Network Centric Warfare: A Survey

Gangadharaiah S
Department of Information Science & Engineering
Acharya Institute of Technology
Bangalore, India

Umashankar Hallur
Department of Information Science & Engineering
Acharya Institute of Technology
Bangalore, India

***Abstract*— In recent years the revolution in military has given a way to transform from traditional approach to network of network. This revolution leads to the formation of Network Centric Operation, which is a combined operation of technology and human being to accomplish a task by making reuse of available resources through upgrading to the new technology. The integrated communication reduces much of the manual tasks with fewer amounts of time, capital and human resource.**

Keywords-Network Centric Warfare, Military Transformation, Network Centric Operation, Military, Defence

I. INTRODUCTION

The Defense transformation has revolutionized from platform centric to network centric thinking. The transformation is being occurring in order to accelerate the tempo of movement of forces, maintains an unremitting operational tempo, and determinedly engages the enemy at the time & place of our choosing. The conversion doesn’t change the existing system but it creates new kind of command relationship with other fundamentals of war. It requires focused endeavor to work closely with allied coalition partners. The change to Network Centric Warfare increases the combat power by improved synchronization events and their consequences in the battle space. Many defense departments demonstrate the increased combat power associated with robust networking of sensors, shooters, command and control (C2) capabilities.

Network centric warfare is an emerging theory of war in information age. It describes the amalgamation of strategies, emerging campaign, methods and procedures. It is all about human and organizational behavior. It endow with new conceptual framework with which to examine the military missions, operations, and organizations. It focuses on the combat power that can be generated from linking/ networking of war fighting enterprise. It is illustrated by the ability to create a high level of shared awareness that can be utilized via self synchronization and network centric operation to achieve commanders’ aim. It supports speed of command, better-quality information position to action. Overall it is about an emerging military response to the information age [1].

Fig.1: The basic principle of the partition between sensor, C2 and engagement elements, connected by the communication of information, is ancient. In land battles of centuries ago, viewers on hilltops would pass on their interpretation on the state of the battle via couriers to the general in his tent. The gathered information was used to take the action; the general again pass on the message to the troops, again via couriers. The modern concept of NCW differs only in level of degree: now our goal is to integrate all entities operating in disparate environments (sea, land, air, space). These entities may be thousands of kilometers apart, and may travel at hundreds or thousands of kilometers per hour. The information conveyed across the communication is not only restricted to sentences, it includes data as live video feeds and imagery which is a real time data.

NCW need much time to get mature. However, some significant NCW-related goals have already been achieved. For example, during Operation Iraqi Freedom, the United States Air Force flew Global Hawk Uninhabited Aerial Vehicles over Iraq to collect imagery data using their sensors. This information was passed through satellite communications links to the continental United States for analysis. Information related to target was then passed back to US Air Force or Army elements in Iraq, who employed the targets. All of this took only a few minutes. In situations where the timeliness of information was critical, Global Hawk sensor information could be communicated directly to army elements that were closing with adversary forces. This allowed them to see what the Global Hawk had seen only seconds previously [2].

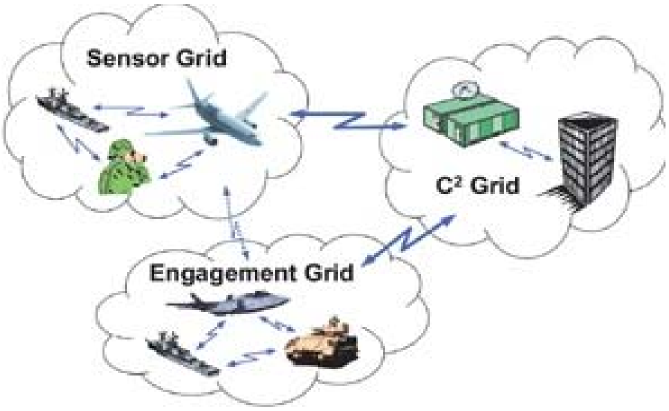

Figure 1. The Grids of Network Centric Warfare

II. INFORMATION AGE WARFARE

The principles of NCW provide a new foundation with which to examine & consider changes in military operations and organizations in the information age. Information technology advances in the areas of command and control (C2), intelligence, surveillance, and reconnaissance (ISR), precision arms delivery are reforming the conduct of warfare. The complete application of these principles will speed up the decision cycle with pace and quality, increases the speed of command pre-empting adversary options, creates new options and improves the effectiveness of selected options. This operation promises successful conclusion more rapidly at a lower cost.

