

NETWORK-CENTRIC WARFARE: SOME FUNDAMENTALS

PREM CHAND

INTRODUCTION

The emergence of microelectronics has led to the design of high performance military systems. The performance edge in terms of faster and accurate response emanates from embedded intelligence, which has proliferated into almost every facet of systems. Therefore, technologically advanced nations have produced platforms, weapon systems, delivery systems, and command and control infrastructure which can provide them overwhelming superiority almost instantaneously in terms of detection of targets, location and targeting in any part of the globe, under water, on surface or in space.

This potential of information technology (IT) to turn into a war-winning effort has led to some very innovative and revolutionary models of simultaneous and concurrent engagements resulting in quicker, easy, cost effective victories with comparatively less loss of human life on both ends. The detection of enemy presence, processing of targets, command decision-making and engagements have become possible through creation of collaborative networking amongst sensors, command and control elements and weapons. This new paradigm shift in operational concepts has come to be recognised as network-centric warfare (NCW). There are other new terms like “cyber warfare”, “information warfare” and “net war” which are being used interchangeably in literature and being more precisely mapped as

Dr. **Prem Chand**, former Commodore in the Indian Navy and Additional Director General in the Ministry of Defence, Government of India, is Vice President, Mahindra British Telecom Ltd. He is also Chairman, World Telemangement Forum's Security Committee for Next Generation Operations Support Systems (NGOSS) Programme.

information based operations (IBO) resulting in the revolution in military affairs (RMA).

NCW is a new warfare paradigm which affects civil and military IT infrastructures alike and, thus, has serious implications on the social,

In order to build a credible engagement capability in the information age, India would need to transform the conventional IT supported operational capability of its armed forces into an NCW capability.

economic, political and military landscape of a country. The impact of NCW on the overall warfare perceptions and perspectives, the need to change doctrines at tactical and strategic levels, alterations in organisational structure, force level, training, etc.,

have become a stark reality facing every country, including India.

The paper presents an overview of NCW and its basic building blocks. The paper signifies that the conventional approach for warfare, even with the induction of IT, will not meet the future national security needs of India. It, therefore, emphasises that in order to build a credible engagement capability in the information age, India would need to transform the conventional IT supported operational capability of its armed forces into an NCW capability. It presents the key transformation objectives and emphasises that NCW is about networking, and developing doctrines, and that the information grid is a vehicle for NCW. The paper highlights that IT infrastructure is germane to the NCW functionality and describes how this capability can be built by India. It brings out that there are increasing instances of the private sector following the network-centric approach to meet its business objectives and recommends that the armed forces should leverage them. It presents two case studies from Oracle and IBM, giving details of their large scale participation in NCW initiatives of the US Department of Defence (DoD). The paper presents an overview of the strategy and road-map being attempted by the US DoD in its NCW initiatives and recommends that India should examine and address its NCW needs on similar lines.¹

