . .

---

[90] Tisserand, *Network Centric Warfare Case Study - U.S. V Corps . . .,* 15.

[91] *Ibid. ,* 3.

[92] Gonzales et al, *Network Centric Operations Case Study – The Stryker . . .,* 96.

[93] Tisserand, *Network Centric Warfare Case Study - U.S. V Corps . . .,* 10.

all relevant personnel were able to access continually updated information" and stayed updated on the situation.[94]

In addition NCW technology reduce the time needed for planning and the traditional distribution of detailed paper orders as this can be done electronically and even more visually based than the traditional written word.[95] The higher operational tempo provided by use of NCW technology gives more responsive forces and force agility,[96] which again gives increased mission effectiveness.[97]

3.4 Command and Control

Based on the facts already discussed above, it is clear that NCW also has the opportunity to improve command and control as there are several of the factors that directly influence how command and control is performed. Shared situational awareness simplifies command and control because there is already a common understanding between the commander giving the order and the subordinate receiving the order.[98] The enhanced situational awareness also simplifies and enhances the commander's assessment and contributes to more timely decisions.[99] The use of NCW technology to network the battlespace entities together ". . . *facilitates the flow of battle command*. .

---

[94] *Network-Centric Operations Case Study - Task Force 50 During Operation ENDURING FREEDOM ARBRIDGED REPORT Version 1*.0, Report Prepared for the Office of Force Transformation in the Office of the Secretary of Defense, March 2006, 2.

[95] Gonzales et al, *Network Centric Operations Case Study – The Stryker. . .,* 95.

[96] Tisserand, *Network Centric Warfare Case Study - U.S. V Corps . . .,* 11.

[97] *Ibid. ,* 113.

[98] Gonzales et al, *Network Centric Operations Case Study – The Stryker. . .,* 76.

[99] Tisserand, *Network Centric Warfare Case Study - U.S. V Corps . . .,* 14.

."[100] and changes the ". . . *way it sent orders and operational graphics to its subordinate teams*."[101] The possibilities to communicate by combining both transmission of graphics and 'written words' electronically simplifies the command and control process and to a greater extend ensure a better and common understanding of the orders transmitted. Graphics in form of digital overlays also improve the understanding of orders and contribute to the speed of command. As said by Gonzales et al: "*These pictures help make sense of the commander's words, presumably faster*."[102]

3.5 Development of tactics

In order to fully utilise NCW, tactics has to be developed and adapted to the benefits NCW gives. One example already developed and utilised by U.S. Army in OIF is the 'Swarm tactics' which give several benefits: a widely dispersed formation that makes it harder for an enemy to attack effectively, the combat units can cover more ground because they do not have to be in a close formation, the fact that all units know the location of friendly units because of the use of NCW technology reduces fratricide during operations and finally swarming can make it possible to attack directly the enemy command structure instead of just operate in the periphery. Since these benefits give a more effective and more controllable organisation this tactic may also lead to the need for fewer troops and less equipment.[103] Similarly did the 101st Airborne develop new tactics involving ". . . *close coordination between ground forces and [Combat Air Support] CAS"*

---

[100] Tisserand, *Network Centric Warfare Case Study - U.S. V Corps . . .,* 44.

[101] *Ibid. ,* 50.

[102] Gonzales et al, *Network Centric Operations Case Study – The Stryker. . .,* 92.

[103] Clay Wilson, *CRS Report RL32411 Network Centric Operations: Background And Oversight Issues For Congress*, Report Prepared for the U.S. Congress, 2 June 2004, CRS-7.

because of the increased situational awareness provided by its use of the Force XXI Battle Command Brigade and Below/Blue Force Tracker (FBCB2/BFT).[104]

Another example is the introduction of Link-16 in U.S. Air Force fighter aircrafts.[105] Link-16 improved the pilot's situational awareness which again enabled development of their tactics: first they achieved higher number of engagements within a given timeframe because the pilots could ". . . *quickly recognise the most efficient attack trajectories*"[106] second they achieved a better employment of the wingman as combatant instead of just being a patroller because of a ". . . *shared understanding of the engagement*,"[107] third they were able to use other planes' track information allowing the possibility to ". . . *enter an engagement from a position of maximum advantage*," [108] and finally they were able to use "ambush" combat air patrols (CAPs) and the terrain to trap and destroy enemy aircrafts because all friendly aircraft's ". . . *locations are known by all friendly fighter pilots*." [109] The Royal Air Force had similar success with the introduction of Link-16. Their U.K. 29 Squadron fitted with Link-16 increased their kill ratio over the

---

[104] *Network-Centric Operations Case Study - Coalition Operations in Operation IRAQI FREEDOM (OIF): U.K. Perspective of FBCB2/Blue Force Tracker (BFT)*, Report Prepared for the Office of Force Transformation in the Office of the Secretary of Defense, 16.

[105] David Gonzales et al, *Network-Centric Operations Case Study - Air-to-Air Combat With and Without Link 16*, Report Prepared for the Office of Force Transformation in the Office of the Secretary of Defense, (Santa Monica: RAND Corporation, 2005), xv.

[106] Gonzales et al, *Network-Centric Operations Case Study - Air-to-Air . . .,* xxvi.

[107] *Ibid*., xxvii.

[108] *Ibid*., xxviii.

[109] *Ibid*., xxviii.

fighters equipped only with voice communication with approximately 4-to-1 because of improved tactics.[110]

3.6 Mission effectiveness

The ability to achieve mission effectiveness is closely linked to the advantages discussed above and the interrelation between those.[111] The Stryker Brigade case study uses four measures to decide mission effectiveness: "*Quality of individual and shared information, speed of command, ability to control the speed of command and Blue:red casualty ratio."* [112] The conclusion is that the networked SBCT had a much better mission effectiveness than a traditional light infantry brigade. In addition to the quality of shared situational awareness mentioned above, the speed of command for SBCT was 3 hours while the traditional infantry brigade was 48 hours. Further SBCT had the ability to control the speed of command and the Blue:red ratio was 1:1 compared to the traditional organisation's 10:1.[113]

Similarly does the case study of "*Air-to-air Combat With and Without Link 16*" conclude that:

> . . . the robustly networked force enabled by Link 16 improved information sharing and the resulting quality of information, which enhanced shared situational awareness, which in turn enabled self-synchronization and which resulted in dramatically increased mission effectiveness as measured by the kill ratios.[114]

---

[110] John J. Garstka, "*Network-Centric Warfare Offers Warfighting Advantage*." *Signal* 57, no. 9 (May, 2003): 58.

[111] Gonzales et al, *Network Centric Operations Case Study – The Stryker. . .,* 9.

[112] *Ibid*., 105.

[113] *Ibid*., 105.

[114] Gonzales et al, *Network-Centric Operations Case Study - Air-to-Air . . .,* 76.

Also within the maritime environment is the mission effectiveness enhanced by enhanced awareness and communication.[115] Task Force 50 (TF 50) achieved increased situational awareness by ". . . *networked information systems, sensors, and extended connectivity*" which together with increased ". . . *collaboration, audacity and synchronisation"* enhanced combat effectiveness to a level not previously possible.[116]

3.7 Economy of force

Based on the fact that military forces are expensive both to equip, educate and operate there is always a desire to reduce the necessary force to a minimum. 'Economy of force' is also one of the 'Principles of war' where the aim is to conduct a mission or a task with the least amount of resources as possible in order to be able to save resources for other missions or tasks later.[117] NCW provides increased mission effectiveness and it will be possible within NCW to have smaller-size units reducing both manpower and supplies without reducing the ability to effectively accomplish the mission.[118]

3.8 Logistics

Logistics is also an area that might benefit from NCW because of military logistics similarity to civilian logistics and the technological development and use of information technology within civilian logistics.[119] NCW technology enables logistics information of subordinate units to be automatically forwarded as status messages.[120]

---

[115] *Network-Centric Operations Case Study - Task Force 50 . . .,* 15.

[116] Tisserand, *Network Centric Warfare Case Study - U.S. V Corps . . .,* 9.

[117] Joint Chiefs of Staff, *Joint Operations*. JP 3-0. Vol. 3.0. (Washington DC: The Joint Chiefs of Staff, 2006), II-2.

[118] Wilson, *Network Centric Operations: Background And Oversight Issues . . .,* CRS-5.

[119] Forsvarsstaben, *Forsvarssjefens Forsvarsstudie . . .,* 40.

[120] Gonzales et al, *Network Centric Operations Case Study – The Stryker . . .,* 90.

Keeping the logistics service informed early has a significant impact on their ability to sustain combat forces and by that increased mission effectiveness.[121] For example can consumption of fuel and ammunition in vehicles, ships and aircrafts be collected in real time and combined with a rule-set to decide re-supply, prioritising the use of the assets and/or other actions necessary.[122] Such technology is available and already in civilian use which indicates that NCW principles within logistics can probably be introduced in short time.[123]

3.9 Military advantages - Conclusion

The military advantages discussed in this chapter can be linked directly back to the 'Tenets of NCW' described in paragraph *2.7 Tenets of NCW*. NCW is providing shared situational awareness, which again has enabled collaboration and self synchronisation exemplified by increased tempo, reduced sensor-to-shooter time, command and control and improved tactics to utilise the other advantages. The 'Tenets of NCW' proves to be true when compared to use and findings of NCW technology today. Even though the advantages are based mainly on American theory and use of NCW technology, the advantages are also interesting for smaller nations. Increased mission effectiveness with better economy of force is tempting when trying to keep an efficient military with limited resources. The challenge is to balance the advantages with the disadvantages.

---

[121] Tisserand, *Network Centric Warfare Case Study - U.S. V Corps . . .,* 94.

[122] Alberts et al, *Network Centric Warfare . . .,* 177.

[123] Forsvarsstaben, *Forsvarssjefens Forsvarsstudie . . .,* 40.

4 Critical issues and challenges

As always during development and implementation of a new type of technology there are challenges, and there are not exceptions for NCW. NCW is complex, and has probably a wider impact than what is the fact during traditional change in technology. The complexity of NCW even results in some interesting points of view as some of the advantages also can transfer into challenges, e.g. information. Much information is good, but too much information can be bad. Similarly may mission effectiveness lead to overreliance of the same effectiveness. As with advantages it is not intended to make a complete list of the challenges, but give examples of some of the most important ones.

4.1 Overconfidence about the effectiveness

Everybody is talking about and have an opinion about NCW, even though most people only have scratched the surface of the issue and do not have a sound understanding of neither what it is, the implementation challenges, nor what it can provide. It is fair to say that this lack of knowledge is present also within organisations planning future forces and operations. There is a danger that wrong assumptions are made about the benefits of NCW and that this can lead to a reduction in the forces because misinterpretations and misunderstandings of what NCW is all about.[124] Similarly there is a danger that the NCW advocates are able to argue for constructing forces to prepare for a war suitable for NCW instead of planning for wars that are more likely to be fought.[125]

So far information itself has been said to be the key to success, better target data availability and better shared situational awareness are among the benefits presented as a

---

[124] Wilson, *Network Centric Operations: Background And Oversight Issues . . .*, CRS-7.

[125] *Ibid*., CRS-8.

consequence of increased and better information sharing. However, there is a danger that incomplete information may not necessarily give the correct picture of the situation. NCW bases much of its information collection on sensors and a situational awareness solely based on sensors may not reflect the operational reality.[126]

4.2 Overreliance on information

One of the important concepts of NCW is to be able to collect, contain and distribute information to the entities within the network. The information is presented basically visually on screens using symbols with colour codes. It is easy for those who see the 'information' to believe that this is the truth, even though it might not be real-time data that is presented.[127] This fact has now started to be looked into by analysts and critics who state that the amount of information within NCW may be overestimated as an asset and that one should be careful in basing important military decision only on the information available within an NCW system.[128] Even though it is agreed that information is important in military operations there is not done enough to reduce the risk "*. . . associated with data-dependent military doctrine.*"[129]

---

[126] Wilson, *Network Centric Operations: Background And Oversight Issues . . .,* CRS-7- CRS-8.

[127] This is based on personal experience from an old Norwegian naval system where data presented could be as old as hours and people looking at the screen still thought it presented the real situation.

128 Martin Burke, *Information Superiority Is Insufficient To Win In Network Centric Warfare,* Joint Systems Branch, Defense Science and Technology Organization, 2001, http://www.dodccrp.org/events/2000/5th_ICCRTS/cd/papers/Track4/024.pdf: Internet; Accessed 12 March 2008.

[129] Michael Schrage, *Perfect Information and Perverse Incentives: Costs and Consequences of Transformation and Transparency*, Security Studies Program Working Paper, (Boston: Massachusetts Institute of Technology, E38-600, May 2003), 15.

4.3 Management of information overload

There is a real danger of information overload and focus has to be put on that it is actual information that both is provided and extracted.[130] This is especially important when it comes to information needed in the decision-making process.[131] Research is underway to reduce the problem of information overload; one way of solving the problem is the 'post and smart pull approach' where those who need information can pull out what they need instead of the traditional approach where everybody gets what is 'in the system'.[132] The move from 'push' to 'post and smart pull' implies that the information owner does not have to identify who should get the information. The 'problem' is instead transferred to those who need information to identify what they need and where to get it. Even though this does not seem to be a better solution, it is easier for those who need information to determine what they need than for the information owner or producer.[133] The 'smart pull' is in general built up in the same way as the 'world wide web' where the users can pull out the information they need.

4.4 Increasing complexity of military systems

There is a continuous development of technology in society in general and the technology, both hardware and software, is becoming more and more complex, e.g. the lines of computer code in Microsoft Word increased from 27.000 in 1982 to 2 million lines in the 1995 version.[134] There are no exceptions for military systems in this

---

[130] Alberts et al, *Network Centric Warfare . . .,* 108.

[131] Wilson, *Network Centric Operations: Background And Oversight Issues . . .,* CRS-10.

[132] Alberts and Hayes, *Power to the Edge . . .,* 81-82.

[133] *Ibid*., 82.

[134] Stewart Brand, "The Physicist", *Wired*, Sep 1995. http://www.wired.com/wired/archive/3.09/myhrvold.html; Internet; Accessed 4 April 2008.

development and the U.S. Army's 'Army Future Combat System' has tripled its lines of computer code from the initial calculations in 2003 to the estimated number of 95.1 million lines of computer code in March 2008, and it is assumed that the number will increase even more in the future.[135] Other military systems like the Blue Force Tracking system has 3 million lines of computer code,[136] while civilian relatively complex systems like Microsoft's newest operating system Windows Vista has 50 million lines of code.[137]

Architectural challenges not experienced before will also be more common since the use of stand-alone systems will be reduced and everybody will be tied together in a network.[138] The technological evolution makes it difficult for the operators and technicians to have full knowledge of the system. Since the system again is connected to other systems and a part of a whole 'system of systems', problems in one part may transfer to other systems within the whole and create severe problems not intended in the first place. The problems can be caused both by the users and automated components and is even a problem that can be exploited by adversaries.[139] In a NCW system where the

---

[135] Bob Brewin, "GAO: Future Combat Systems network still more concept than reality," *Government Executive* (March 2008). http://www.govexec.com/dailyfed/0308/0310008nn1.htm; Internet; accessed 4 April 2008.

[136] Matthew French and Frank Tiboni, "Tracking troop movement," *Federal Computer Week* (March 21 2004). http://www.fcw.com/print/10_7/mews/82386-1.html; Internet; accessed 4 April 2008.

[137] Stephen Manes, "Dim Vista," *Forbes* 179, no. 4, Feb 26, 2007, 50.

[138] Wilson, *Network Centric Operations: Background And Oversight Issues . . .,* CRS-10- CRS-11.