We need to consider the impact of information age as it recounts to the job of command and control. Information age permits us to employ and consider force with greater accuracy and granularity. Identifying what needs to managed, noting that attention needs to be focused on the interactions among entities like sensors and actors, supporting infostructure, command and control, and perceptions. Shifting to thin architecture minimizes unit costs of sensors and actors and allows buying larger quantities [3].

A. Benefits of Network Centric Warfare

In some engagements, superior platforms were easily defeated by less fit platforms that were fit to influence request of magnitude upgrades in data exchanging enabled by systems administration or networking. In different engagements, digitized and organized ground forces with less number of platforms were able to replace information for mass and forces with more number of platforms not digitized and connected. Considerably more astonishingly, the mixture of networked and digitized ground and aviation based armed forces was equipped to defeat an opposition force with exceptional lethality by making and leveraging an information advantage.

Some benefits of NCW are listed as below.

- Improved information sharing with the help of networking.
- Digitized and networked ground forces with a reduced number of platforms.
- Increased situational awareness, enhanced survivability and lethality.
- Increased effectiveness in the war fighting with lower cost.
- Allows exchange of real time data.
- Reduced time between the sensors and shooters.
- A robustly networked force improves information sharing.

B. Challenges of Network Centric Warfare

Networking relates to gathering of the right data to the right forces who in turn can take the right action, quicker, against the right intent. It cut downs the kill chain which detects, decides, attack, assess and shrinks the amount of resources required to move through each link.

1) Bandwidth Limitations: Bandwidth is the transmission capacity for any given channel on a network. Since 1991, there has been an explosive increase in military demand for bandwidth, largely due to efforts to speed up the delivery of digital information [4]. Network centric operations will constantly require more and more communications bandwidth. This means that the service providers must make efforts to manage bandwidth more efficiently, with better communications technology, and with command and control systems that are better able to prioritize and manage signal flow [5].

The table I shows the increased usage of bandwidth in the military operation.

TABLE I. BANDWIDTH UTILIZATION IN DIFFERENT SCENARIOS

Serial	Conflict	Bandwidth usage
1.	Desert Stroam 1991	99 Mbps
2.	Kosovo 1990	250Mbps
3.	Enduring Freedom 2002	736 Mbps
4.	Iraqi Freedom 2003	3200 Mbps

.

2) Efficient Transfer of Infromation: Different levels of communication have different security levels in the network so it is very difficult to transfer data efficiently. However, a somewhat ironic difficulty can arise when commanders at different levels became inundated with information from different sensors and sources. Information may become intoxicating, turning tactical challenges into quantitative equations and distracting commanders from such basic military principles as initiative and decisiveness. Too much information may cause commanders to tune out [6]. Ultimately, the appropriate information not just data must be matched to the differing requirements of tactical commanders and theatre commanders .

3) Secure Communication: It is difficult to provide much efficient encryption method for mobile systems, the data which is to be decrypted in very less amount of time. Moreover computers, software and other processor and software centric war fighting equipment are susceptible to cyber attack. The risk level is high because increased dependence on network and easy availability of information would incapacitate friendly forces when these resources are not available.

For example, People’s Liberation Army (PLA) of china has developed more than 250 trojans like intelligent and vacuum trojans along with similar tools to attack PCs. Group of Chinese hacker with website known as EvilOctal attacked on the US firm in the early 2009. He created a PDF document which was used to carry malicious software with a tool that is only available in Chinese called FreePic2Pdf, v 1.26. [6, 7].