1. Andreas Tolk, PhD: "A Common Framework for Military M&S and C⁴I Systems, 2003," Dominion University.

NETWORK-CENTRIC WARFARE

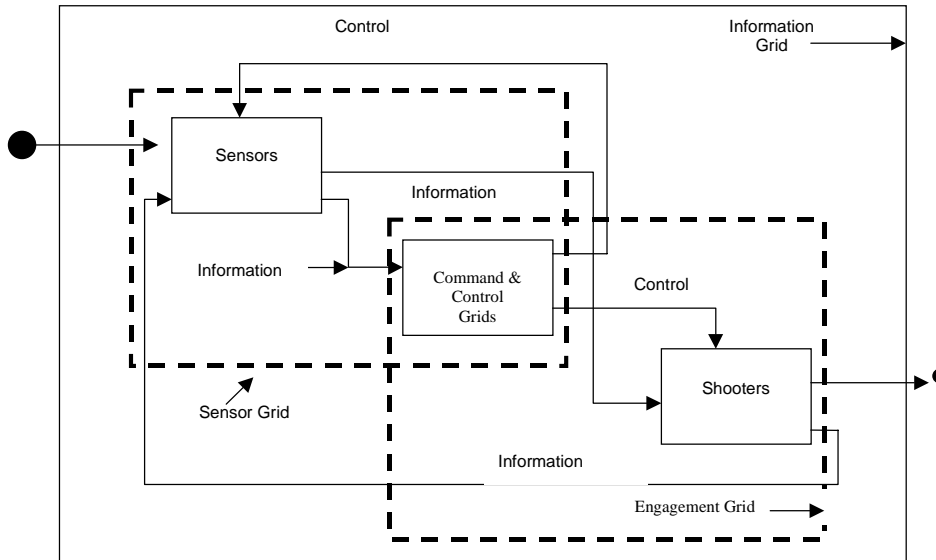
Armed forces need to fulfill their tasks with decreased resources and decreased manpower. This necessitates working smarter and looking for force multipliers. Network-centric warfare enables us to manage this paradox. Emergence of new technologies has created the conditions for network-centric computing. There is an explosive growth of the Internet, intranets, extranets, transmission control protocol/Internet protocol (TCP/IP), hypertext transfer protocol (HTTP), hypertext markup language (HTML), Web browsers, search engines, and Java Computing. These technologies, combined with high-volume, high-speed data access and technologies for high-speed data networking have led to the emergence of network-centric computing. Information “content” now can be created, distributed, and easily exploited across the extremely heterogeneous global environment. Networking, for example, in stock markets has led to a shift from a trader-centric system to a network-centric system. This has considerably reduced the time taken to complete transactions and increased customer awareness about prices of stocks and shares. This is very similar to a soldier having real-time battlefield awareness, which will enable him to complete his task quickly and efficiently. Network-centric retailing in departmental stores enables better inventory management. Similarly, a shift to network-centric operations will help the military improve its logistics management. It can be concluded that the military stands to benefit from network-centric operations in the same way as the corporate sector does.^{2,3}

The structure or logical model for network-centric warfare is shown in Fig. 1. It consists of a high-performance information grid that provides a backplane for computing and communications. The information grid enables the operational architectures of sensor grids and engagement grids. Sensor grids rapidly generate high levels of battlespace awareness and synchronise awareness with military operations. Engagement grids exploit this awareness and translate it into increased combat power. New classes of threats have

2. VADM Arthur Cebrowski and John Garstka, “Network-Centric Warfare, its Origin and Future,” US Naval Proceedings, January 1998.

3. John J. Garstka, *Defence Transformation and Network-Centric Warfare*.

Fig. 1: Logical Model of Network-Centric Warfare



Source: VADM Arthur K. Cebrowski and John Garstka, "Network-Centric Warfare, its Origin and Future," US Naval Proceedings, January 1998, p. 33.

required increased defensive combat power for joint forces. The combat power that has emerged—the cooperative engagement capability (CEC)—was enabled by a shift to network-centric operations. The CEC combines a high-performance sensor grid with a high-performance engagement grid. The sensor grid rapidly generates engagement quality awareness, and the engagement grid translates this awareness into increased combat power. This power is manifested by high-probability engagements against threats capable of defeating a platform-centric defence. The CEC sensor grid fuses data from multiple sensors to develop a composite track with engagement quality, creating a level of battlespace awareness that surpasses whatever can be created with stand alone sensors. The whole is clearly greater than the parts.

The pace of the future battle will be so swift that there will be no time to revert to the rear headquarters all the time for instructions and advice. A typical military hierarchical structure in such an environment will fail. It

would be necessary to decentralise and delegate, while the people on the battlefield will have to be fully aware of rules of engagement and the political factors so that they can take quick decisions. Network-centric warfare enables a shift from attrition style warfare to a much faster and more effective warfighting style characterised by the new concepts of speed of command and self-synchronisation. Strategically, it allows an understanding of all elements of battlespace and battletime; operationally it provides a close linkage between the units and the operating environment; and tactically it provides speed.

The pace of the future battle will be so swift that there will be no time to revert to the rear headquarters all the time for instructions and advice.