[139] *Ibid*., CRS-11.

entities are connected in a network the problem gets even bigger as the "*The frequency of normal accidents increases with the degree of coupling in systems.*"[140]

4.5 Vulnerability of military software and data

As military systems contain information that might be of interest for an adversary there is a continuous threat to military computers by attack from hackers and others who would like to get the information or just make trouble.[141] This leads to a discussion about whether commercial or bespoke systems should be used in military systems as systems based on commercial computers might be more vulnerable. In addition to the discussion about the hardware system there is probably more concern about the software, especially when open-source software is less expensive and in general more reliable than proprietary software. For government organisations and decision makers reduced cost and reliability, which again reduces maintenance cost, are advantages that might have strong impact on their decision.[142] From a security point of view there might be problems with open-source software as it is easier for an eventual adversary to get some malicious code inserted secretly which may cause malfunction of the system. However, other experts again argue that since open-source software, e.g. Linux which is widely used in military systems, are reviewed by programmers all over the world it cannot easily be compromised as it will be quickly discovered. [143]

---

[140] David Fisher and Dennis Smith, "Emergent Issues in Interoperability," *News@ SEI*, 2004, No.3. http://www.sei.cmu.edu/news-at-sei/columns/eye-on-integration/2004/3/eye-on-integration-2004-3.htm; Internet; Accessed 24 March 2008.

[141] Wilson, *Network Centric Operations: Background And Oversight Issues . . .,* CRS-12.

[142] *Ibid*., CRS-13.

[143] *Ibid*., CRS-13.

4.6 Vulnerability of military equipment to electronic warfare

Electronic equipment is vulnerable to electronic warfare attacks. One possible type of attack is use of Electromagnetic Pulse (EMP), which is caused by an intense energy field that can disrupt sensitive electronically system, e.g. microcircuits.[144] However, such an attack will also hamper the attacker's use of electronically system if he is within the energy field. Another way to disrupt NCW is traditional electronic jamming of communications. Communications regardless of frequency band, shore based or space, can be jammed and the severity of the jamming depends on the jammer's effect and bandwidth. Especially vulnerable are communication using civilian satellite communication and the Internet which is extensively used in today's operations. For example a large part of U.S. military communication during OIF was carried by commercial satellites and military administrative information via the Internet.[145]

4.7 Reduced effectiveness for urban counter-insurgency operations

Similar to the argument above, that planners might plan for wars other than the wars that will be fought are the arguments from critical researchers saying:

> . . . opponents using guerrilla tactics can significantly reduce the value of high-technology and that the utility of NCO can be less certain in urban counter-insurgency operations.[146]

This problem has already been seen in OIF where U.S. forces had to ". . . *go out and meet [insurgents] on the ground*" and engage in close combat in order to gain effective

---

[144] Wilson, *Network Centric Operations: Background And Oversight Issues . . .,* CRS-14.

[145] *Ibid*., CRS-14

[146] *Ibid*., CRS-8.

reconnaissance.[147] The information provided with modern surveillance equipment gave the adversary's position, size and composition, but did not say anything about his intent. "*To understand the enemy's intent, they needed human intelligence (HUMINT)*."[148]

4.8 Underestimating our adversaries

NCW collects information by using sensors in a network where the sensors are the source for gathering both enemy and friendly position and movement. Throughout history, development of new technology, tactics, strategy etc have always led to a development to try to find the countermeasures. This is most probably also the case when it comes to NCW. A 2002 Rand Corporation study concluded that:

> . . . as remote assets become more capable, it is likely that a future [enemy] force will develop counter technologies and become more sophisticated at cover, concealment, deception, and electronic warfare. Taking all of these into consideration, the net effect may actually be a decrease of knowledge and ultimately of situational awareness on the battlefield.[149]

There are several examples of ongoing development of weapons to counter NCW such as powerful directed energy devices to disrupt satellite communication, directed energy weapon to burn out computer circuits and malicious computer code to disrupt computer software.[150] It is also reported that Russia has sold equipment for jamming of GPS signals and that such equipment has been found in Iraq.[151] Taking into account the

---

[147] Curtis Taylor, Trading the Saber for Stealth: Can Surveillance Technology Replace Traditional Aggressive Reconnaissance?, *AUSA Land Warfare Institute, The Land Warfare Papers*, No. 53, September 2005, 23. http://www.ausa.org/pdfdocs/LWP_53.pdf; Internet; Accessed 12 March 2008.

[148] Taylor, Trading the Saber for Stealth . . ., 8.

[149] John Matsumura et al., *Preparing for Future Warfare with Advanced Technologies*, Report sponsored by the United States Army, (Santa Monica: Rand Corporation, Arroyo Center, 2002), 11.

[150] Wilson, *Network Centric Operations: Background And Oversight Issues . . .,* CRS-9.

[151] Alan D. Campen, "Information Operations may Find Definition and Validation in Iraq." *Signal* 57, no. 10 (June 2003): 44.

overreliance on GPS for own positioning, and consequently reporting of own position, jamming of GPS signals could lead to undesired episodes.

4.9 Technical Challenges

4.9.1 Interoperability

One of the major challenges when implementing NCW is interoperability, both between services for joint operations and between countries in coalition operations. NATO defines 'interoperability' as the *"The ability to operate in synergy in the execution of assigned tasks,"*[152]and 'force interoperability' as "*The ability of the forces of two or more nations to train, exercise and operate effectively together in the execution of assigned missions and tasks*." [153]

The concrete problems occurring from lack of interoperability are that the entities within the network will not have access to all available information and will not be able to provide its own information to others. This will lead to limitations in how they can cooperate with others and their ability to take part in an operation will be limited.[154]

Interoperability is more than just technical issues related to connection and communications. It is also about ". . . *important doctrinal, organisational, and cultural issues."*[155] These problems have to be solved as well as the technical ones. One should believe the problem was largest when it comes to combined operations, but the problem seems to be quite as large when it comes to joint. There are differences between services

---

[152] NATO, *AAP-6 - NATO Glossary Of Terms And Definitions* (Brussels: NATO, April 2008), 2-I-8.

[153] NATO, *AAP-6 . . .,* 2-F-6.

[154] Alberts and Hayes, *Power to the Edge . . .,* 108.

[155] Perry, *Network-Based Operations for the Swedish Defence Forces . . .,* 38.

and it seems that navies and air forces are better off than the armies. Basically this is because navies and air forces have been operating together for years using common link systems within coalition, while networking armies is a modern phenomenon. However the challenge is present also for navies and air forces, especially when new countries join a coalition.

In addition to the challenges in the joint and combined environment are the challenges occurring when other government departments and non-government organisations are supposed to participate. Presumably, those challenges are even bigger based on the fact seen about interoperability within joint operations. When the military has problems achieving interoperability within one organisation, the problems will increase when several organisations get involved.[156]

Some people question if it ever will be possible to achieve true networking interoperability between services. To solve these problems some countries are planning systems trying to link all users into on common system, e.g. the U.S. is planning to link everybody into the Global Information Grid (GIG).[157]

So far problems related to joint, combined and integrated operations are identified. In addition there are also challenges within an organisation, and especially between the different layers or levels within an organisation. This must also be solved in order to

---

[156] European Institute, *Transatlantic Interoperability in Defence Industries*, (Washington DC, 2002), 6.

[157] Wilson, *Network Centric Operations: Background And Oversight Issues . . .,* CRS-16.

achieve a force fully capable of NCW. Interoperability must be present in all the 'domains' to achieve full NCW capabilities.[158]

4.9.2 Space dominance – Satellite communications dependant

Information exchange is dependent on communications and as military forces is moving and manoeuvring mobile communications is necessary. Location, geography and topography give challenges regarding communication both when it comes to which frequency band to be used, and by that bandwidth, size of equipment and range. The answer to these problems is use of satellite communications which is more and more used both in military operations and during training. It is also a fact that the availability of civilian communications satellites is bigger than military. According to the Defense Information Systems Agency (DISA) *". . . up to 84 percent of the satellite communications bandwidth provided to the OIF theatre was supplied by commercial satellites."*[159] However, experience has shown that the use of civilian satellites might not necessarily give the required service. The use of the civilian INMARSAT in OIF showed that it was incapable of giving the required bandwidth of 128 kilobits per second and had to reduce to 64, which was too slow for the Army's need.[160]

4.9.3 Bandwidth

Bandwidth is the transmission capacity regardless of communication type (radio, lines, Internet, satellite etc). As seen in the civilian market among Internet providers during the last years there have been a big increase in demand for bandwidth. Similarly

---

[158] Alberts and Hayes, *Power to the Edge . . .,* 107-108.

[159] Wilson, *Network Centric Operations: Background And Oversight Issues . . .,* CRS-16.

[160] Warren Ferster, "Military Bandwidth Demand Energizes Market," *SpaceNews*, September 2, 2003. http://www.space.com/spacenews/archive03/militaryarch_090203.html; Internet; Accessed 18 March 2008.

has there been an almost explosive demand for bandwidth for military use mainly due to *". . . delivery of digital information."*[161] During OIF the U.S. commanders in Qatar and Kuwait had 42 times the bandwidth available compared to the first Gulf War.[162] It is expected that the bandwidth demand will continue to increase. The U.S. Congressional Budget Office estimates that there will be at least an increase of bandwidth requirement of 15 percent per year, probably much more due to ongoing developments.[163] However, the communications infrastructure must provide enough bandwidth to serve the military needs. It must be possible for several users located around in the battlefield to pull out the information simultaneously without having to line up in a queue doing it in series using the same limited bandwidth.[164] Another problem related to limited bandwidth is that when there is a problem getting information through people feel forced to prioritise their messages:

> The do this by literally pulling the plug temporarily on some radio or computer switching equipment in order to free up enough bandwidth to allow the highest-priority messages to get through. [165]

This may solve the problem of getting important messages through, but if equipment and radios are switched off to do this they might lose other important messages.

---

[161] Wilson, *Network Centric Operations: Background And Oversight Issues . . .,* CRS-17-CRS-18.

[162] David Talbot, "How Technology Failed in Iraq", *Technology Review*, November 2004, http://www.technologyreview.com/articles/04/11/talbot1104.asp; Internet; Accessed 29 February 2008.

[163] U.S. Congressional Budget Office, "The Army's Bandwidth Bottleneck," Aug. 2003. http://www.cbo.gov; Internet; Accessed 18 march 2008.

[164] Matthew French, "Bandwidth in Iraq a subject of debate," *Federal Computer Week*, (Oct. 20,2003): 43.

[165] Wilson, *Network Centric Operations: Background And Oversight Issues . . .,* CRS-18.

4.10 Conclusion NCW challenges

Several challenges with NCW have been discussed, some are related to knowledge and perception of NCW, others to how the technology is used, and finally some are about the technology itself. There are of course ways to overcome some of the challenges, if not all. The challenges related to knowledge, perception and how the technology is used can be met by better education and training while the technological challenges can be met by more research, development and finally more money. Some of the challenges, especially those related to perception of NCW, might need time and more experience to be solved. The challenges described are valid for all users of NCW technology, but a problem for smaller countries with limited resources is to define how much effort and resources they should put into solving the challenges. The use of NCW technology today might help to give answers to some of the challenges and prepare the way for future development.

5 NCW today

NCW is already in use today giving experience and lessons learned for future development. Written material available describing experiences are mostly from the use of different types of NCW technology by U.S. forces in OIF, but other countries are starting to introduce NCW technology and adapt to the future as well. This chapter will first introduce some of the experiences made by the use of NCW technology in OIF and then give some examples of NCW technology in use in Norway as an example of the NCW status within a typical 'small country'.

5.1 Experience

There are analysts leaning more towards that the U.S. is heading in the right direction and there are analysts that have a more negative approach. Dennis Murphy concludes that "*Network-enabled operations achieved proof of concept in the major combat operations phase of Operation Iraqi Freedom."* [166] His main arguments are that the U.S. forces were able to conduct battles and campaigns with a common operating picture and a situational awareness they had not experienced in combat before. But at the same time he recognises that NCW is not the answer to all problems as there will always be 'fog and friction in war'.[167] Others, like Milan Vega are more reluctant and argues that the experiences from OIF ". . . *shows only that NCW is effective in fighting weak and passive opponents*" and that the networked force has little practical value in ". . . *obtaining accurate, timely and relevant information on the enemy*."[168] This section will

---

[166] Dennis Murphy, *Network Enabled Operations in Operation Iraqi Freedom: Initial Impressions*, CSL Issue Paper, Vol. 06-05 (March 2005), 4. http://www.oft.osd.mil/initiatives/ncw/docs/csl_issue_paper_0605.pdf; Internet; accessed 8 March 2008.

[167] Murphy, *Network Enabled Operations in Operation Iraqi Freedom . . .*, 4.

[168] Milan Vega, "The NCW illusion," *Armed Forces journal*, (1 January 2007): 17.

not attempt to prove whether it is Murphy or Vega that is right, but give an overview of the most important positive and negative experiences so far.

5.1.1 Network communications

One of the benefits of NCW experienced by U.S. forces during OIF, was that they were able through increased networking to develop an improved capability for coordination of quick targeting. Elapsed time for targeting was reduced to forty-five minutes, while it during Operation Desert Storm in 1991 was as much as four days.[169] When experiencing communication problems, people tend to find the easiest way around the problem. During OIF it was experienced that when there was problems with line-of-sight communications during movement, military e-mail and chat were used which again normally required satellite communications.[170] This proves that in a networked system there are possibilities to still get information through, even though the main channel might be problematic.

Another problem was that they were required to operate different types of communication equipment because information was received over many different networks.[171] This increased the workload of the operators and required knowledge of different types of equipment. Hopefully such problems are solved when more mature NCW technology is available.

---

[169] Dan Caterinicciа and Matthew French, "Network-Centric Warfare: Not There Yet," *Federal Computing Week*, (June 9, 2003), http://www.fcw.com/print/9_20/news/79869-1.html; Internet; Accessed 8 March 2008.

[170] Wilson, *Network Centric Operations: Background And Oversight Issues . . .,* CRS-23.

[171] Matthew French, "Technology a Dependable Ally in Iraq War," *Federal Computer Week*, vol. 18, no.8, (Mar. 29, 2004): 46.

The line-of-sight communications used hampered the movement of the convoys as they were moving too fast to get the communications systems work. In three cases this led to attack on U.S. vehicles which stopped to receive intelligence data on enemy positions. [172] Similarly the line-of-sight microwave-rely communication system did not provide the services it should, such as imagery etc, to the tactical level, while the information was available at command levels above. This problem seems to have been throughout:

> There were issues with bandwidth, exploitation, and processes that caused this state of affairs, but the bottom line was no [access to fresh spy photographs] during the entire war. [173]

5.1.2 Information Overload

As mentioned earlier information overload might be a problem and communicators, operations officers and commanders have reported they felt overloaded with information and that much of the information they got was not valid for their missions.[174] The lower levels had problems getting the information they needed, while the command level seemed to have the information they needed. However, the commanders had their own problems; their connectivity was too good and they received too much data from the sensors that they were not able to process all of it. And when they tried to transmit the information to the front they were not able to get through due to the problems experienced with the line-of-sight microwave-relay system.[175]

---

[172] Talbot, "How Technology Failed in Iraq"

[173] *Ibid*.

[174] Wilson, *Network Centric Operations: Background And Oversight Issues . . .,* CRS-23.

[175] Talbot, "How Technology Failed in Iraq."

5.1.3 Sensors

The Blue Force Tracker is one of the mostly recognised successes from OIF. The Blue Force Tracker is a portable computer that gets its own position using Global Positioning System (GPS) and then continuously transmits its own position data using satellite communications. The Blue Force Tracker can be used both by personnel and vehicles. The position of each unit is displayed on other Blue Force Tracker terminals and improves the situational awareness and gives the commanders a better overview of disposition of own forces. It also includes a possibility to communicate using an e-mail similar form (text message).[176]

The use of Blue Force Tracker was a strong contributor to the reduced friendly fire (blue-on-blue) compared to the 1991 Gulf War. In 1991 there were 35 fatalities while there in 2003 were only 2 caused by friendly ground fire.[177] The system was able to track at least 2500 vehicles which gave the commanders located in Qatar a good situational awareness and overview of their own forces disposition and it gave those in battle a good awareness of adjacent units.[178]

5.1.4 Situational Awareness

Shared situational awareness is one of the key goals with NCW and experience in OIF shows this is a challenging issue. A battalion defending a bridge did not get any information about the situation in the area, even though the levels above the battalion commander had relevant information. The only information received was from a communication intercept that one Iraqi brigade was moving south of the airport. But no

---

[176] Wilson, *Network Centric Operations: Background And Oversight Issues . . .,* CRS-24.