4) Satellite Communication: It is difficult Satellite communications plays an important role for transmitting message and imagery data. A growing dependence on space communications may also become a critical vulnerability for NCW. In future dedicated satellites may not meet the demand of military so are much chances for opting the commercial satellites for communication.

For example, The United States has six orbital constellations for early warning, for imagery, and for signal intelligence. Defense Information Systems Agency (DISA) reported that 84% of satellite communication bandwidth was provided by the commercial satellites [8].

5) Outsourcing and Technology Transfer: An increase in offshore outsourcing of high tech jobs, including computer programming and chip manufacturing may enable a transfer of knowledge and technology. The Greater Group research firm has reported that corporate spending for offshore information technology services has increased to $1.8 billion in 2003 and $26 billion in 2007, with work going to Asian countries. Outsourcing may increase the number of foreign nationals who are experts in newer Internet technologies and software applications.

Case in point, as unanticipated as 1998, Intel Corporation, Microsoft Corporation, and other IT sellers opened R&D offices in Beijing and different parts of Asia. Microsoft supposedly has 200 Ph.D. competitors and 170 scientists right now working in its Asia R&D offices. Engineering exchange likewise happens for the assembling of high-innovation supplies used to backing NCW operations. For instance, just 20 percent of the thermal batteries utilized as a part of U.S. rockets, guided cannons, and guided shells are handled by domesticated suppliers, while 80 percent of these gadgets are prepared by outside supplier. Night vision infrared apparatuses that have earlier given U.S. strengths an enormous military point of interest are presently fabricated with materials and segments that come just about completely from remote sources. [8].

III. NCW MILITARY OPERATION AND ITS AWARENESS

The battlespace entities are interconnected that will take the full advantage of available information, convert this information into knowledge, and produce increased combat power.

Battlespace entities have three prime functional forms: sensing, deciding, and acting. The level to which one functional form will take over at a particular point in time determines the function of an entity in a military operation. Entities that have a prime role of sensing are called sensors. Actors are those entities that have the primary role of generating the high value in combat power of battlespace. Actors occupy both traditional and non-traditional means. Decision makers execute a variety of functions. NCW is based upon sharing data to achieve the maximum effectiveness, with having a high level performance, communications, and computational capability allowing access to proper information sources, and permitting flawless interactions among battlespace entities in a plug and play fashion. This is called the infostructure.

For example in [9], Military Operations in Urban Terrain (MOUT) is the capacity to work and behavior military operations in constructed up zones and to attain military destinations with least casualties and collateral damage. In Fig.2: MOUT incorporates nonlethal weapons, exact weapons, reconnaissance, and circumstance awareness through effective communication in urban zones. MOUT is less a one of a kind proficiency but rather more an environment in which the operational ideas of Joint Vision 2010 - particularly accuracy precision, full-dimensional protection, and prevailing move will be tried under the most requesting conditions. In the close term, the emphasis will be on the exploitation and incorporation of existing innovations into frameworks offering enhanced competence for engagement, force protection, and maneuver in urban environment. The long haul emphasis which will structure the groundwork for a correct change of the conventional capacities of strike, security, and maneuver will be a command and control, and intelligent structure that will allow the war fighter, at any level, to utilize forces and mass impacts in revolutionary ways. In an expansive sense, MOUT is much the same as general warfare: our battle powers must have the ability to battle and survive superior to their foes. MOUT is exceptional since it is maybe the most complex and resource intensive environment in which they will battle.