FUNDAMENTALS OF NETWORK-CENTRIC WARFARE

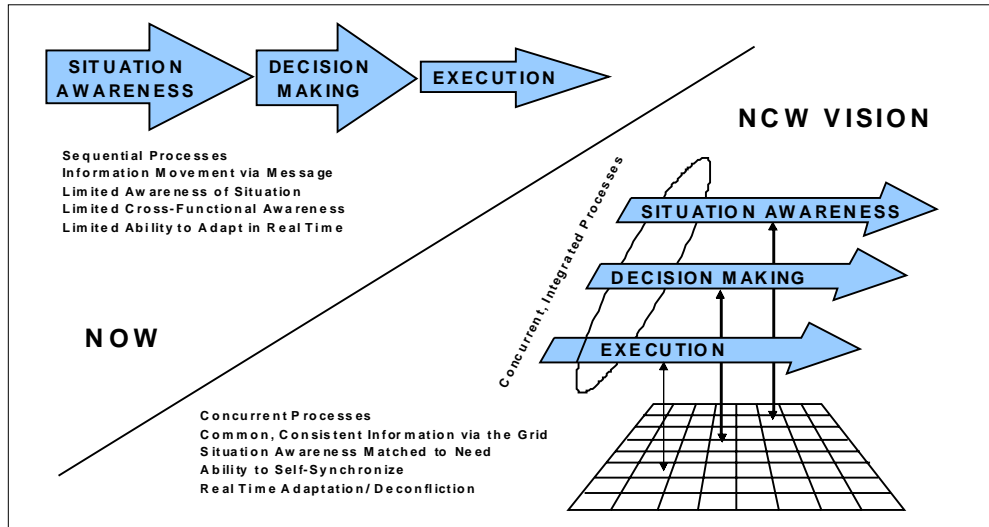
There are numerous definitions of NCW available in the literature. The US Navy defines NCW as “military operations that exploit information and networking technology to integrate widely dispersed human decision-makers, situational and targeting sensors, and forces and weapons to highly adaptive, comprehensive systems to achieve unprecedented mission effectiveness.” The literature is very supportive of the following operational benefits of NCW operations

- (a) Increased speed of command by ensuring operations within the observe, orient, decide, act (OODA) loop and achieving high sustained operational tempo.
- (b) Ability to take individual initiative within a forcewide decision context. This provides flexibility and adaptability to operational situations.
- (c) Decision superiority through effective use of all the available information and use of force assets and capabilities.

The operational processes and their effectiveness in the conventional and NCW paradigm are presented in Fig. 2.⁴

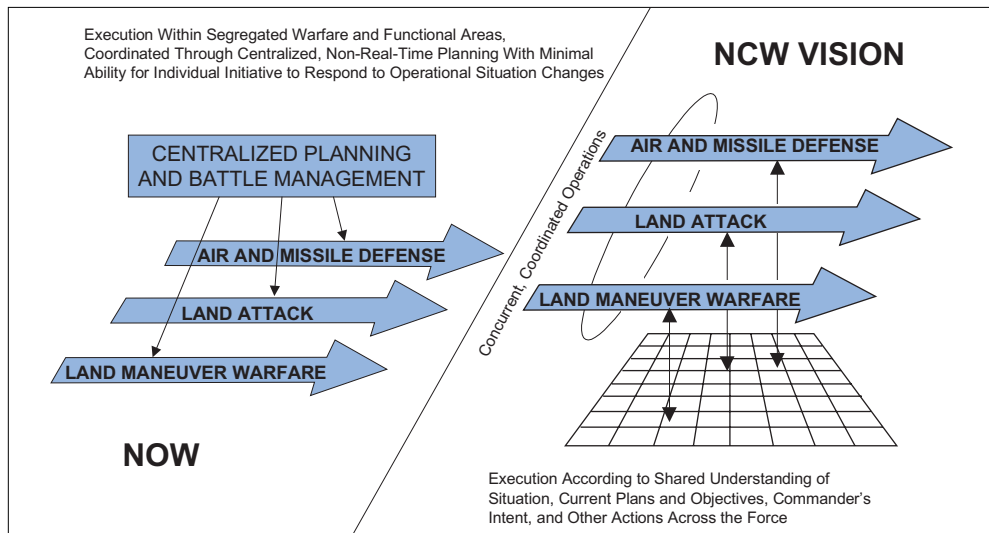
4. Dr. Howard S. Marsh, “Information Technology, S&T to Enable Network-Centric Operations,” April 1, Marshh@ONR.navy.mil.

Fig. 2: Operational Processes and Effectiveness



Source: Marshh@ONR.navy.mil

Fig. 3: Impact All Missions and Functions



Source: Marshh@ONR.navy.mil

The functional structure in the conventional warfare paradigms and the new vision of NCW are presented in Fig 3.

NCW: THE TRANSFORMATION FOR THE DIGITAL AGE

Considering the current operational structure of the armed forces and its underpinning information and communication technology (ICT) infrastructure, the transformation for the digital age is inescapable and inevitable. The initiatives for transformation would involve understanding the objectives and needs of digital age armed forces, the strategy, approach and clearly identified roadmaps as presented in the succeeding paragraphs.

Transformation Objectives

The literature survey reveals that the USA, NATO (North Atlantic Treaty Organisation), China, etc. have identified the following objectives for transformation into the digital age. We need to map our thought process to these objectives and come up with our own wish list.