[177] French, "Technology a Dependable Ally in Iraq War," 46.

[178] Talbot, "How Technology Failed in Iraq".

"…sensors, no network, conveyed the far more dangerous reality…."[179] There was not one brigade, but three, and *". . .between 25 and 30 tanks, plus 70 to 80 armoured personnel carriers, artillery, and between 5,000 and 10,000 Iraqi soldiers coming from three directions.*"[180] This massive firepower attacked a U.S force of 1,000 soldiers supported by 30 tanks and 14 Bradley fighting vehicles. At the division level and above they had good situational awareness with good feeds from the sensors but at the front line they had ". . . *terrible situational awareness".* This was a universal problem in the front line and known from the first Gulf War, but they had hoped that newer technology in 2003 would have solved the problem.[181] There are however, examples of increased situational awareness. Normally, combat pilots would have been briefed before takeoff while in the Iraq War more than half of the sorties started without a briefing. Targets were identified by ground sensors and then communicated to already airborne pilots who were able to attack the targets because of increased situational awareness.[182]

5.1.5 Bandwidth

Bandwidth experience from OIF seems to prove that there will be issues related to bandwidth problems in several years from now. As previously mentioned the line-of-sight microwave-rely communication system did not have sufficient bandwidth to give the tactical level the information they needed. Due to the fact that they had to stop their vehicles when they were downloading information it proved to be slow when they needed it to be fast. The bandwidth problems also caused computer problems and the system

---

[179] Talbot, "How Technology Failed in Iraq".

[180] *Ibid*.

[181] *Ibid*.

could be locked for up to ten to twelve hours. Lacking the possibility to get necessary information led to that in several occasions the U.S. troops *". . . found the enemy by running into them, much as forces have done since the beginning of warfare."* [183] Unnecessary to say, this is not the intention behind NCW. However, the problems related to bandwidth taught them the value of 'bandwidth allocation' to utilise the restricted bandwidth available. It seems that the problem will continue some time into the future as it is not likely it will be possible to meet the bandwidth requirement in the near future. [184]

5.1.6 Organisation

Some of the problems that occurred and hampered information to the troops seem to have been based on the military organisation and ". . . *old-fashioned command and control systems"*. The whole process regarding information collection and dissemination seem to be in accordance with traditional ways of doing business. Information went up the chain where it was interpreted by commanders and decisions made before they tried to pass it down the chain again. Using the 'traditional way of organising' resulted in ". . . *time delays and the magnification of individual communications failures."* [185]

5.1.7 NCW Experience – Conclusion

Important experience by use of NCW technology is made everyday, whether it is in ongoing conflicts in Iraq and Afghanistan or in exercises in more peaceful areas of the world. The experience shows positive signs like the increased situational awareness of own forces by the use of the Blue Force Tracker and more negative signs like the

---

[182] Talbot, "How Technology Failed in Iraq".

[183] *Ibid*.

[184] French, "Technology a Dependable Ally in Iraq War," 46.

problem of disseminate information downwards in the organisation to those who need it. However, the experience so far shows the importance to continue the analysis of NCW elements in today's operations in addition to regular experimentation to fully understand NCW's potential for future development.[186]

5.2 Examples of NCW technology in use in Norway

There are a lot of things that could be included in NCW technology as NCW entities can be sensors, decision makers and shooters. However, from an interoperability point of view and also the part that links the entities with their technology together, it is the networks and the communication systems that probably is the most critical part. Further the development and interoperability of the networks and communication systems will also say something about level of maturity and the development status within NCW. Norway's and several other countries' approach to NCW are to utilise existing equipment and the 'heritage' when possible.[187] So far the only 'new, large-scale' procurement of NCW type equipment is Link 16.[188]

5.2.1 Link 11

Link 11 is an old system but is still used, especially in the maritime environment. Norway has Link 11 onboard the frigates, the Fast Patrol Boats (FPBs) (and the future Missile Corvettes), the Maritime Patrol Aircrafts (MPAs), some shore stations for providing the air picture to ships and some portable (or more correctly, moveable) systems for use with Task Group commands onboard ships. Link 11 utilise mainly High

---

[185] Talbot, "How Technology Failed in Iraq".

[186] Alberts et al, *Network Centric Warfare . . .,* 104.

[187] Bård K. Reitan and Lene Pålhaugen, *Forventningene til nettverksbasert forsvar – 6 tema* (FFI/Rapport-2004/04004), Kjeller: Forsvarets Forskningsinstitutt, 2004, 12.

Frequency (HF) and Ultra High Frequency (UHF) for communication, but it is also possible to transmit Link-11 messages via satellite communication (SATCOM) with limited functionality.[189] Link 11 has proven to be a reliable system, but has its limitations in bandwidth, speed and by that functions. Another issue is that the system is based on that the Net Control Station (NCS) triggers everybody in the network to send their messages after turn so if the NCS has lost communication the whole network falls down.[190] The only possible mitigation for this problem is that the operators notice what happens and somebody else takes over the role as NCS. Link 11 can be linked to other systems only if the other systems are able to read Link 11 messages (M-messages).

5.2.2 Link 16

The Norwegian Parliament decided in 2003 that Link 16 should be procured for the F-16 fighter aircrafts, Fridtjof Nansen-cl frigates, Skjold-cl missile corvettes and the Norwegian Ground Based Air Defence (GBAD) and be part of the NCW solution for implementation of NCW in Norway.[191] The GBAD will be equipped with Link 16 due to its cooperation with the F-16 in the air defence of Norway. Link 16 communicates basically using UHF,[192] but can also send its messages via SATCOM (JSAT).[193] As with Link 11, Link 16 can also be linked to other systems only if the other systems are able to read Link 16 messages (J-messages). Link 16 is a true NCW system and according to

---

[188] Forsvarsdepartementet, *The Norwegian Defence Budget 2003* (Oslo: FD Norge, 2003), 83-84.

[189] Forsvarsdepartementet, *Fremskaffelsesløsning P6451 - SATCOM for Skjold-klassen* (Oslo: FD Norge, August 2006, 17.

[190] Norman Friedman, "They Link it Together," *Naval Forces* 26, no. 3 (2005), 36-37.

[191] Forsvarsdepartementet, *The Norwegian Defence Budget 2003*, 83-84.

[192] Friedman, "They Link it Together," 40.

Alberts it enables ". . . *a force to operate in the network-centric region of the information domain*" within the ". . . *air-to-air mission area*."[194] However, Norway intends to use in the maritime area as well.

5.2.3 Northern European Command-C2 Information System (NEC CCIS)

NEC CCIS is a system used by Denmark, Norway and Poland (and soon the Baltic states) providing support to NATO Headquarter units within the NATO Air Command And Control System (ACCS). It was developed in the 1980's to give command and control functionality in all operational areas within air operations but is now primarily used for planning and tasking of air operations. NEC CCIS has been further developed over time and has been operational in the current configuration since 2004. NEC CCIS is interoperable with several systems[195] using NATO standards and formats.[196]

5.2.4 NORDIS

The Norwegian Defence Information Services Secure (NORDIS-S) functions as a host platform for a wide range of services and functions where the most important is the NORCCIS II command and control application which will be described below. NORDIS S is based on a commercial off the shelf (COTS) computer and can run on both desktops and laptops. The NORDIS S services are e-mail, groupware, webservice, Military

---

[193] Forsvarsdepartementet, *Fremskaffelsesløsning P6451 – SATCOM . . .,* 17.

[194] Alberts, *Understanding Information Age Warfare*, 244.

[195] CWID - Coalition Warrior Interoperability Demonstration, 2006 Final Report, http://www.cwid.js.mil/public/CWID06FR/htmlfiles/101sei.html; Internet; Accessed 24 March 2008.

[196] Examples of such formats are "*USMTF, Allied Data Publication (ADatP) ADatP-3, OTH-Gold, Link 1, and Link 11b.*

Message Handling System (MMHS), IP-telephone and conferencing in addition to the security and communication services provided to the function applications.[197]

5.2.5 NORCCIS II

The Norwegian Command and Control Information System II (NORCCIS II) is the main and joint command and control and information system in Norway and has been in use since 1992. It has mainly been used at the operational level in headquarters, but has during the recent years been successfully tested out at the tactical level mainly within the Navy and the Army. In addition NORCCIS II is also in use in international headquarters where the NAF is represented,[198] in addition to headquarters set up for the duration for the mission.[199] NORCCIS II is also used within the government, e.g. the Prime Minister's Office, departments, directorates, embassies etc. For those users NORCCIS II is mainly a tool for fast and secure communications both within NATO Secret and national Secret information. In addition NORCCIS II contains a vast amount of information either web based or databases based on a "*Post – Smart Pull*" concept.[200] NORCCIS II Land C2

---

[197] Norwegian Defence Logistics Organisation - Communication Information Systems (NDLO/CIS), http://www.c2is.net; Internet; Accessed 24 march 2008.

[198] Examples of headquarters with Norwegian representation: Supreme Headquarters Allied Powers Europe (SHAPE), Allied Forces Northern Europe (AFNORTH), NATO Headquarters Brussels, Kosovo Force (KFOR), International Stabilisation Force Afghanistan (ISAF), and Norwegian Liaison U.S. Central Command (NO LNO CENTCOM).

[199] For example during the maritime contribution to the United Nations Interim Force in Lebanon II (UNIFIL II)

[200] Norwegian Defence Logistics Organisation - Communication Information Systems (NDLO/CIS), http://www.c2is.net/nii/index.html; Internet; Accessed 24 march 2008.

Services has been field proven in operations since 2002[201] and the NORCCIS II Maritime C2 Services since 2001.[202]

NORCCIS II provides several functional services where the most important is the Common Operational Picture (COP) contributing to shared situational awareness within the battlespace. The COP is a fused representation of the situation in the battlefield presented graphically together with relevant maps and overlays. The COP consists of three main components: Recognized Air Picture (RAP), Recognized Land Picture (RLP) and Recognized Maritime Picture (RMP). In addition to the COP, the most important functions in NORCCIS II are:[203]

- Land C2 Services (to build, maintain and exchange the RLP).
- Maritime Services (production of the RMP).
- Air Services (display of the RAP, Air order of battle, geographical disposition and status of Air units and graphical presentation of Air Tasking Order (ATO) and Airspace Control Order (ACO)).
- Targeting Services (to support the targeting process and the Joint Operational level).
- Military Geographic Information and Analysis functions.
- Meteorological and Oceanographic service
- Plans and Orders service

---

[201] Norwegian Defence Logistics Organisation - Communication Information Systems (NDLO/CIS), http://www.c2is.net/nii/services/landc2.html; Internet; Accessed 24 march 2008.

[202] Norwegian Defence Logistics Organisation - Communication Information Systems (NDLO/CIS), http://www.c2is.net/nii/services/maritimec2.html; Internet; Accessed 24 march 2008.

[203] Norwegian Defence Logistics Organisation - Communication Information Systems (NDLO/CIS), http://www.c2is.net/nii/; Internet; Accessed 24 march 2008.

- Information Management
- Operational Logistics.
- Web-based Services with access to different types of available information.

Norway is putting effort into the development of NORCCIS II to make it the main tool for NCW in the future with special focus on interoperability with similar systems within NATO. As stated by the Norwegian Defence Logistics Organisation Command and Control and Information Branch website:

> *NORCCIS II represents breakthroughs in many areas. It is flexible, scaleable and cutting edge. The Norwegian Defence is committed to continuously develop the NORCCIS II system into the network centric warfare future.*[204]

5.2.6 Satellite communications

The increased amount of Norwegian participation in international operations in areas with bad or missing communication infrastructure has lead to a reliance on use of satellite communication. Satellite communication is the more or less only reliable type of communication capable of providing necessary bandwidth to accompany a network based operational concept. So far the NAF has leased or rented bandwidth mainly from civilian providers of satellite communication, but also from allies. However, recent operations have shown that allies need their own bandwidth more and more and the availability has decreased significantly. Based on this fact the NAF started in 2006 a preliminary project to achieve 'Secure access to a space segment'[205] The aim of the project is to get a reserved position in space for deployment of either a Norwegian national satellite or a satellite in companionship with allies. The Norwegian Parliament approved the

---

[204] Norwegian Defence Logistics Organisation - Communication Information Systems (NDLO/CIS), http://www.c2is.net/nii/index.html; Internet; Accessed 24 march 2008.

preliminary project in June 2007 and required the project to be established and include the cost in the budget for 2009.[206] In principle the project will be accomplished in the period 2009-2011 and the goal is that it should be possible to deliver operational satellite communication services from 2012. [207]

5.2.7 Sensors

Sensors will not be discussed in details as the use of sensors within the framework of NCW will be based on the heritage from existing equipment. However, one new capability is going to be implemented, basically due to the lack of sensors in the Army, and that is the new Army ISTAR Battalion.[208] However, which types of sensors, except Eye Ball Mk I and MK II, that will be used by this battalion is still unknown. It will independent of which types of sensors that will be implemented increase the Army's capability to produce the RLP.

5.3 NCW today – Conclusion

Norway has some NCW technology already in use and is expected to implement even more, e.g. Link 16 and expansion of the NORCCIS II environment, in the near future. However, the equipment introduced indicates a heavy reliance on the NORCCIS II as both a tri-service joint and combined NCW enabler. Link-11 is first of all a maritime link and Link-16 is an air-force link, even though Norway intends to use the latter as a maritime link as well. NORCCIS II is the only NCW system planned to be implemented

---

[205] "Sikker tilgang til romsegment" translates to "Secure access to a space segment."

[206] Stortinget, *Stortingsinnstilling nr 287 (2006-2007)* (Oslo: St.t. Norge 2007), 8.

[207] Stortinget, *Stortingsinnstilling nr 287 (2006-2007),* 8.

[208] Forsvarsdepartementet, *Stortingsproposisjon nr 42 (2003-2004) Den videre moderniseringen av Forsvaret* (Oslo: FD Norge),56.

in all three services and is also foreseen to be utilised in a combined environment. One of the major challenges introduced in chapter *4 Critical issues and challenges* is interoperability which will be an issue when NORCCIS II is going to be used in a combined environment. However, this will also rely upon how the Norwegian military forces will be used and under which policy they will operate.

6 Smaller nations defence policy

As introduced in chapter *2 What is Network Centric Warfare?* NCW is more than just technology. Implementation of NCW should have an impact throughout the organisation and at all levels. This chapter will describe some of the smaller countries' defence policies with emphasise on the Norwegian defence policy in order to give an introduction to both the priorities in use of those countries' armed forces, but also to see if they start to include NCW into their defence policies. To give an example of a small country's armed forces the Norwegian armed forces will be briefly described. Finally this chapter will deal with Norway's defence budget as this is an important indicator of how much money a small country is able to spend on development and implementation of NCW in the future.