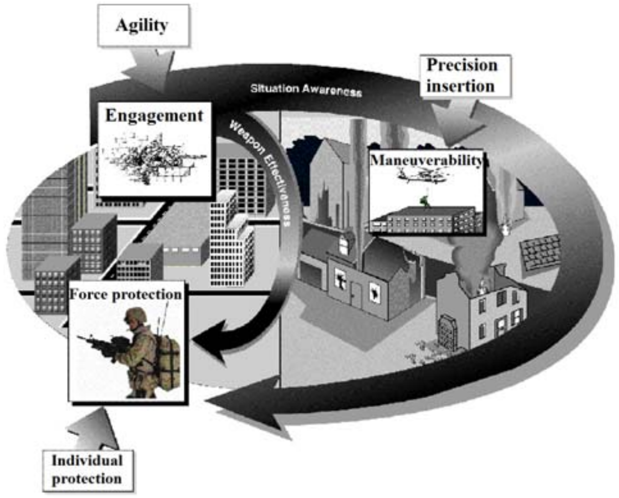

Figure 2. The Concept of Military

The issues like connectivity and division of responsibility are explored as the experimentation with NCW starts. A sensor network can be viewed as providing the information from which battlespace awareness is created. NCW focuses on the proper linking of sensor entities, and on the offerings they make to create shared battlespace awareness. Proper linking of sensor entities doesn't mean that sensors should be directly connected each other or they should be in the same sensor network. Shared battlespace awareness needs that information gathered by sensors be put in a universal form that makes it possible for other entities to combine proper data, put it in framework, and understand its impact. This will allow the exchange of data that is so important to initiate obtaining the power of NCW.

Sensor entities and actor entities are networked to many more entities but more closely to actors. Actor entities perform with both platform as well as network centric operations. Research is going on linking the entities to sensor entities directly which in turn increases the performance with more effectiveness.

A. Role of Battlespace Entities

Sensors, actors, and decision makers are organized and each entity is connected to each other. Fig.3: Sensors provide the data they gather either to data storage centres that support one or more common operational pictures (COPs), as well as directly to preferred actors. Decision entities can perform a small number of sensors; view COPs, and direct C2 actors. Actors get required information from sensors, local databases or from COPs which are continuously updated. Actors can also add information to data centres and communicate with other actors, passing information or commands to and fro [10].

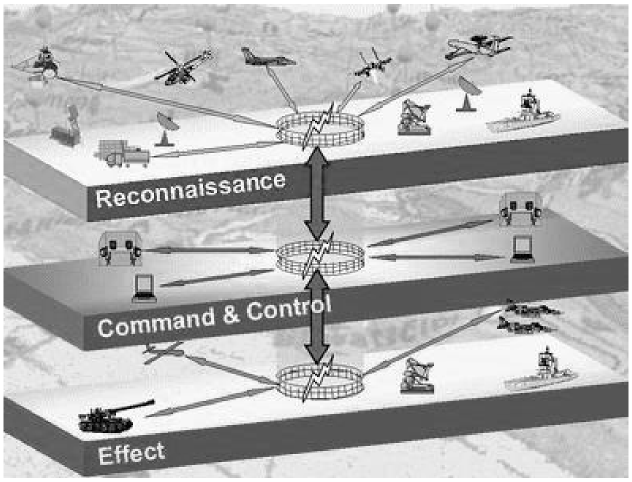

Figure 3. The Entities of Network Centric Warfare

B. Sensor Network

The battlespace awareness which is generated by the performance of sensor network depends upon following factors which includes:

- The performance of component sensors.
- Sensor geometry: the locations of the sensors with respect to each other and the objects of interest.
- The velocity of information.
- Fusion capabilities.
- Tasking capabilities.

Sensor network emerges as a key for increased combat power in the shift to network centric operations. Stand alone sensors can generate more precise and timely information. The performance advantage that emerges from the enabling of sensor networks is a function of the active or passive sensors being employed and the class of objects of interest like missiles, aircraft, tanks, submarines, etc.

Sensor networks can generate considerably improved battlespace awareness and provide advantages over stand alone sensors in key mission spaces by overcoming the fundamental performance limitations like coverage, accuracy, and target identification properties. The data fusion process and sensor tasking can partly overcome these limitations. This implies that almost all operation areas can benefit to some extent from the shift to network centric operations [10].