- (a) Link force transformation to key elements of military strategy and integrate transformation with policy, strategy, joint operations and tactics.
- (b) Develop innovative concepts to leverage India's advantages in terms of speed of technology, manpower, operational and tactical culture. Work at the intersection of unarticulated needs and non-consensual change.
- (c) Create elements of transformation which do not exist. Catalyse activities to expand breadth of capabilities. Fund and support prototyping. Promote industry participation.
- (d) Identify and develop new paths and linkages to implementation. Act outside the normal course.
- (e) Provide unbiased feedback to the senior leadership

The digital age armed forces constitute a paradigm shift when compared with the industrial age military structures and capabilities.

Digital Age Armed Forces: Needs

The digital age armed forces constitute a paradigm shift when compared with the industrial age military structures and capabilities. The digital age

needs are viewed in the context of new strategy, threat spectrum and ICT as follows:

- (a) New strategic context:
 - New theory of war based on information age principles and phenomena.
 - New relationship between operations on borders and internal security.
 - New concepts/ sense of security in the citizen.
- (b) Larger threat context in the information age:
 - State/non-state.
 - Nodal/non-nodal.
 - Symmetric/asymmetric.
 - Traditional/unrestricted.
- (c) New technological opportunities:
 - Immediate accessibility to highly capable low cost IT.
 - Opens key operational domains to industry and institutional collaboration.

Strategy for Transformation

The following strategic issues would need to be examined in the context of digital age capability building.

- (a) Transform the armed forces from the industrial age to the information age. Think through collaboration.
 - Move from platform-centricity to networks.
 - Imbibe automation.
- (b) Aim for sustained digital superiority.
- (c) Broaden the capabilities base.
- (d) Leverage IT advantages and opportunities.

APPROACH FOR DEVELOPMENT OF NCW CAPABILITY

The Indian armed forces have been engaged in a number of development and procurement initiatives to embed IT into sensors, command and control elements and weapon systems, in one form or the other. The engagement

process and operational work flow still follow the conventional serial approach of 'detect', 'process', 'decide', 'engage', and 'monitor' for feedback. A paradigm shift is needed to develop NCW capability whereby all components need to be examined from the network-centricity perspective.

This would require work flow as well as the engagement processes to be altered to suit end to end network-centric operations. To make this paradigm shift possible it would also be prudent to examine some of the fundamental issues of digital age armed forces and the role of various agencies to make a meaningful beginning. These are presented as follows:

A paradigm shift is needed to develop NCW capability whereby all components need to be examined from the network-centricity perspective. This would require work flow as well as the engagement processes to be altered to suit end to end network-centric operations.

- (a) Understanding of information age needs of national security.
- (b) Role of armed forces in digital age national defence
- (c) Basics of readiness status for the digital age. The fundamental amongst them is the transformation and transition of the armed forces from a paper-based work environment to a paperless work environment. This is prerequisite without which no network-centric military operations are feasible.
- (d) Understanding of the network-centric military operational paradigms. There is a need to move beyond slide pack knowhow, whereby the digital age operational paradigms are well understood, and mapped to India's context across civil and military establishments in a documented form.
- (e) Creation and operational availability of some of the basic building blocks of NCW in the form of defence information infrastructure (DII) viz. networking components, satellites, segment application software, etc.
- (f) A well documented, debated and agreed strategy, blueprint and road-map for transformation to digital age armed forces.

OPERATIONAL ISSUES OF DIGITAL AGE ARMED FORCES

The operational issues expected to be faced by the digital age armed forces are extremely complex. A list drawn from a survey of the literature indicates that we can make a beginning by concentrating on the following:

- (a) Transform armed forces from the industrial age to the information age by the following:
 - (i) Embed IT across all operational and support functions.
 - (ii) Think through collaboration
 - (iii) Move from platform-centricity to networks.
 - (iv) Imbibe automation across all functions.
- (b) Aim for sustained digital superiority.
- (c) Broaden the capability base.
- (d) Leverage IT advantages and opportunities.
 - (i) Revisit work flow and processes.
 - (ii) Create and anticipate the future in the information age.
 - (iii) Promote co-evaluation of concepts, processes, organisations and technology.
 - (iv) Make fundamental shift in underlying principles.