6.1 Norwegian defence policy

For the Western world, the end of the Cold War changed the threat away from something concrete and quantifiable to today's situation where the threat is uncertain and unpredictable. Simultaneously, the importance of natural resources has increased, which from a Norwegian point of view has given the northern region, especially the sea areas, a strategic importance. The 'global age' has changed the way conflicts inflict on the world societies. Traditionally conflicts were limited by geographical borders while today threats and challenges do not care about borders. This fact has impacted especially the Western world's security and defence policy and by that also how Norway looks upon their use of the Armed Forces. There is a move away from the focus on defending Norway in Norway, to a policy to contribute together with allies and partners to limit ". . . *crises,*

armed conflicts and war" within the areas of interest. [209] The fundamental objectives of Norwegian security policy are:

- to prevent war and the emergence of various kinds of threats to Norwegian and collective security;
- to contribute to peace, stability and the further development of the international rule of law;
- to uphold Norwegian sovereignty, Norwegian rights and interests, and protect Norwegian freedom of action in the face of political, military and other kinds of pressure;
- to defend together with our Allies Norway and NATO against assault and attack;
- to protect society against assault and attack, by state and non-state actors.[210]

Based upon the security policy objectives the NAF has been given the following tasks:

- National tasks
  - To secure a national basis for decision through surveillance and intelligence.
  - Maintain Norwegian sovereignty.
  - Exercise Norwegian authority in limited areas.
  - Prevent and handle episodes and security policy related crises in Norway and within Norwegian areas.
- Task together with allied and others
  - Contribute to a collective defence of Norway and other NATO countries against threats, raids and attack, included use of Weapons of Mass Destruction (WMD).
  - Contribute to multinational crises management, including multinational peace operations.
- Other tasks
  - Contribute with military support to diplomacy and prevention of proliferation of WMD.
  - Contribute to secure the Norwegian society and vital tasks within the society.[211]

---

[209] Forsvarsdepartementet, "*Norwegian Defence 2006*," Oslo 2006, 3. http://www.regjeringen.no/Upload/FD/Dokumenter/FoF_2006_eng.pdf; Internet; Accessed 22 March 2008.

[210] Forsvarsdepartementet, "*Norwegian Defence 2006,*" 3.

[211] Forsvarsdepartementet, *Styrke og relevans* (Oslo FD:Norge, 3 January 2005), 11.

The Norwegian joint doctrine emphasises effect-based operations, NCW and manoeuvre warfare,[212] but without the words 'operation' and 'warfare'. They are replaced with the word 'thoughts', which in this context imply that the essence of vital theoretical theories and directions are incorporated at the individual level.[213] Regardless of semantics, it is beyond doubt that the overarching concept for use of military force is based on those three 'methodologies'. It is especially interesting that the use of NCW is elevated to be an overarching principle in the NAF as this should provide guidance for the implementation of and focus on NCW based technology.

6.2 Other nations

As shown for Norway other small nations have a similar approach to the renewal and modernisation of their defence systems. The main reason is that the security situation in the world is changing. This lead to the fact that nations previously more concerned about defending their homeland now take a more active part in international operations. Again this does not eliminate the need to defend their own country, but adds more tasks to what they need to be able to do. Sweden which traditionally has been very 'self-centric' in their defence and relied on themselves, basically because of their neutrality, is now moving towards participation in international operations including membership in alliances as Partnership For Peace (PfP).[214] The tasks for the Swedish Armed Forces are more or less similar to the tasks already presented for Norway above.[215] Similarly has the

---

[212] Forsvarsstaben, *Forsvarets Fellesoperative Doktrine*, 3.

[213] *Ibid*., 8.

[214] Regjeringskanseliet, *The New Defence – prepared for the next millennium (Short version of the Government Bill 1999/2000:30),* (Stockholm 2000), 3.

[215] Regjeringskanseliet, *The New Defence – prepared . . .,* 6.

Swedish armed forces committed to the introduction of NCW or ". . . *network-based concepts*" as is closer to the wording used by the Swedes.[216]

Another of Norway's neighbouring countries, Finland, also has a very similar approach to the Norwegian and Swedish way of organising the armed forces to both take care of the defence of the home country and to participate in international operations.[217]

6.3 Defence capabilities

The NAF has decreased in size since the end of the Cold War and is moving towards a more efficient, professional and technologically modern force. In peacetime the NAF consist of approximately 14250 personnel distributed as follows; Army 7500, Navy 3700, Air-Force 1850 and the Home Guard 1200. To put these numbers into reality, the Norwegian population per 23 March 2008 was 4 751 400.[218] Norway still have the concept of conscription and mobilisation in war and in case of mobilisation the NAF will consist of approximately 70000 personnel with the major increase within the Home Guard while the single services will have an average increase of approximately 2000.[219] The figures also includes personnel posted in joint organisations as headquarters, materiel procurement, logistics, education and training organisations and civilians as well which reduces the total number of combatant personnel drastically.

---

[216] Perry, *Network-Based Operations for the Swedish Defence Forces . . .*, 4.

[217] *Finnish Defence Forces – Network-Centric Operations*, 7, http://www-01.ibm.com/industries/government/ieg/pdf/finnish_defence_forces-nco.pdf; Internet; Accessed 22 February 2008.

[218] Statistisk Sentralbyrå (Statistics Norway), http://www.ssb.no/befolkning; Internet; Accessed 23 March 2008.

[219] Forsvarsdepartementet, "*Norwegian Defence 2006*," 16-19.

Taking into account the challenges discussed in this paper it is the peacetime organisation that is mostly interesting as that part of the organisation will be in the technological upper end also in case of war. Further, that is also the part of the organisation that contributes in today's international operations in a joint and combined environment.

It is not the aim of this paper to analyse the capabilities provided by the NAF but it is evident that the size of the NAF and the capabilities it can provide is relatively low. The Army has a peacetime structure of one mechanised brigade, a mobile tactical land command, a battalion and the Army Special Forces Command, but a majority of the forces will be under education and training.[220] The Navy will after the vessels currently under production are phased in, consist of 5 frigates, 6 submarines, 6 missile corvettes and 6 mine countermeasures vessels. In addition the Navy has a 'blue-green-black' environment consisting of the Coastal Rangers Command, Mince Clearance Command and the Naval Special Operation Force Command. The Coast Guard is sailing 14 vessels, of which 4 are helicopter carrying.[221] As for the Army a major part will be under education and training which means that the operational Norwegian Task Group (NoTG) will consist of 2 frigates, 2-3 missile corvettes, 2 submarines, 2-3 MCM vessels and elements from the 'blue-green-black' environment. The Air-Force is also relatively small with 57 F-16 fighters which have been through Mid Life Update (MLU), 6 P-3 Maritime Patrol Aircrafts (MPA), 6 C-130 Hercules transport aircraft, 3 DA-20 Jet Falcons for Electronic Warfare (EW), 6 Lynx helicopters (currently in use only by the Coast Guard)

---

[220] Forsvarsdepartementet, "*Norwegian Defence 2006*," 16.

[221] *Ibid*., 17.

and 18 Bell 412 helicopters (for support of Army operations). A project to replace the F-16s between 2015 and 2020 in ongoing. In 209 the Lynx helicopters will be replaced by in total 14 NH-90 FHL to be organic helicopters onboard the frigates and the Coast Guard vessels. The Air Force also has 2 Norwegian Air-force Surface to Air Missile System (NASAMS) mobile missile units with AMRAAM missile to provide air defence.[222] The Home Guard consist in peace time mainly of the staffs and training institutions to prepare the Home Guard personnel to be ready if mobilised.[223]

6.4 Economy and budget

It follows naturally that for small countries with small armed forces the defence budget is also relatively small. The Norwegian Defence budget for 2008 is in total 31,5 billion Norwegian kroner which amount to 6 billion US dollars. The budget is distributed into operation and maintenance of 4.2, property and building investment of 0.3 and materiel investments of 1.5 billion US dollars.[224] A major problem regarding the distribution of the budget is that too much is used for operation and maintenance, around 70% of the total budget, which has a direct impact on the possibilities to get into line with the ambitions to be a technologically modern force. A big part of the investment budget has for the recent years gone to the procurement of the frigates, the missile corvettes and the new NH-90 FHL helicopters. The next big project will be the replacement of the F-16 fighters that again will need a major part of the investments and after that again the submarines will probably have to be replaced. This means that the major part of the

---

[222] Forsvarsdepartementet, "*Norwegian Defence 2006*," 18.

[223] *Ibid*., 19.

[224] Forsvarsdepartementet, *Stortingsproposisjon nr 1 (2007-2008) Statsbudsjettet for budsjettåret 2008 – Forsvaret* (Oslo: FD Norge 2007), 30.

materiel investments until 2025 is probably already committed which does not leave enough room to modernise and to be in front of the development of new technology.

6.5 Smaller nations' defence policy – Conclusion

Most western countries have adapted their defence policies towards the situation in the world today. Norway and other smaller countries like Sweden and Finland have more or less a similar approach to how to use their armed forces; defence of their own country and participation in international operations. NCW is beginning to be a part of the defence policy and both Norway and other smaller countries are focusing on the benefits of NCW and that NCW will be a basic function of the future armed forces. The combatant part of the NAF is relatively small compared to other nations and this should simplify the implementation of NCW as the organisation itself is simpler and more visible compared to complex organisations as for example the U.S. However, smaller nations tend to struggle with their defence budget and as shown the Norwegian budget is relatively small and one of the main problems is that a large part of the budget is committed to operation and maintenance leaving less money for future investments.

7 Specific NCW challenges for small nations

One of the problems facing smaller nations is that the existing command, control, communication, and computer information systems (C4IS) were developed to support mainly one service within the military. The Finnish Defence Forces (FDF) Chief of Operations sums this up:

> Most of our current C4 systems are stove-piped systems to support Army, Navy or Air Force operations. We face the same challenge as most of today's militaries. We cannot afford to develop future systems on top of old systems by patching and bridging gaps and trying to maintain old technology. … Technical, data, and application integration can take us only so far.[225]

As Markku Koli indicates this is not only a problem for small nations, but most of today's militaries. However the impact this problem have on small nations could be significant and this chapter will describe some of those implications.

7.1 Should the focus be joint or combined?

Smaller countries may face the problem that they have to choose between whether they should gain interoperability nationally (joint) or within a coalition (combined).[226] Which line to choose will depend on each nation cost benefit evaluation for which type of interoperability will give them most value in their defence. Normally nations will minimise the effort where possible and just keep the lowest possible level.[227]

---

[225] Markku Koli, "Experiences and Challenges in Implementing Network Enabled Defence," presentation given to Network Centric Warfare Europe 2006, 7 June 2006. Quoted in *Finnish Defence Forces – Network-Centric Operations*, 1, http://www-01.ibm.com/industries/government/ieg/pdf/finnish_defence_forces-nco.pdf; Internet; Accessed 22 February 2008.

[226] Kym MacMillan, *Evolving command & control – The challenge for smaller defence forces* (Canberra City: CCRP Paper, 2004), 7. http://www.dodccrp.org/events/2004_CCRTS/CD/papers/074.pdf: Internet: Accessed 28 February 2008.

[227] Wolfers, Arnold. "'National Security' as an Ambiguous Symbol." *Political Science Quarterly* 67, no. 4 (Dec., 1952), 488.

There are differences between the services and this is also visible in the literature available about NCW. Mostly everything, with a few exceptions, is oriented towards the Army and the land battle. There are mainly two reasons for this. First it is a fact that the ongoing conflicts today are in the land environment and by that gains experience and priority. Second, NCW is for the Navies and Air Forces of the world a more inherent and natural approach. Link 11 has been around for decades and the way ships and aircrafts operate are more in line with NCW concepts. There has existed NATO procedures for Third Party Targeting (TPT) for decades using both voice and link communication between only ships or between ships and aircrafts. TPT is a simple form of NCW with separation of sensor, decision-maker and shooter mainly used for weapon delivery outside own (shooter) sensor range. The differences between the services complicate the path towards NCW especially for those nations already within an alliance. NATO navies are in general more interoperable with other NATO navy vessels than they are with their own country's army using Link 11, secure voice systems, message handling systems etc. The case is similar for air forces, but when it comes to armies it is completely different.

Choosing between joint or combined interoperability will basically be a cost challenge. Unfortunately, several nations will probably gain interoperability nationally as that probably will have the lowest cost as simple solutions can solve their joint challenges. This will again reduce the value of the forces within a coalition operation which require agreed interoperability between several nations.

7.2 Army complexity – implications for levels of implementation

The differences between the services are also visible when it comes to which level NCW should be implemented. For navies and air forces it is quite simple as the lowest level consists of ships and aircrafts and number of levels above is also limited. For the

Armies the situation is different and the challenge is to determine the lowest level where NCW should be implemented. Some nations are developing and testing NCW equipment down to individual level, e.g. the Blue Force Tracker was tested out at individual soldier level during operations in the Balkans.[228] However, even such a system is more commonly used at unit level, mainly as low as company level and in vehicles.[229] Even though it might have been smart to keep track of every soldier in the battlefield it could easily lead to information overload and it requires a 'smart pull' concept in place to ensure that not everyone in the network is overloaded with soldier data.

7.3 Different types of approach

The United Kingdom (UK) has called their version of NCW for Network Enabled Capability (NEC) which is designed to implement networking capabilities where it is most cost effective and might increase the military capabilities. They will avoid to reorganise the armed forces around a network which could have been the case is they adopted the U.S. model. This approach is cheaper and it seems to be a model for smaller countries that are not capable of taking the U.S. approach. UK has a series of small programmes as satellite communication, Unmanned Air Vehicle (UAV) as sensors, different types of communication kits for different levels of warfare etc. Overall these programmes are similar to what is being developed within the US but instead of a large overall program it is smaller and more applicable to the UK forces. Other nations as France, Germany, Sweden and Australia have a similar approach.[230] Australia is even

---

[228] PA Consulting Group and Evidence Based Research, Inc. *A Network Centric Operations Case Study : US/UK Coalition Combat Operations during Operation Iraqi Freedom*. Version 2.0 ed. (Washington DC: PA Consulting Group, 2004), 3-6.

[229] PA Consulting Group and Evidence Based Research, Inc. *A Network Centric . . .,* 6-3 – 6-5.

[230] Richardson, "Network-Centric Warfare . . .," 66.

more relaxed as they seem to let other countries do the development and implement what other countries are able to produce based on the fact that they do not have a budget big enough for doing their own development. [231]

The UK plans to implement NEC in states where the content and intention of each phase also is similar to the Norwegian approach which will be described later. There are however, minor differences in the scheduling of when the different states are achieved. UK plan to achieve the 'Initial' state in 2007, the 'Transitional' state in 2015 and finally the 'Mature' state in 2020-2030,[232] while Norway's ambition is 2008-2009, 2012 and 2030. [233] A similar approach is also taken by Australia who has 2010, 2015 and 2020 for its target states,[234] while New Zealand does not even plan to reach further than the 'transitional' state due to its limited resources.[235]

7.4 Where should they focus?

The main opportunities and benefits of NCW have been discussed earlier but as an example the Australian approach of focus can be worth to notice. Australia is, when it comes to military a relatively small nation with limited defence budget. Australia sum up the advantages of NCW and where the focus should be for smaller nations as:

> . . . superior information that can be processed into actionable intelligence, shared situational awareness, improved decision making and improved

---

[231] Fish, "NCW Development in Small Countries," 33.

[232] *Ibid*., 32.

[233] Forsvarets Overkommando, Forsvarssjefens militærfaglige utredning 2003 – Vedlegg B – Arbeidsutvalg NBF (Oslo: FO Norge, October 2002), 15-18.

[234] Australia. Dept. of Defence. Office of the Chief Information Officer. *A Concept for Enabling Information Superiority & Support* (Canberra, ACT: Dept. of Defence, 2004), 21.

[235] MacMillan, *Evolving command & control – The challenge for smaller . . .,* 10.

application of force.[236]

The Australian approach is in general similar to the UK NEC approach where the focus is on ". . . *better networks, better information sharing, better shared understanding, better decisions, better actions and better effect*s."[237] Similarly are the functions in the Norwegian command and control system NORDIS-S/NORCCIS II directed towards giving the same benefits. It seems that countries with limited budgets and possibilities end up with a relatively similar approach and focus on information sharing, better situational awareness, improved command and control which again will lead to improved application of force or in other words better effects.

7.5 Cost

Cost is the main problem for smaller nations when it comes to accompany the development in the U.S. As shown above the Norwegian defence budget for 2008 is $ 6 Billion, and the amount available for investments is $1.5 Billion per year. In comparison the U.S. 'Future Combat Systems' for the U.S. Army has an expected cost of more than $100 billion.[238] In other words, the U.S. is planning for an Army system with a cost more than sixteen times the annual Norwegian defence budget, or 67 times the Norwegian annual investment budget. Similarly has the U.S. GIG, a NCW system planned to network the complete U.S. Armed Forces into one network, an estimated cost of several

---

[236] Australia. Dept. of Defence. Office of the Chief Information Officer. *A Concept for . . .,* 21.