IV. NCW CASE STUDIES

The main goal of NCW conceptual framework is to enhance the understanding of NCW by gathering and analysing the evidence on associated technologies and practices. Some case studies illustrate the progress till date

A. Ground Operations (Stryker Bridge Comabt Team)

NCW capabilities were effectively demonstrated by the Stryker Brigade mission capability package (MCP). The Brigade's new organizational structure, battle command and linking capabilities, and budding operational concepts improved the quality of information available to soldiers all through the unit. In turn, enhanced information quality resulted in superior interactions and collaboration, which led to enhanced shared awareness and understanding. Ultimately, the Brigade's NCW capabilities provided commanders with better decision options and enabled better control of the speed of command. Collectively, all of these information based attributes made the Stryker Brigade's decision-making ability more agile.

The Stkryker Bridge combat team is consisting of total 3,900 to 4000 soldiers with three Stryker infantry battalion, reconnaissance, surveillance and target acquisition squadron, fires battalion, brigade support battalion, and individual companies. These qualities, along with improved organizational, equipment, and training capabilities, increased combat effectiveness [11].

B. Air-to-Ground Operations

The air-to-ground operations case study examined close air support (CAS) in Operation Iraqi Freedom (OIF) and determined that NCO technologies and practices provided U.S. forces in Iraq with the ability to reconcile air and ground perspectives and successfully attack ground targets in a limited number of engagements. Most CAS missions conducted during OIF depended primarily on legacy systems at the aviator-ground manoeuvre element level. Both Army and Marine ground units usually called for CAS and guided CAS aircraft to the target using voice communications.

NCO systems were used extensively between air and ground components at the operational level and within component chains at all levels. Multiple network centric systems supported networking between staffs. F-14s from VF-2, VF-31, VF-32, VF-154, and VF-213 partook in Operation Iraqi Freedom. The F-14s flew 2,547 battle fights and dropped 1,452 GBU, JDAM, and MK-82 shells with only one lost plane (from motor disappointment). F-14s headed strikes on Baghdad, striking targets, for example, the Iraqi Ministry of Information's Salman Pak radio transfer transmitter office at Al Hurriyah (southwest of focal Baghdad) with JDAM shells [12, 13].

V. CHALLENGES IN IMPLEMENTING NCW

Transformation, including the execution of NCW potential to allow the joint force and the constant shift from platform centric to network centric thinking, is a continuing process with no apparent end point. Those involved in transformation and NCW implementation in the Department of Defense (DoD) must anticipate the future and wherever possible help create it.

Transformation and NCW implementation deal with the co-evolution of the seven key functional areas of doctrine, organization, training, materiel (technology), leadership and education, personnel, and facilities (DOTMLPF). Consequently, development in implementing network centric warfare cannot be measured only by focusing on one dimension, such as technology or doctrine. Rather, progress must be assessed in terms of the maturity of mission capabilities that integrate key elements of DOTMLPF.

Fig.4: The network centric enterprise relay on the basic elements necessary to produce combat power. As in the commercial sector, it all initiates with infrastructure. This in turn enables the formation of shared battlespace awareness and knowledge. This awareness and knowledge is influenced by new adaptive command and control approaches and self synchronizing forces. The bottom line is increased tempo of operations, responsiveness with lower cost and risk and increased combat effectiveness.