INFRASTRUCTURE NEEDS OF NCW

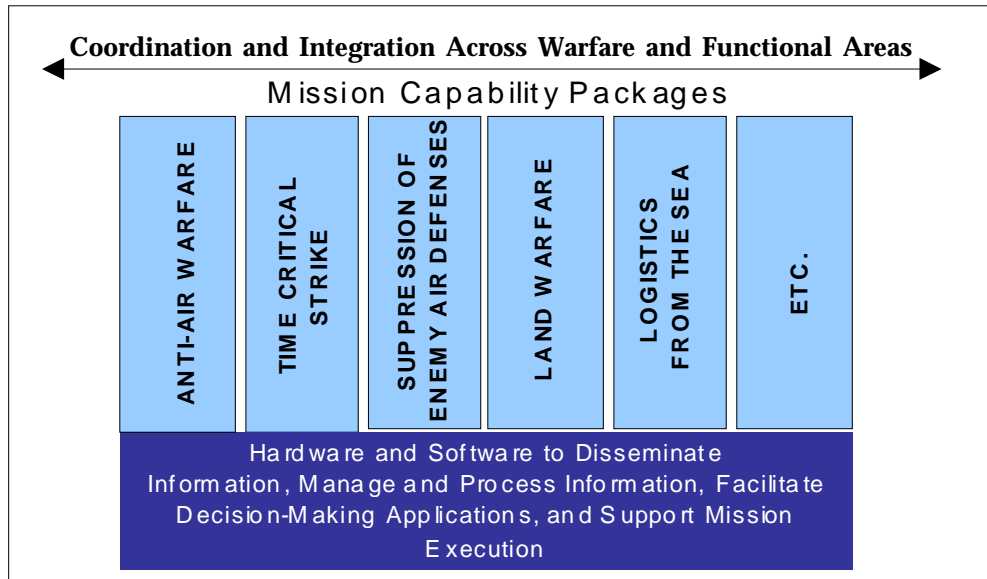
IT infrastructure is the foundation for building NCW capability. An overview of the hardware and software infrastructure as the basic building blocks and the mission capability application packages for coordination and integration across warfare functional areas are presented in Fig. 4.⁵

The availability of robust IT infrastructure is the core of the network-centric operations. Some of the basic IT building blocks are as follows:

- (a) Universal and robust connectivity.
- (b) Mission responsive resource control.
- (c) User focussed information dissemination.
- (d) Assured information integrity.
- (e) Effective information presentation.

5. Oracle White Paper, "Network-Centric Warfare Architecture."

Fig. 4: Infrastructure is the Foundation for NCW



Source: Marshh@ONR.navy.mil

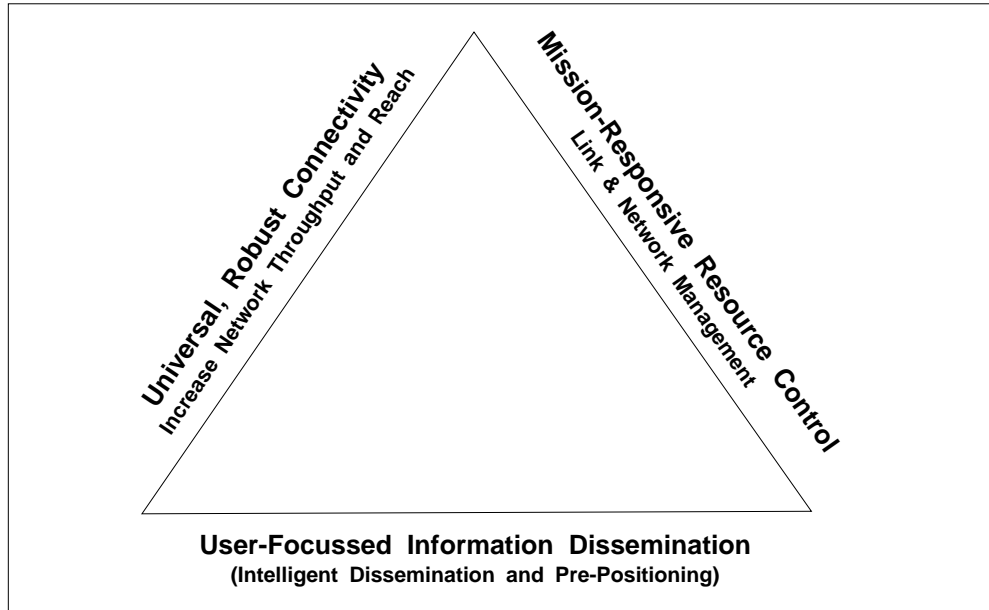
- (f) Effective distributed collaboration.
- (g) Empowered dismounted users.