[237] Ministry of Defence, *Network Enabled Capability, Joint Services Publication 777*, (London: MOD UK, 2005) 10.

[238] Talbot, "How Technology Failed in Iraq."

hundred billions dollars.[239] Beyond doubt, the U.S. Armed Forces and even the U.S. Army is a much bigger organisation than the NAF and a similar system for a smaller force would have been less expensive. However, this gives an indication of the costs involved to be among the leading NCW nations.

Finland, with an Armed Forces of similar size as the Norwegian, expect that their Finish Network Enabled Defence (FiNED) will consume 20% of the Finnish investment budget by 2012 ($ 1.25 billion by 2012),[240] which equals 78 percent of the Norwegian investment budget.

When the decision was made by the Norwegian Parliament to procure Link 16 for the 5 new Fridtjof Nansen-cl frigates and for 20 of the F-16 MLU Fighters the planned cost was $ 91 million for the 5 frigates and $ 22 mill for the 20 F-16 MLU.[241] The higher cost for the frigates is because of a higher degree of integration into the combat management system (CMS) onboard. If Link-16 should have been implemented throughout the NAF with similar systems as the frigate version on all the ships not already equipped, all the aircrafts with the F-16 MLU version and around one hundred terminals for the Army and shore organisation the cost would have been approximately one complete annual investment budget (1.6 billion dollars).

The figures presented gives an indication of the cost related to development and implementation of NCW. There are no signs that the cost will be reduced as the defence

---

[239] Tim Weiner, "Pentagon Envisioning Costly Internet for War," *New York Times*, November 13, 2004.

[240] Finnish Defence Forces – Network-Centric Operations, 3, http://www-01.ibm.com/industries/government/ieg/pdf/finnish_defence_forces-nco.pdf; Internet; Accessed 22 February 2008.

[241] Forsvarsdepartementet, *Stortingsproposisjon nr 50 (2002-2003)* . . ., 4.

industry very well knows the value of today's market in that business. Further the figures shows that the major part of a small country's investment budget over a period of time is needed to implement NCW. This makes the cost issues the biggest challenge for smaller nations with other investment challenges as well, and leads to the need for a sound prioritisation of where to spend the investment budget.

7.6 NCW challenges for small nations - Conclusion

Countries have different approaches to how to implement NCW, but a common line seems to be that smaller countries tend to find a sober-minded ambition level which gives them the opportunity to build on equipment already in use. Shared situational awareness and the advantages this provides seem to be a common major goal for most countries. However, the biggest challenge for all the small countries is the budget related to the cost of implanting NCW. The examples shown above indicates that the investment portion of the defence budgets are relatively small, making it difficult to finance an overall implementation of new NCW technology at the same time as other big and necessary investments are ongoing. This leads to different levels of ambition which will be a topic for discussion, exemplified by the Norwegian ambition, in the next chapter.

8 The Norwegian level of ambition for NCW implementation

To establish the starting point regarding NCW development and implementation in Norway the criteria for success for NCW implementation as outlined from Alberts et al's "*Network Centric Warfare: Developing and Leveraging Information Superiority*"[242] will be discussed along the Norwegian status related to these criteria today. Then the Norwegian NCW ambition will be described in general before the different levels of ambition as described in the Norwegian implementation phases is introduced. These levels of ambition are described in a model based on Alberts' NCW Capability Model as outlined in "*Understanding Information Warfare*,"[243] and his model will be briefly introduced in order to give a better understanding of the foundation and background of the Norwegian levels of ambition. Finally the Norwegian levels of ambition will be discussed against today's NCW status in Norway based on the characteristics within each level.

8.1 Norway's status versus Alberts' criteria for success

Implicit in Alberts et al's description of "*Making NCW a Reality*," "*Assessing the Potential of NCW*" and "*The Journey Ahead*" [244] there are some criteria for success that can be utilised to assess the status of a successful implementation of NCW. Essentially these are the following four criteria: First, concepts and strategies should be developed to meet the challenges of implementing NCW and the ability to transform NCW into operational capability.[245] Second, there should be a change in how systems are acquired

---

[242] Alberts et al, *Network Centric Warfare . . .,* 199-229.

[243] Alberts, *Information Age Transformation . . .,* 86-88.

[244] Alberts et al, *Network Centric Warfare . . .,* 199-229.

[245] *Ibid*., 199.

and investments are planned to facilitate for the effects of NCW technology. The traditional model for procurement and investment is time consuming and a lot of the requirements are based on assumptions and products might already be outdated when they are introduced in service.[246] As a consequence of the rapid development of the technology there is a need for early user involvement, use of prototyping, frequent testing during development and to use architecture which makes future changes and development possible.[247] Third, experimentation is critical in order to get empirical data and measures for analysis of how to transform NCW from a theory into practice.[248] Fourth, there is a need for a change in how education and training is performed to enable individuals to be better prepared for NCW. According to Alberts et al a thorough change in education is needed:

> The adoption of NCW will involve significant, if not fundamental changes in how DoD task organizes duties and responsibilities of individuals. Individuals will need to adopt new attitudes, accept more responsibility, learn new skills, master new approaches, and operate new systems—all in a faster-paced environment. The future DoD is likely to have fewer, but more educated and highly trained individuals. Current up-and-out and job-rotation personnel practices will need to be reexamined in the face of these changes. A hard look at our whole approach to education and training is required. Given the pace of change, education and training will need to be continuous and closely integrated with day-today activities. [249]

These four criteria will be the bases for the discussion of Norway's status of NCW implementation today.

---

[246] Alberts et al, *Network Centric Warfare . . .,* 205.

[247] *Ibid*., 208.

[248] *Ibid*., 218.

[249] *Ibid*., 229.

8.1.1 Concepts and strategies

Norway is on the correct path with the introduction of NCW, and as discussed in paragraph *6.1 Norwegian defence policy* there is a focus on 'network thoughts' as one of the overarching principles in the Joint Doctrine.[250] The Norwegian Joint Doctrine defines 'network thoughts' as:

> 'Network thoughts' are about development of human beings, organisation and technology, and how to organise the resources effectively to achieve increased system integration, situational awareness and an understanding of the commander's intent. This doctrine uses the term 'network thoughts' to emphasise that the NCW concept shall not the seen as a final and 'correct' ideal condition, but that network-centric must be understood as a continuous development process going on in an interaction between the organisation and the individual.[251]

The focus on 'network thoughts' is so far only implemented in the Joint Doctrine and there is still work to be done before this approach is included in the underlying document structure and throughout the organisation in the NAF.

8.1.2 Technology development

There are no signs that there will be any changes either in the organisational structure of the Norwegian Defence Logistics Organisation (NDLO) who is responsible for the procurement in the NAF, or in the way procurement is done. NDLO has been through several changes during the recent years and the last big change was a reorganisation from a service oriented organisation to a joint organisation where the services' functional departments were merged, e.g. one department for artillery instead of one army, one navy and one air force. Since this was a relatively large structural reorganisation, the plan is to avoid further reorganisations for some years in order to calm

---

[250] Forsvarets Fellesoperative Doktine (The Armed Forces' Joint Doctrine), Forsvarsstaben, Oslo, June 2007, 55.

[251] *Ibid*., 55.

down and settle the organisation.[252] However, the reorganisation into a more joint organisation is probably an enhancement of the organisation to handle issues related to NCW from a joint point of view. NCW issues can now be dealt with within one office instead of reaching agreements from three service offices.

NDLO is responsible for the procurement based on the operational requirements from the user environment. When the user environment has delivered the operational requirements they are not normally involved again until the product is ready for service. The proposed changes in the CHOD Norway Defence study do not indicate any changes to this practise.[253] Even though the procurement organisation has become more 'joint' and by that better suited to handle joint NCW challenges, the time consuming procurement process itself is not optimised to meet the new challenges requiring user involvement, prototyping and testing throughout the development of the technology.

8.1.3 Experimentation

When is comes to experimentation as a criterion Norway is relatively well prepared. Norway established the Norwegian Battle Lab & Experimentation (NOBLE) as the first battlelab in Europe in 1999. So far, NOBLE has within the area of NCW experimented within command and control components, chat systems and the human aspect of network organizing.[254] The results from the experimentation are important inputs regarding technological possibilities and human computer interface lessons learned

---

[252] Forsvarsstaben, *Forsvarssjefens Forsvarsstudie . . .,* 50.

[253] *Ibid*.

[254] Norwegian Battlelab and Experimentation (NOBLE) webpage. http://www.battlelab.no; Internet; Accessed 12 March 2008.

both to those planning implementation of and writing requirements for future systems, and to those currently developing such technology.

8.1.4 Education and training

Introduction of NCW technology requires both organisational changes and changes in individual's duties and responsibilities. As presented above the individual changes are related to attitudes, acceptance of more responsibility, new skills, new approaches, and operation of new systems in a 'faster-paced environment'. Alberts et al predict that there is a need for fewer, but more educated and trained individuals in the future.[255] Even though there has been advanced technical equipment in use by the military before, NCW introduces even more complex systems[256] requiring better understanding at all levels in the organisation. NCW will also require use of technology by personnel categories not previously involved with such technology. This will require that NCW is part of all education and training to achieve a better understanding of NCW concepts, possibilities and limitations at all levels within an organisation in addition to concrete user training on different systems. This will probably also imply that there is a need to look at how recruitment is done to find the right people to educate and train to fully utilise NCW. [257]

One source to look at the level of knowledge and the education and training part is the curriculum at the Army, Navy and Air Force Academy. The major part of the curriculum at the three services Academies is, not surprisingly, given to military

---

[255] Alberts et al, *Network Centric Warfare . . .,* 229.

[256] Complex systems are described in paragraph *4.4 Increasing complexity of military systems.*

[257] Alberts et al, *Network Centric Warfare . . .,* 230.

leadership, military knowledge and international and security politics.[258] However, the future Maritime Surface and Subsurface (MARS) officers curriculum have a 'communications and C2IS' module consisting of 160 hours of lectures where only 2 hours are for NCW knowledge and 8 hours for practise on the NORCCIS II map system, while the remaining time is related to traditional military and maritime communications.[259] The weapon system engineers are educated within network technology and other technical skills, but only within the technical part, not the operational implementation and utilisation of such technology. Further they are not given the same amount of education within maritime operations as the MARS officers and are lacking skills in such topics. [260] The army is a little bit better as NCW is included in their schedule, but again only as a small part of a topic called military technology.[261] Not surprisingly is the Air Force leading the NCW part of the education as the Air Force Academy teaches understanding of NCW concepts related to air operations.[262] These are examples of what the cadets graduating now and those who are going to graduate as officers from 2011 are learning today. NCW is starting to be included in the curriculum, but so far only as an introduction. The curriculum clearly indicates that the policy and ambition set by the CHOD will not be met.

---

[258] Sjøkrigsskolen, *Fagplaner for Sjøkrigsskolens Bachelorprogram, Felles officersfag* (Bergen: SKSK Norge, 2005), 2-19.

[259] Sjøkrigsskolen, *Fagplaner for Sjøkrigsskolens Bachelorprogram, Lederskap med fordypning i nautikk* (Bergen: SKSK Norge, 2005), 16.

[260] Sjøkrigsskolen, Fa*gplaner for Sjøkrigsskolens Bachelorprogram, Lederskap med fordypning i elektronikk og data* (Bergen: SKSK Norge, 2005), 32.

[261] Krigsskolen, *Studiehåndbok 2007-2008, Bachelor i militære studier* (Oslo: KS Norge, 2007), 25.

[262] Luftkrigsskolen, *Studiehåndbok for LKSK kull 58* (Trondheim: LKSK Norge, July 2007), 15.

8.1.5 Criteria for success - Conclusion

Even though Norway meet the criterion such as 'experimentation' relatively well, and meet the criterion 'Concepts and strategies' partly by a 'top level joint doctrine' setting the condition for further doctrinal development, there are still room for improvement within 'Technology development' and 'Education and training'. The last two areas need significant changes in order to be ready for both today's and the future's challenges of implementing NCW.

8.2 Norway's NCW ambition

Norway has a relatively high ambition for implementation of NCW. The 'Defence Study 07' issued by the Norwegian CHOD fall 2007 states the following

> . . .the importance of NCW for the total efficiency of the Norwegian Armed Forces is so high that the cost of investment, operation and maintenance of the communication networks gives a higher effect that if the same resources were used to invest in a larger number of autonomous weapon systems and platforms. The NAF will, as other countries in the alliance and the industrialised part of the world, have a high level of ambition for the implementation of NCW.[263]

However, Norway has recognised the fact that, because of the high cost related to the development of defence materiel, it will not be possible for a small country to keep pace with the development continuously. Even though there is a high level of ambition for implementation of NCW it must also be a realistic and sober-minded level of ambition with priority on procurement of the capabilities giving greatest operational effect, and to invest in similar type of materiel as Norway's allies and coalition partners within the framework of multinational cooperation.[264]

---

[263] Forsvarsstaben, *Forsvarssjefens Forsvarsstudie . . .,* 10.

[264] *Ibid.*, 10.

The CHOD's 'Defence Study' also recognise the fact that conflicts are seldom solved by use of technology alone and technology suitable in one type of operation may not necessarily be suitable in another kind of operation. Based on this the NAF should be prepared and equipped to counter a widest possible spectrum of tasks and this will again have implication on the materiel standard.[265] The 'Defence study' is emphasising the separation of sensor, decision maker and shooter as one of the major benefits by introducing NCW. Better range and precision on fire effects is over time expected to give a better opportunity for long range effects both against land, sea and air targets and by that increase the joint capability, flexibility and contribute to mutual amplification between the services.[266] One of the other reasons for going along the path of NCW is the large national surveillance area in the Norwegian territorial waters and economic zone. Connecting several platforms as maritime patrol aircrafts, coast guard vessels, naval ships, combat aircrafts and shore based sensors together in a network and under joint command increase the capability for exercising authority, maintain sovereignty and crisis management.[267]

Based on the recognition of a smaller armed forces and the need to utilise information technology and networked capabilities both joint and combined, the 'Defence study 07' recommends a high level of ambition for the development of NCW:

> The goal is that network based capabilities and network thoughts shall be integrated in NAF within 2012. Norway shall accompany NATO's development within this area and not underlie within any areas. Norway shall

---

[265] Forsvarsstaben, *Forsvarssjefens Forsvarsstudie . . .,* 9.

[266] *Ibid*., 10.

[267] *Ibid*., 10.

> as a minimum be in line with the most important countries Norway cooperate with.[268]

This means that Norway's ambition is to achieve the NCW 'transitional' phase within 2012. When it comes to the 'initial' phase the ambition is around 2008-2009 while it is estimated that is not possible to achieve the 'mature' phase before around 2030.[269] The three phases will be further described and discussed below.

Even though countries like Norway would like to have a sober-minded approach to technological standard and renewal of defence materiel the national freedom of action is limited especially when it comes to cost reduction. This is mainly due to the fact that the Norwegian Armed Forces technological level is determined by two conditions:

- The NAF's material and equipment cannot be older nor have a lesser quality than the material of an adversary that can be met in war. This is based both on operational requirement based on the possibility for mission success, and ethical requirement to achieve a high degree as possible to ensure the personnel's safety and survivability.
- The NAF's material and equipment should not be of lesser quality than the Norwegian allies' corresponding equipment in order to ensure interoperability with allies both in national and international operations.[270]

Normally, the defence industry in western countries does not produce materiel of lower standards or quality. [271] The alternative is to buy older, used equipment other countries are phasing out. Buying such equipment might be less expensive and seem like a good idea seen from a pure investment point of view, but normally such an approach will lead to increased cost for operation and maintenance and increase the life-cycle cost, and

---

[268] Forsvarsstaben, *Forsvarssjefens Forsvarsstudie . . .,* 6.