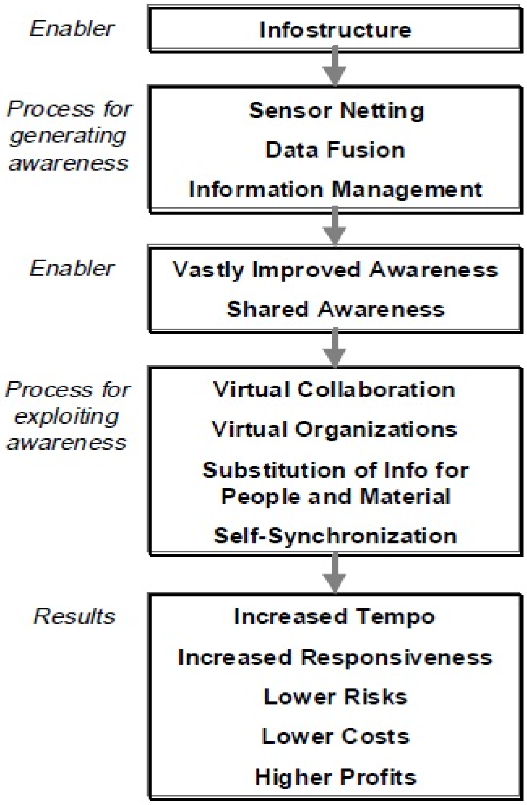

Figure 4. The Military as a Network Centric Enterprise

VI. NCW CAPABLE COUNTRIES

Military organizations are generating responses to the challenges of information age warfare. Some countries, such as Sweden which uses the term Network Based Defense, may view NCW concepts and the promise of more efficiency and effectiveness through networking with coalition partners, as a way to reduce military budgets. Denmark, Norway and the Netherlands have all adopted the term Network Centric Warfare; Australia uses the term Network-Enabled Warfare; the U.K. uses the term Network-Enabled Capability; and, the armed forces of the Republic of Singapore uses the term Knowledge-Based Command and Control. Observers have reported that units of the Chinese military have been using computer systems for online tactical simulation exercises. The simulation involved networking and multimedia presentations to train commanders and troops in an on-line classroom, where battles are fought using an electronic sand table, and results are judged for scoring. Officers and troops could also exchange messages and share information via the network. The NCW capabilities under development by other countries include technologies similar to what is described for joint U.S. forces in this report.

NATO is currently building a capability for dynamic interoperability with U.S. forces in the future and is developing a framework for high-technology warfare using the combined forces of multiple nations, called NATO Network Enabled Capabilities, similar to the U.S. military's Joint Vision 2020. Other NATO initiatives for coalition operations include the Multinational Interoperability Program, the Cross System Information Sharing Program, and the Multi-functional Air-based Ground Sensor Fusion Program. [13]

REFERENCES

[1] A. K. Cebrowski, Director, Office of Force Transformation, The Implementation of Network-Centric Warfare

[2] Wing Commander Peter R McLennan, and Wing Commander Peter A White, GradDipAdmin, ADF Health April 2005 – Volume 6 Number 1

[3] David S. Alberts, John J. Garstka and Frederick P. Stein Network Centric Warfare Developing and Leveraging Information Superiority, II edition (Revised)

[4] Mr. John Luddy, Adjunct Fellow, The Challenge and Promise of Network-Centric Warfare, February 2005.

[5] Wg Cdr Arif Salam Qazi (Pakistan Air Force), Network Centric Warfare: A new Dimension for Pakistan Defense Forces

[6] Colonel Deepak Sharma, Institute for Defense Studies and Analysis, New Delhi, Integrated Network Electronic Warfare: China's New Concept of Information Warfare

[7] Vinod Anand, Chinese Concepts and Capabilities of Information Warfare, Volume: 30, Issue: 4, October 2006

[8] Clay Wilson, CRS Report for Congress, Network Centric Operations: Background and Oversight Issues for Congress, June 2, 2004

[9] Joint War fighter S&T Plan, Chapter IV – Achieving Joint War fighting Capability Objectives

[10] http://militaryanalysis.blogspot.in/2012/05/ncw.html

[11] https://sites.google.com/site/usarmyforcecomposition/home/stryker-brigade-combat-team

[12] Andrew F. Krepinevich, Operation Iraqi Freedom: A first-Blush Assessment, Center for Strategic and Budgetary Assessments, 2003

[13] Reiner K. Huber, Beyond Defense Reform: Challenges for Transforming the European Pillar, September 2006

AUTHORS PROFILE

Gangadharaiah S. received the B.E. and M.Tech. Degree in Computer Science & Engineering from Visvesvaraya Technological University, Karnataka in 2003 and 2011, respectively. He is an Assistant professor in the Department of Information Science & Engineering, Acharya Institute of Technology, Bangalore. His research interests include wireless sensor network, Embedded Systems.

Umashankar Hallur, pursuing Master of Technology in Computer Network and Engineering, Department of Information Science and Engineering, Acharya Institute of Technology, Bangalore, Karnataka, India. His areas of interest are Networking and Wireless Sensor Networks.