[269] Forsvarets Overkommando, Forsvarssjefens militærfaglige utredning 2003 – Vedlegg B – Arbeidsutvalg NBF (Oslo: FO Norge, October 2002), 15-18.

[270] Forsvarsstaben, *Forsvarssjefens Forsvarsstudie . . .,* 9.

finally lead to a need to replace the equipment earlier that if new equipment were procured.[272] Basically this cyclical problem implies the need to stay in front of the technological development both because of interoperability and fire power, which again will be a cost driver.

8.3 Norway's level of ambition versus the NCW capability model

In order to evaluate the progress of the development and implementation of NCW different models have been developed. Alberts propose three models as a basis for the development: NCW capability model; NCW value chain; and inherent characteristics of Information Age organisations.[273] For the purpose of this paper the NCW capability model will be used to analyse the NCW development and implementation in Norway. There are mainly two reasons for using this model: first it can be used to make a snapshot at any time to decide the status of the development of the NCW capability,[274] second the Norwegian levels of ambition fit more or less directly into the levels of the NCW capability model.

8.3.1 The NCW capability model

The 'Capability Model' is based around four values describing the maturity of the NCW capability considering two aspects of network-centric behaviour: First, the process of developing situational awareness, second the nature of command and control. The lower end of the scale, value 0, describes platform-centric operations, and the upper end, level 4, describes mature network-centric operations involving:

---

[271] Forsvarsstaben, *Forsvarssjefens Forsvarsstudie . . .,* 9.

[272] *Ibid*., 9.

[273] Alberts, *Information Age Transformation . . .,* 88.

> . . . widespread information sharing, the development of a fully integrated common operational picture (COP) that promotes shared awareness, collaborative planning processes, and a self-synchronizing approach to command and control.[275]

The model is visualised in Figure 1 - NCW Levels of Application Maturity.[276] At Value 1 there is ability to share information to achieve improved awareness. Value 2 includes in addition some form of collaborative planning among the participants, and Value 3 involves even richer collaboration with more actors and integration. Finally at Value 4 self-synchronisation must be possible based on integrations across ". . . *doctrine, organization, training, material, and other aspects of the force and its supporting systems.*"[277]

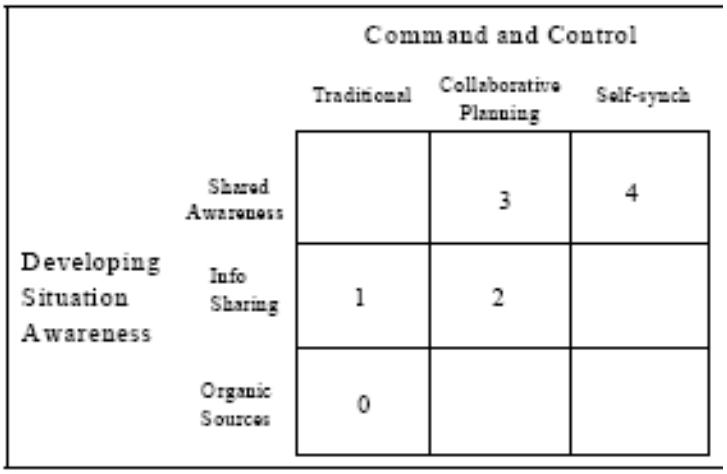

Figure 1 - NCW Levels of Application Maturity

8.3.2 The Norwegian Capability model

The Norwegian Armed Forces has developed a similar model but with three levels describing the phases of NCW development and implementation.[278] The three levels are

---

[274] Alberts, *Information Age Transformation . . .*, 87.

[275] *Ibid*., 242.

[276] Department of Defense, *Network Centric Warfare Department of Defense Report to Congress,* Report Prepared for the U.S. Congress (Washington: DoD U.S. 27 July 2001), 8-5; Internet; http://www.dodccrp.org/files/ncw_report/report/ncw_cover.html; accessed 12 March 2008.

[277] Alberts, *Understanding Information Age Warfare*, 242.

also similar to the three NEC states used in the UK in their approach to Network Enabled Capability: 'initial, transitional and mature'. [279] The three phases cover level 1 to 4 in the NCW capability model as NCW capability model level 0 is defined to be platform-centric. The Norwegian phase 'initial' equals the NCW capability model level 1, 'transitional' equals something in between level 2 and 3 and finally 'mature' equals level 4. The characteristics of the 'initial' and 'transitional' are included in the analysis of each phase in paragraph *8.3.3 Analysis of the Norwegian capability model*. However, the 'mature' phase which is supposed to be implemented around 2030 is so far into the future and is more like a 'vision' and will not be discussed in the analysis. Therefore the description of the 'mature' phase is included here to give an overview of the Norwegian NCW vision for 2030.

'Mature' NCW is in the Norwegian Joint Doctrine described as follows:

> 'Mature' NCW is networked based in all activities with a dynamic organisation adapted to the situation and able to run parallel processes with emphasise on horizontal coordination. There will be an entirety based infostructure everybody can access. A thorough information management is implemented to ensure that the information is available, understandable and possible to exploit for those who need the information. Technological, organisational and procedural interoperability are present within the organisation and there are some interoperability with relevant and prioritised actors and departments outside the organisation. The personnel are specialised and independent with ability to cooperate. The person chosen to do a specific task is determined by competency. Information technology is used both to rationalise and make possibilities. 'Mature' NCW have better cost efficiency than 'transitional' NCW. [280]

---

[278] Forsvarsstaben, *Forsvarets Fellesoperative Doktrine,* 97-98.

[279] Ministry of Defence, Network Enabled Capability, 10.

[280] Forsvarsstaben, *Forsvarets Fellesoperative Doktrine*, 98.

'Mature' NCW has a relatively high ambitions related to 'the network', a dynamic organisation, horizontal coordination, interoperability in several levels and knowledge requirements.

8.3.3 Analysis of the Norwegian capability model

Both the 'initial' and the 'transitional' phase will be analysed against today's status and plans in order to give a picture of the NCW development and implementation in Norway. It is important to keep in mind the dates given for when the phases should be reached. The 'initial' phase should be reached within 2008-2009. In other words, parts of this phase should more or less already be in place. The expressed ambition is to reach the 'transitional' phase in 2012[281] which is relatively optimistic compared to other countries like the UK[282] and Australia[283] who set 2015 as dates for this phase.

8.3.3.1 Initial phase

One of the characteristics of the 'initial' phase is that good knowledge of NCW is required and that NCW is part of all education and training. [284] The source used to evaluate education and training against the criteria for success was the curriculum at the Army, Navy and Air Force Academy and it is also valid here. As shown in paragraph '*8.1 Norway's status versus Alberts' criteria for success*' there are not much NCW included in the curriculum so far. And a change in the curriculum now will not give any benefits related to the 2008-2009 goal set for the 'initial' phase as the cadets will be graduated as officers before the change can take effect.

---

[281] Forsvarsstaben, *Forsvarssjefens Forsvarsstudie . . .,* 16.

[282] Fish, "NCW Development in Small Countries," 32.

[283] Australia. Dept. of Defence. Office of the Chief Information Officer. *A Concept for Enabling Information Superiority & Support*. Canberra, ACT: Dept. of Defence, 2004, 21.

Another characteristic related to education and training is that the personnel will be a combination of generalists and specialists.[285] There will always be a combination, but this is related to NCW and should be understood as NCW specialists. With today's education system the amount of specialists are those with special interest in NCW that have acquired this knowledge more or less by themselves as there are no possibilities that they could have got it through the education system. Until the education system changes there will be a majority of generalists in the NAF when it comes to NCW.

There should also be a separation between the daily operation and operations, education and training with a higher integration level of NCW in the latter.[286] However, today it is the opposite. The administrative system FISBasis[287] introduced in 2001 is continuously updated with administrative and support applications while the effort has not been similar when it comes to implementing NCW in operations, education and training.

The organisation should be characterised by relatively small changes in sequential processes while at the same time there should be increasing use of horizontal coordination.[288] The CHOD Defence Study[289] presented in the fall 2007 does not give any indication of any proposed organisational changes except relocations and closing

---

[284] Forsvarsstaben, *Forsvarets Fellesoperative Doktrine*, 97.

[285] *Ibid*., 97.

[286] *Ibid*., 97.

[287] Forsvarets Informasjonsssystem Basis – The basic IT platform for all Norwegian administrative application. It connects all NAF organisations and employees into one common network.

[288] Forsvarsstaben, *Forsvarets Fellesoperative Doktrine*, 97.

[289] Forsvarsstaben, *Forsvarssjefens Forsvarsstudie . . .*

down of installations and bases. The concept of horizontal coordination is neither described as a new approach in the Defence Study, nor as a concept for operations in the Joint Doctrine issued in June 2007.[290] The organisation will most likely be as it is with minor changes, and there are no signs that horizontal coordination will be a reality within 2008-2009.

The technical infrastructure will mainly consist of existing equipment but some enhancements and individual solutions might be used when appropriate.[291] As presented in paragraph '*5.2 Examples of NCW technology in use in Norway*,' there are some NCW systems available today. Some are mainly for use within the different services, some joint between two services and finally NORCCIS II, intended to be the major joint system. The technical infrastructure is in line with the relatively sober-minded ambitions for the 'initial' phase.

There should be a common network for selected components providing situational awareness.[292] The only Norwegian NCW 'tool' planned to do this is as presented above the NORCCIS II. The systems is based on COTS technology and relatively simple to implement. The challenge is integration towards other systems and communications.[293] There are no possibilities for sensor input to NORCCIS II so target information must come as tracks from other systems or by manual input.[294] Communication is mainly

---

[290] Forsvarsstaben, *Forsvarets Fellesoperative Doktrine*.

[291] *Ibid*., 97.

[292] *Ibid*., 97.

[293] Forsvarsdepartementet, *Fremskaffelsesløsning P6451 - SATCOM . . .*, 9.

[294] Norwegian Defence Logistics Organisation - Communication Information Systems (NDLO/CIS), http://www.c2is.net/nii/services/maritimec2.html; Internet; Accessed 24 march 2008.

based on satellite communication or landlines, which gives challenges especially for integration in small, mobile units.[295] The common network described as a characteristic for the 'initial' phase can probably be established by use of NORCCIS II for selected components, but the integration problems, both when it comes to sensor inputs and communications are clear indications that there could be problems achieving situational awareness.

Interoperability should be prioritised for components within an operation.[296] It seems that this has been a priority in the operations where NCW technology has been used. The use of NORCCIS II in current operations has focused on interoperability against similar systems to exchange messages, command and control, and information exchange to achieve situational awareness within the alliance or coalition. Similarly has other systems been taken into use to achieve interoperability within single operations, e.g. implementation of 'Battleforce e-mail' in accordance with STANAG 5066 during the Norwegian naval contribution to UNIFIL II.

8.3.3.2 Transitional phase

The 'transitional' phase is characterised by similar description as the 'initial' phase but with a higher level of ambition. The daily operation should in this phase be mainly network based.[297] As discussed under the 'Initial phase' this is already more or less the case and there is a continuous development in this area. However, the concepts and

---

[295] Forsvarsdepartementet, *Fremskaffelsesløsning P6451 - SATCOM . . .*, 9.

[296] Forsvarsstaben, *Forsvarets Fellesoperative Doktrine*, 97.

[297] *Ibid*., 97.

doctrines should also be mainly network based.[298] The last update of the Joint Doctrine was issued in June 2007, 7 years after the first version of the document. This is an indication that update of documents to meet new challenges takes time. In addition to this, concepts and doctrines are closely linked to the technology, and when the technology is not available throughout the organisation there will also be a problem with the concepts and doctrines. The goal is, as already mentioned, both within the 'Defence Study' and the 'Joint Doctrine' that there should be an increased focus on networked operations, but it is difficult, if not impossible, to achieve this until the technology are available. This is because of the fact that knowledge of how to use the technology is important inputs when it comes to writing concepts and doctrines.

The organisation should be more horizontally oriented than in the 'initial' phase.[299] The 'Defence Study' has a 20 year perspective but focuses mainly on, and gives concrete recommendations for 2009-2012[300] and does not give any indications of a change to a more horizontally oriented organisation. However, the fact that more dynamic types of organisations and processes will be used in some situations might be a reality. In general the NAF is able to quickly adapt to new challenges and establishing ad hoc organisation when needed.[301] Taking this into account more horizontally oriented organisations might be established when there is a need.

---

[298] Forsvarsstaben, *Forsvarets Fellesoperative Doktrine*, 97.

[299] *Ibid*., 97.

[300] Forsvarsstaben, *Forsvarssjefens Forsvarsstudie . . .,* 3.

[301] Regjeringen, *Stortingsproposisjon nr 48 (2007-2008), "Et forsvar til vern om Norges sikkerhet, interesser og verdier,"* (Oslo: FD Norge, March 2008), 13.

Another of the characteristics describing the organisation states that the organisation will be mostly static with focus on military interoperability.[302] Military interoperability in this context should be understood to be the non-technological part of interoperability, i.e. human and the organisational aspects. The facts described above indicate that this characteristic could be fulfilled. The organisation seems to be relatively static, but with the possibility to adapt when needed.

In the 'transitional' phase the number of specialists should have increased.[303] If this should be achieved before 2012 these specialists should be within the educational system now. And as shown about the education system the curriculum at the academies does not give such an education. The educational system might change during the next years but that is not sufficient to gain a significant increase in number of specialists from 2012.

The use of information technology and communication should in the 'transitional' phase be an innovative tool. [304] This must be seen in conjunction with the number of specialists available, and when there is a lack of specialists there is not likely that this will happen as early as 2012. Contractors with special skills could be hired to help out, but they again have to be educated and trained in military business.

Old and new equipment should be used together in a network.[305] This is partly achievable due to the fact that several of the old systems already are networked and are

---

[302] Forsvarsstaben, *Forsvarets Fellesoperative Doktrine*, 97.

[303] *Ibid*., 97.

[304] *Ibid*., 97.

[305] *Ibid*., 97.

partly interoperable with the NORCCIS II, e.g. both Link 11 and Link 16 messages can be imported by NORCCIS II.[306] Related to this is the interoperability issue where the ambition is interoperability to a large extent internally in the NAF.[307] Even though there is a possibility to import different types of data into NORCCIS II, it is not possible to import messages from NORCCIS II into the older systems. This complicates the issues for the units with both old equipment and NORCCIS II as they need to use both systems to achieve situational awareness. In general it is a fact that interoperability can be achieved internally if everybody is using NORCCIS II, but if there is a mixture of old equipment involved the interoperability issue is more complicated.

There should be a common communication network and a management of the information to enable all users in need of information access.[308] The common communication network will mainly be served by the planned SATCOM space segment as other communication means do not give the necessary bandwidth. The plan for the SATCOM space segment is that it should be in operation from 2012, but the final decision, including funding, is not taken yet.[309] And if the space segment is ready from 2012 there will still be challenges related to control the system and get everybody of the users interoperable with it, as well as education and training. The ambition is also to manage the information available to ensure all users get the information they need. Such a management has to be performed at the operational headquarters which is the central

---

[306] Forsvarsdepartementet, *Fremskaffelsesløsning P6451 - SATCOM . . .,* 9.

[307] Forsvarsstaben, *Forsvarets Fellesoperative Doktrine*, 97.

[308] *Ibid*., 97.

[309] Stortinget, *Stortingsinnstilling nr.287 (2006-2007), "Investeringar i Forsvaret,*" (Oslo: St.t. Norge June 2006), 8.

node in the NORCCIS II for command and control, information management and situational awareness. The headquarters are doing this in a smaller scale today and will probably be capable to handle this in a larger scale in 2012. The problem related to this is whether it is possible to gain a shared situational awareness as the sensor inputs will have different accuracy and there will be time delays. The common operational picture (COP) is far from 'near real-time' and the problem is that different users have different need for detailed data or information. If the goal is to share a 'strategic picture' NORCCIS II might solve this, while it will not be able to give a 'tactical picture'.

It is also said that the 'transitional' phase is characterised by more uncertainty because big investments in technology are necessary to replace old equipment. [310] As discussed in paragraph '*6.4 Economy and budget'* the Norwegian investment budget is more or less already committed to bigger investments. The new 'long term plan'[311] presented 28 March 2008 outlines the governments plan for the NAF in the period 2009-2012, and will be decided by the Norwegian parliament during spring 2008. In this plan the investment budget is reduced by $ 305 million pr year (down to $ 1.2 million) in order to finance operations and maintenance of the existing structure and the commitments in ongoing operations.[312] Taking into account the ongoing investments and their 'piece of the cake' this reduction in the investment budget gives even less possibilities for spending money on NCW technology.

---

[310] Forsvarsstaben, *Forsvarets Fellesoperative Doktrine*, 97.

[311] Forsvarsdepartementet, *Stortingsproposisjon nr 48 (2007-2008)*.

[312] *Ibid*., 134.

8.4 Norwegian ambition level - Conclusion

For a small country with restricted defence budgets the Norwegian ambition is relatively high. As shown there will be problems for Norway within several areas even though Alberts' criteria for success gives an indication that something is done correctly to prepare for the implementation of NCW. However the four criteria are not even halfway fulfilled. The analysis of the two first ambition levels, 'initial' and 'transitional' in the Capability model shows several shortcomings that will be difficult to overcome in time to fulfill the ambitions. The severity of the shortcomings differ as some are more fundamentally originated in the organisation and educational system and by that need time to get solved, while others, like the technical ones could be solved in time by putting more money into the NCW development and implementation. However, it is not likely that it will happen as it seems that the Norwegian investment budget will be further decreased to ensure operations and maintenance of the existing structure. Based on the analysis of the 'initial' and 'transitional' phases it is unlikely that Norway will be able to reach its ambition of achieving the 'initial' phase in 2008-2009 and 'transitional' phase in 2012.

9 Conclusion

The idea behind NCW emerged from the use of information technology in the retailing industry and Cebrowski and Gartska conceptualized this into how NCW could be used for military purposes. The theory behind NCW is an important input when trying to understand NCW, its impact on technology and the organisations in the future, and to understand both the advantages and challenges NCW will impose on the military. The complexity of NCW is important to keep in mind as this gives bigger challenges for smaller countries than bigger due to lack of, or limited resources.

It is quite obvious that it would not have been such eagerness present in the NCW pursuing countries if it had not been possible to gain military advantages by implementing NCW. The 'tenets of NCW' provides a good summary of the advantages:

> A robustly networked force improves information sharing.
> Information sharing and collaboration enhances quality of information and shared situational awareness.
> Shared situational awareness enables collaboration and self synchronisation.
> These, in turn, dramatically increase mission effectiveness.[313]

Shared situational awareness is a key output from using NCW and this again more or less enables and provides the other advantages such as collaboration, self synchronisation, increased tempo, command and control and improved tactics. Advantages such as reduced sensor-to-shooter time is also essential but is again more a result of the network itself and not the situational awareness. As the main output of NCW is increased mission effectiveness it is something all nations pursue. However it is, due to limited resources, even more interesting for small nations.

---

[313] Alberts. *Information Age Transformation . . .,* 8.

As with almost all types of technology there are not only advantages, but also challenges when implementing NCW. Several challenges have been presented in this paper. Some are related to knowledge and perception of NCW and other again directly to the technology. Some of the challenges can be met by better education, training and simply time to let the system set within the organisation, and other challenges like the technological ones can be solved with more money into research and development or simply by buying better and more capable equipment. Small nations must decide and define how much effort and resources to put into meeting these challenges. For some of them the best solution might be to let time solve it, simply by ignoring it until someone with more resources and capabilities has a solution to the challenges.

Important experience is made everyday both in today's conflicts in Iraq and Afghanistan, and in exercises. The experience shows advantages and challenges, but it also shows where the focus is in today's use of NCW technology. Situational awareness and shared situational awareness are as shown important issues and is, not surprisingly, the main focus in several reports from use of NCW technology. The blue Force Tracker has been a significant contributor to the increased shared situational awareness, while one of the problems has been to disseminate information downwards in the organization to those who need it. The experience so far shows the importance of continuing using NCW technology to get lessons learned for future development.

To give a picture of the status of NCW technology within a small country the Norwegian inventory has been briefly presented. Norway is implementing new systems like the Link-16 and is continuing the development and implementation of the NORCCIS II command and control system. There is a heavy reliance on the NORCCIS II both as a

tri-service and combined NCW enabler. However, this is an example of a small country's approach to NCW. There are not resources available to make a major change and introduce NCW throughout the armed forces in one step. Instead small steps are made by implementing equipment piece-by-piece in a small scale, ensuring NCW capability on new platforms like ships, aircrafts and vehicles introduces and by developing the equipment already in service.

In order to be fully utilised NCW should be introduced from the top level and be a part of the overall policy. As the world has changed since the end of the Cold War so have also the defence policies in most western countries. A common theme in the defence policies is that both the defence of their own country and participation in international operations is emphasised. Further NCW is introduced as an enabler for future advantages and as a basic function of the armed forces.

The Norwegian Armed Forces has been briefly described to give an example of a small nation's military capabilities. Together with relatively small sized armed forces comes a limited defence budget, which again also implies limited investment budgets. Norway as an example has its investment budget more or less obligated long time in the future due to the need for implementation of expensive platforms like new fighter aircrafts and submarines, leaving less money for other future investments.

A common theme among small nations is that they seem to have a relatively sober-minded ambition level related to a large and comprehensive introduction of NCW. Using existing equipment and slowly develop and build on what already is in service is a general approach together with the focus on using NCW to get 'shared situational

awareness'. The biggest challenge seems to be related to cost which again forces smaller countries to be sober-minded in their approach to NCW.

Norway's status and level of ambition are discussed separately. The status in Norway today has been compared with criteria for success outlined from Alberts et al.[314] Norway does not even meet the four criteria more than halfway. The analysis of the two first ambition levels, 'initial' and 'transitional' in the 'NCW capability model' shows several shortcomings that will be difficult to overcome in time to fulfill the ambitions. The severity of the shortcomings differ as some are more fundamentally originated in the organisation and educational system and by that need time to get solved, while others, like the technical ones could be solved in time by putting more money into the NCW development and implementation.

Even though the pronounced ambition in the top level documents is relatively high, Norway does not have the status necessary for a successful implementation of NCW yet. This problem seems to continue into the future as the ambition levels set for 2008-2009 and 2012 will also be difficult to meet; first due to the fact that today's status is not at a sufficient level to support the ambitions relatively close in the future, second, in order to meet the ambition there should already have be initiated changes, e.g. in the educational system, to prepare the basis for meeting the future ambitions. Plans to solve these problems are not present and the limited investment budget does not give any room to solve the challenges by spending more money. Facts and predictions presented show that Norway will not be able to reach its ambition of achieving the 'initial' phase in 2008-2009 and 'transitional' phase in 2012.

---

[314] Alberts et al, *Network Centric Warfare . . .,* 199-229.

There is no doubt that NCW will be a part of the NAF in the future and that challenges described can be overcome, but a more thorough analysis of the NCW status today and the planned and executed future changes to prepare for NCW implementation is needed to establish realistic future levels of ambition.

Appendix A - List of abbreviations

ACCS	Air Command And Control System
ACO	Airspace Control Order
ATO	Air Tasking Order
BFT	Blue Force Tracker
C2	Command and control
C2IS	Command Control Information System
C4IS	Command, Control, Communication, And Computer Information Systems
CAP	Combat Air Patrol
CAS	Combat Air Support
CHOD	Chief of Defence
CMS	Combat Management System
COP	Common Operational Picture
COTS	commercial off the shelf
DISA	Defense Information Systems Agency
EMP	Electromagnetic Pulse
EW	Electronic Warfare
FBCB2	Force XXI Battle Command Brigade and Below
FD	Forsvarsdepartementet
FDF	Finnish Defence Forces
FiNED	Finnish Network Enabled Defence
FO	Forsvaret Overkommando (Changed name to Forsvarsstaben in 2003)
FPB	Fast Patrol Boat
FST	Forsvarsstaben
GBAD	Norwegian Ground Based Air Defence
GIG	Global Information Grid
GPS	Global Positioning System
HF	High Frequency
HUMINT	human intelligence
ICW	Information Centric Warfare
ISTAR	Intelligence Surveillance Target Acquisition Reconnaissance
IT	Information Technology
JDAMs	Joint Direct Attack Munitions
JSAT	J-message Sattelite Transmission
MARS	Maritime Surface and Subsurface
MLU	Mid Life Update
MMHS	Military Message Handling System
MOD	Ministry of Defence
MPA	Maritime Patrol Aircraft
NADGE	NATO Air Defence Ground Environment
NAF	Norwegian Armed Forces
NASAMS	Norwegian Air-force Surface to Air Missile System
NATO	North Atlantic Treaty

NBD	Network Based Defence
NCC	Network Centric Capabilities
NCO	Network Centric Operations
NCS	Net Control Station
NCW	Network Centric Warfare
NDLO	Norwegian Defence Logistics Organisation
NEC	Network Enabled Capabilities
NEC CCIS	Northern European Command-C2 Information System
NFN	Naval Fires Network
NOBLE	Norwegian Battle Lab & Experimentation
NORCCIS II	Norwegian Command and Control Information System II
NORDIS-S	Norwegian Defence Information Services Secure
NoTG	Norwegian Task Group
OIF	Operation Iraqi Freedom
OODA	Observe, Orient, Decide, Act
RAP	Recognised Air Picture
RLP	Recognised Land Picture
RMA	Revolution in Military Affairs
RMP	Recognised Maritime Picture
SATCOM	Satellite Communication
SBBCS	Stryker Brigade Battle Command System
SBCT	Stryker Brigade Combat Team
STANAG	Standard Agreement
TCP/IP	Transmission Control Protocol/Internet Protocol
TES	Tactical Exploitation System
TPT	Third Party Targeting
TST	Time Sensitive Targeting
UAV	Unmanned Air Vehicle
UHF	Ultra High Frequency
UNIFIL	United Nations Interim Force In Lebanon

Bibliography

"Defense Watch." *Defense Daily*, 21 Jan 2003, 1.

"For the First Time, Soldiers are Connected to the Tactical Internet." *Defense Daily* 231, no. 66 (Oct 9, 2006): 1.

"Krieg Reaffirms Imperative for Coalition Interoperability, but Says Process Will Take Time." *Defense Daily International* 7, no. 35 (Sep 8, 2006): 1.

"Navy Adds Component to Network Centric Warfare Plan." *Defense Daily* 211, no. 3 (Jul 5, 2001): 1.

"Studies Examining Role of Network Centric Operations in Iraq." *C4I News,* 14 Apr 2005, 1.

"Finnish Defence Forces – Network-Centric Operations." http://www-01.ibm.com/industries/government/ieg/pdf/finnish_defence_forces-nco.pdf; Internet; accessed 22 February 2008.

"Rumsfeld presses for more agile military," CNN.com, 31 January 2002, http://archives.cnn.com/2002/US/01/31/rumsfeld.speech. Accessed 2 March 2008.

Ackerman, Robert K. "Data Holds the Key to Network-Centricity." *Signal* 59, no. 5 (Jan, 2005): 37.

Alberts, David S. and Richard E. Hayes. *Power to the Edge : Command, Control in the Information Age*. Information Age Transformation Series. Washington, DC: CCRP Publication Series, 2004.

Alberts, David S. *Information Age Transformation : Getting to a 21st Century Military*. Information Age Transformation Series. Washington, D.C.: CCRP Publication Series, 2002.

Alberts, David S. *Understanding Information Age Warfare*. Washington, DC: CCRP Publication Series, 2001.

Alberts, David S., John Garstka, and Frederick P. Stein. *Network Centric Warfare : Developing and Leveraging Information Superiority*. CCRP Publication Series. 2nd (Rev.) ed. Washington, DC: National Defense University Press, 2000.

Australia. Dept. of Defence. Office of the Chief Information Officer. *A Concept for Enabling Information Superiority & Support*. Canberra, ACT: Dept. of Defence, 2004.

Betz, David J. "The More You Know, the Less You Understand: The Problem with Information Warfare." *Journal of Strategic Studies* 29, no. 3 (Jun, 2006): 505.

Blaker, James. "ARTHUR K. CEBROWSKI: A Retrospective." *Naval War College Review* 59, no. 2 (Spring, 2006): 129.

Brand, Stewart, "The Physicist", Wired, Sep 1995 http://www.wired.com/wired/archive/3.09/myhrvold.html, Internet; Accessed 4 April 2008.

Brewin, Bob, "*GAO: Future Combat Systems network still more concept than reality*," Government Executive, March 2008. [http://www.govexec.com/dailyfed/0308/0310008nn1.htm]

Brigadier Lamont Kirkland. "Future Challenges for Land Forces: A Personal View." *British Army Review* no. no. 142 (Summer 2007): 10-13.

Brooker, Martin. "How Will the Royal Australian Navy Realise the Benefits of Network Centric Warfare?" *Journal of the Australian Naval Institute* no. 122 (Summer 2007): 12.

Burke, Martin, "*Information Superiority Is Insufficient To Win In Network Centric Warfare*," Joint Systems Branch, Defense Science and Technology Organization, 2001, http://www.dodccrp.org/events/2000/5th_ICCRTS/cd/papers/Track4/024.pdf; Internet; Accessed 12 March 2008.

Campen, Alan D. "Information Operations may Find Definition and Validation in Iraq." *Signal* 57, no. 10 (Jun, 2003): 43.

Cateriniccia, Dan and French, Matthew, "*Network-Centric Warfare: Not There Yet*," Federal Computing Week, June 9, 2003. http://www.fcw.com/print/9_20/news/79869-1.html: Internet; accessed 8 March 2008.

Chaisson, Kernan. "MNF Addresses Time-Critical Targeting." *Journal of Electronic Defense* 24, no. 5 (May 2001): 16.

CWID - Coalition Warrior Interoperability Demonstration. http://www.cwid.js.mil/public/CWID06FR/htmlfiles/101sei.html; Internet; accessed 24 March 2008.

Dora, Johann-Georg. "Network Centric Operations and German Forces Transformation." *Military Technology* 29, no. 8 (Aug 2005): 53.

English, Allan D., Carol McCann, Richard Howard Gimblett, Howard G. Coombs, Canada. Dept. of National Defence, Defence R&D Canada, and KMG Associates. *Beware of Putting the Cart before the Horse : Network Enabled Operations as a Canadian Approach to Transformation*. DRDC Toronto Contract Report. Vol. CR 2005-212. Toronto: Defence R&D Canada - Toronto, 2005.

European Institute, "Transatlantic Interoperability in Defence Industries," Washington, D.C., 2002. http://www.europeaninstitute.org/pdf/IO.pdf; Internet: accessed 8 March 2008.

Evidence Based Research, Inc and United States. Dept. of Defense. Office of Force Transformation. *Network Centric Operations Conceptual Framework : Version 1.0*. Vienna, Va.: Evidence Based Research, 2003.

Ferster, Warren, "*Military Bandwidth Demand Energizes Market*," SpaceNews, September 2, 2003. http://www.space.com/spacenews/archive03/militaryarch_090203.html. Internet; accessed 8 March 2008.

Fish, Tim. "Insurgents Apply NCW Concepts Faster than the West." *Asia - Pacific Defence Reporter* 32, no. 7 (Sep 2006): 18.

Fish, Tim. "NCW Development in Small Countries." *Asia - Pacific Defence Reporter* 32, no. 7 (Sep 2006): 32.

Fisher, David and Smith, Dennis, "*Emergent Issues in Interoperability*," News@ SEI, 2004, No.3, http://www.sei.cmu.edu/news-at-sei/columns/eye-on-integration/2004/3/eye-on-integration-2004-3.htm; Internet; accessed 8 March 2008.

Forces Transformation and Resources. *Network-Centric Operations Case Study - Coalition Operations in Operation IRAQI FREEDOM (OIF): A U.K. Perspective of FBCB2/Blue Force Tracker (BFT) ARBRIDGED REPORT Version 1.0*. Report Prepared for the Office of Force Transformation in the Office of the Secretary of Defense. Transformation Case Study Series, 28 August 2007.

Forces Transformation and Resources. *Network-Centric Operations Case Study - The Stryker Brigade Combat Team ARBRIDGED REPORT Version 1.0*. Report Prepared for the Office of Force Transformation in the Office of the Secretary of Defense. Transformation Case Study Series, 28 August 2007.

French, Matthew and Tiboni, Frank, "*Tracking troop movement*," Federal Computer Week March 21 2004. http://www.fcw.com/print/10_7/mews/82386-1.html; Internet; accessed 24 March 2008.

French, Matthew, "Bandwidth in Iraq a subject of debate," Federal Computer Week, Oct. 20, 2003. http://www.fcw.com/print/9_39/news/81220-1.html; Internet; accessed 24 March 2008.

Friedman, Norman. "Making NEC Worthwhile." RUSI Journal 149, no. 6 (Dec 2004): 42.

Friedman, Norman. "NCW - Why should it be Worthwhile?" *Asia - Pacific Defence Reporter* 31, no. 5 (Jun 2005): 22.

Friedman, Norman. "Network-Centric Warfare in the Middle East." *United States Naval Institute.Proceedings* 132, no. 10 (Oct 2006): 90.

Friedman, Norman. "They Link it Together." *Naval Forces* 26, no. 3 (2005): 35.

Garstka, John J. "Network-Centric Warfare Offers Warfighting Advantage." *Signal* 57, no. 9 (May, 2003): 58.

Gonzales, David et al. *Network Centric Operations Case Study – The Stryker Brigade Combat Team*. Report Prepared for the Office of Force Transformation in the Office of the Secretary of Defense. Santa Monica: RAND Corporation, 2005.

Gonzales, David et al. *Network-Centric Operations Case Study - Air-to-Air Combat With and Without Link 16.* Report Prepared for the Office of Force Transformation in the Office of the Secretary of Defense. Santa Monica: RAND Corporation, 2005.

Gonzales, David et al. *Networked Forces in Stability Operations - 101st Airborne Division, 3/2 and 1/25 Stryker Brigades in Northern Iraq.* Report Prepared for the Office of Force Transformation in the Office of the Secretary of Defense. Santa Monica: RAND Corporation, 2007.

Gorbachev, Yu E. "Network Centric War: Myth Or Reality?" *Military Thought* 15, no. 1 (2006): 143.

Hamrin, Mats. "Netc4i: Web Based Approach for Coalition Interoperability." *Naval Forces* 26, no. 3 (2005): 37.

Horn, Bernd and Gizewski, Peter, Canada. Dept. of National Defence. Directorate of Land Strategic Concepts, and Canada. *Towards the Brave New World : Canada's Army in the 21st Century*. Kingston, Ont.: Directorate of Land Strategic Concepts, 2003.

Houghton, Peter and Defence Science and Technology Laboratory. *Potential System Vulnerabilities of a Network Enabled Force*. Malvern , Worcestershire, UK: Defence Science and Technology Laboratory, 2004.

Kenyon, Henry S. "Sweden Prepares to Command the Digital Future." *Signal* 60, no. 2 (Oct 2005): 30.

Kerr, Julian. "Networking the ADF: NCW Roadmap Released." *Asia - Pacific Defence Reporter* 31, no. 8 (Oct/Nov 2005): 6.

Langley, James A. G. "Network-Centric Warfare: An Exchange Officer's Perspective." *Military Review* 84, no. 6 (Nov/Dec 2004): 47.

Lawlor, Maryann. "Engineering Network-Centric Warfare." *Signal* 61, no. 12 (Aug 2007): 23.

Lescher, William K. "Network-Centric: Is it Worth the Risk?" *United States Naval Institute Proceedings* 125, no. 7 (Jul 1999): 58.

MacMillan, Kym. *Evolving command & control – The challenge for smaller defence forces*. Canberra City: CCRP Paper, 2004. http://www.dodccrp.org/events/2004_CCRTS/CD/papers/074.pdf: Internet: Accessed 28 February 2008.

Malham, Mark C. and Debora Gabbard. "Battle Command Systems: The Force XXI Warfighter's Advantage." *Military Review* 78, no. 2; 2 (03//Mar/Apr98, 1998): 33.

Manes, Stephen. "Dim Vista." *Forbes* 179, no. 4 (Feb 26 2007): 50.

Matsumura, John et. al. *Preparing for Future Warfare with Advanced Technologies*. Report sponsored by the United States Army. Santa Monica: RAND Corporation, Arroyo Center, 2002.

McKenna, Ted. "Right on Time." *Journal of Electronic Defense* 28, no. 4 (Apr 2005): 44.

McKenna, Ted. "The Network-Centric Craze." *Journal of Electronic Defense* 29, no. 5 (May 2006): 38.

Mitchell, Paul T. "Small Navies and Network-Centric Warfare: Is there a Role." *Naval War College Review* 56, no. 2 (Spring 2003): 83.

Moon, Terry. "Net-Centric Or Networked Military Operations?" *Defense & Security Analysis* 23, no. 1 (Mar 2007): 55.

NATO, "*AAP-6 - NATO Glossary Of Terms And Definitions*", Brussels: NATO, April 2008.

Norge. Forsvarets overkommando. *Forsvarssjefens militærfaglige utredning 2003 – Vedlegg B – Arbeidsutvalg NBF.* Oslo: FO Norge, October 2002.

Norge. Forsvarsdepartementet. *Fremskaffelsesløsning P6451 - SATCOM for Skjold-klassen.* Oslo: FD Norge, August 2006.

Norge. Forsvarsdepartementet. *Norwegian Defence 2006.* Oslo: FD Norge, 2006. http://www.regjeringen.no/Upload/FD/Dokumenter/FoF_2006_eng.pdf; Internet; accessed 22 March 2008.

Norge. Forsvarsdepartementet. *Styrke og relevans.* Oslo: FD Norge, 3 January 2005

Norge. Forsvarsdepartementet. *The Norwegian Defence Budget 2003*. Oslo: FD Norge, 2003.

Norge. Forsvarsstaben. *Forsvarets Fellesoperative Doktrine*. Oslo: FST Norge, June 2007.

Norge. Forsvarsstaben. *Forsvarssjefens Forsvarsstudie 2007 Sluttrapport.* Oslo: FST Norge, October 2007.

Norge. Krigsskolen. S*tudiehåndbok for 2007-2008 - treårig operativ grunnutdanning bachelor i militære studier.* Oslo: Krigsskolen Norge, juli 2008. http://www.krigsskolen.no/studiehandboker.html; Internet; accessed 18 March 2008.

Norge. Luftkrigsskolen. *Studiehåndbok for LKSK kull 58.* Trondheim: Luftkrigsskolen Norge, 2 juli 2007. http://www.mil.no/luft/start/karriere/Luftkrigsskolen/sbok/: Internet; accessed 18 March 2008.

Norge. Sjøkrigsskolen. *Fagplaner for Sjøkrigsskolens Bachelorprogram – Lederutvikling.* Bergen: SKSK Norge, høst 2007. http://www.mil.no/multimedia/archive/00102/Fagplan_Lederutvikl_102765a.pdf; Internet; accessed 18 March 2008.

Norge. Sjøkrigsskolen. *Fagplaner for Sjøkrigsskolens Bachelorprogram - Lederskap med fordypning i nautikk.* Bergen: SKSK Norge, høst 2005. http://www.mil.no/multimedia/archive/00102/Fagplan_Operativ_Ma_102773a.pdf: Internet; accessed 18 March 2008.

Norge. Sjøkrigsskolen. *Fagplaner for Sjøkrigsskolens Bachelorprogram - Felles offisersfag*. Bergen: SKSK Norge, høst 2005. http://www.mil.no/multimedia/archive/00102/Fagplan_Felles_offi_102766a.pdf; Internet; accessed 18 March 2008.

Norge. Sjøkrigsskolen. *Fagplaner for Sjøkrigsskolens Bachelorprogram - Lederskap med fordypning i elektronikk og data.* Bergen: SKSK Norge, høst 2005. http://www.mil.no/multimedia/archive/00102/Fagplan_Marineingen_102958a.pdf; Internet; accessed 18 March 2008.

Norge. Stortinget. *Stortingsinnstilling nr.287 (2006-2007) - Investeringar i Forsvaret.* Oslo: St.t. Norge, June 2006.

Norge. Stortinget. *Stortingsproposisjon nr 1 (2007-2008) - Statsbudsjettet for budsjettåret 2008 – Forsvaret*. Oslo: St.t Norge, 2007.

Norge. Stortinget. *Stortingsproposisjon nr 42 (2003-2004) - Den videre moderniseringen av Forsvaret.* Oslo: St.t. Norge, 2003.

Norge. Forsvarsdepartementet. *Stortingsproposisjon nr 48 (2007-2008) - Et forsvar til vern om Norges sikkerhet, interesser og verdier*, Olso: St.t. Norge, March 2008.

Norge. Stortinget. *Stortingsproposisjon nr 50 (2002-2003) - Anskaffelse av Taktisk Data Link-16 (TDL-16).* Oslo: St.t. Norge, March 2003.

Norwegian Battlelab and Experimentation (NOBLE). http://www.battlelab.no; Internet; accessed 18 March 2008.

Norwegian Defence Logistics Organisation - Communication Information Systems (NDLO/CIS) http://www.c2is.net; Internet; accessed 24 march 2008.

Norwegian Defence Logistics Organisation - Communication Information Systems (NDLO/CIS) http://www.c2is.net/nii/index.html; Internet; accessed 24 March 2008.

Norwegian Defence Logistics Organisation - Communication Information Systems (NDLO/CIS) http://www.c2is.net/nii/services/Common_functional.html; Internet; accessed 24 March 2008.

Norwegian Defence Logistics Organisation - Communication Information Systems (NDLO/CIS) http://www.c2is.net/nii/services/landc2.html; Internet; accessed 24 March 2008.

Norwegian Defence Logistics Organisation - Communication Information Systems (NDLO/CIS) http://www.c2is.net/nii/services/maritimec2.html; Internet; accessed 24 March 2008.

Olsson, Gustaf. "Defensive Aids Systems in Network Centric Warfare." *Military Technology* 28, no. 6 (Jun 2004): 70.

PA Consulting Group and Evidence Based Research, Inc. *A Network Centric Operations Case Study : USUK Coalition Combat Operations during Operation Iraqi Freedom*. Version 2.0 ed. Washington, DC: PA Consulting Group, 2004.

Perry, Walt L. *Network-Based Operations for the Swedish Defence Forces : An Assessment Methodology*. Santa Monica, CA: Rand Corporation, 2004.

Quijada, Sergio E. "A Hybrid Simulation Methodology to Evaluate Network Centric Decision Making Under Extreme Events." Ph.D. University of Central Florida, 2006.

Raskin, A. V. and V. S. Pelyak. "On Network-Centric Warfare." *Military Thought* 14, no. 2 (2005): 86.

Reitan, Bård K, Pålhaugen, Lene, Forventningene til nettverksbasert forsvar – 6 tema (FFI/Rapport-2004/04004), Kjeller: Forsvarets Forskningsinstitutt, 2004.

Richardson, Doug. "Network-Centric Warfare: Revolution of Passing Fad?" *Armada International* 28, no. 5 (Oct/Nov 2004): 62.

Roosevelt, Ann, "Army Considers Improving 'Oneness' of FBCB2 System." *C4I News,* 5 Feb 2004, 1.

Scarborough, Sheila. "Network-Centric Warfare Meets the Laws of the Navy." *United States Naval Institute.Proceedings* 127, no. 5 (May 2001): 30.

Schrage, Michael, "*Perfect Information and Perverse Incentives: Costs and Consequences of Transformation and Transparency*," Security Studies Program Working Paper, Massachusetts Institute of Technology, E38-600, May 2003.

Sherman, Jason. "The Secrets of Centric." *Sea Power* 48, no. 4 (Apr 2005): 16.

Simmons, Brian M. "Distributed Testing Develops a Network-Centric Warfare Capability for the Future Force." *Army AL & T* (Apr-Jun 2006): 56.

Statistisk Sentralbyrå (Statistics Norway). http://www.ssb.no/befolkning; Internet; accessed 23 March 2008.

Stein, Fred P, "Observations on the Emergence of Network Centric Warfare", http://www.dodccrp.org/files/stein_observations/steinncw.htm; Internet; accessed 2 march 2008.

Sweden. Regjeringskanseliet, "*The New Defence – prepared for the next millennium* (Short version of the Government Bill 1999/2000:30), Stockholm: Regjeringskanselliet Sweden, 2000.

Talbot, David, "*How Technology Failed in Iraq*", *MIT Technology Review*, November 2004, http://www.technologyreview.com/articles/04/11/talbot1104.asp: Internet; accessed 8 March 2008.

The Office of Force Transformation. Network-*Centric Operations Case Study - Task Force 50 During Operation ENDURING FREEDOM ARBRIDGED REPORT Version 1.0*. Report Prepared for the Office of Force Transformation in the Office of the Secretary of Defense. Transformation Case Study Series, 23 February 2007.

The Office of Force Transformation. N*etwork-Centric Operations Case Study - Task Force 50 During Operation ENDURING FREEDOM TECHNICAL REPORT Version 1.0*. Report Prepared for the Office of Force Transformation in the Office of the Secretary of Defense. Transformation Case Study Series. 27 February 2007.

Tisserand, John B. III. *Network Centric Warfare Case Study - U.S. V Corps and 3rd Infantry Division (mechanized) during operation Iraqi Freedom combat operations (mar-apr 2003) Volume iii: Network Centric Warfare insights*. Report Prepared for the Office of Force Transformation in the Office of the Secretary of Defense. Pennsylvania: U.S. Army war college, Carlisle barracks, August 2006.

United Kingdom. Ministry of Defence, *Network Enabled Capability, Joint Services Publication 777*, (London: MOD UK 2005).

U.S. Congressional Budget Office, "*The Army's Bandwidth Bottleneck*," Aug. 2003, http://www.cbo.gov, Internet; accessed 29 February 2008.

United States. Department of Defense, *Network Centric Warfare Department of Defense Report to Congress*, Report Prepared for the U.S. Congress (Washington: DoD U.S. 27 July 2001, http://www.dodccrp.org/files/ncw_report/report/ncw_cover.html; Internet; accessed 12 March 2008.

United States. Joint Chiefs of Staff. *Joint Operations*. JP 3-0. Vol. 3.0. Washington, D.C.: The Joint Chiefs of Staff, 2006.

United States. Joint Chiefs of Staff. *Joint Targeting*. JP 3-60. Vol. 3-60. Washington, DC: Joint Chiefs of Staff, 2007.

Vega, Milan, "*The NCW illusion*," *Armed Forces journal*, 1 January 2007.

Wathen, Alex. "Joint Airspace Management and Deconfliction: A Chance to Trade in a Stovepipe for Network-Centric Warfare." *Air & Space Power Journal* 20, no. 3 (Fall 2006): 26.

Weiner, Tim, "*Pentagon Envisioning Costly Internet for War*", New York Times, November 13, 2004. http://www.nytimes.com/2004/11/13/technology/13warnet.html; Internet; accessed 14 March 2008.

Wilson, Clay. *CRS Report RL32411 Network Centric Operations: Background And Oversight Issues For Congress.* Report Prepared for the U.S. Congress. March 15, 2007.

Wilson, Clay. *CRS Report RL32411 Network Centric Operations: Background And Oversight Issues For Congress.* Report Prepared for the U.S. Congress. June 2, 2004.

Wolfers, Arnold. "*National Security" as an Ambiguous Symbol*." Political Science Quarterly 67, no. 4 (Dec. 1952): 481-502.