An overview of each of these prerequisites for NCW is presented in the succeeding paragraphs. The focus of NCW is information service delivery as shown in Fig. 5.

Universal and Robust Connectivity

In operational terms, the IT infrastructure should provide an assured, user-transparent connectivity, rapid adaptation of networks to contend with real world status, routing and addressing to accommodate mobile users and an assured connectivity from the highest to the lowest echelons of the Services. However, in the existing infrastructure, we lack basic computerisation and networking. In cases where it exists, the nodes on different networks have difficulty in communicating, the network memberships are pre-assigned and programmed, and the connectivity, where

Fig. 5: NCW Focus: Information Service Delivery



Source: Marshh@ONR.navy.mil

it exists, is stove-piped and pre-allocated in functional networks. There are too many radios and antennas squeezed into a platform. What we need is to implement dynamic mobile networks as we see them in the civil sectors of the economy, combine capacity of shared networks and provide multi-channel radio capabilities.

To achieve state-of-the-practice universal and robust connectivity, there would be a need to implement dynamic network configurations. This would necessitate establishment or adaptation of protocols and standards for dynamic backbones spanning the three Services, and adaptation of emerging mobile IP protocols after they are hardened for military use. As these networking concepts are developed, there would also be a need to combine the capacities of shared networks which, in turn, will require development, adaptation and customisation of protocols to accommodate legacy systems and transition from gatewayed stove-pipe to universal connectivity. Besides, it would also be necessary to augment and provide simultaneous multi-

channel radio links which would, in turn, require development of multi-frequency components and strategies for tuning and beam pointing.

Mission Responsive Resources Control

In a real-time engagement scenario, the information infrastructure should have capability to respond to the warfighter's need for information services, tactical control of information assets and status of information assets. In our context, since the basic IT infrastructure is still not in place, there is a limitation on the quality of service, capability is wasted to assure availability, the resource control and coordination is limited to the local level, and reallocation is not feasible. What we require is the current status of assets, their dynamic allocation when needed and measures to prevent degradation or compromise.

In a real-time engagement scenario, the information infrastructure should have capability to respond to the warfighter's need for information services, tactical control of information assets and status of information assets.

In order to build this capability, we would need to create monitoring systems in terms of operational needs – using COTS, develop software to meet QoS objectives and develop systems for status display. In order to allocate resources dynamically, we will need agents to monitor for status and give advice on network status, co-relate mission to QoS objectives, techniques for resources allocation and automated C⁴I.

The system degeneration and compromise would have to be checked by predictive control of grids, integrated grid monitoring and use of tools for reactive defence and restoration.

User Focussed Information Dissemination

For meaningful and assured mission success, we need to provide the right information to the users at the right time, avoid information overload and avoid unnecessary burden on the radio communication. In today's

context, critical information is not available when needed, decision-makers face information overload, dependence on control information nodes and limited bandwidth. What we require is the ability to manage large information and data, distribute and update it and meet the information needs of

We would require security measures to support encryption at all data rates, trusted and fast guard filters, detection and monitoring capabilities and uncertainties, assessment of information quality, credibility and confidence level.

individual end users.

The data and information management will require use of computers to understand the operational situation, provide context-based information delivery and use of indexing and short messages for updates. The data distribution and updates will

require positioning of information on the basis of inferred needs. From a user perspective, we need to provide context-based search and retrieval, deployment of speech and text understanding technologies and use of alerts and alarm systems.

Assured Information Integrity

The information infrastructure in a NCW context is the basic vehicle of warfighting. Therefore, confidence about reliability and availability of information assets, their trustworthiness, quality and currency are critical. In an operational scenario, many a time, the complexity of security solutions compels users to bypass security mechanisms, weakness at the node level can corrupt data, the applications have inherent design weakness from the security perspective and measures are not in place to check audit ability, accuracy and concurrency. What we require are the transparent security measures, end to end network assurance up to application layer, realistic assessment of information trustworthiness and quality.

In order to build this capability, we would require security measures to support encryption at all data rates, trusted and fast guard filters, detection and monitoring capabilities and uncertainties, assessment of information quality, credibility and confidence level.

Effective Information Presentation

For effective engagements, we require information to be presented to suit end user needs. It should also be possible to provide information and knowledge integration and facilitate I/O customisation. In current systems, we have non-intuitive presentations which inhibit operator understanding and the information integration is left to end users. The uncertainties in the derived results are not presented. What we require is the reflection of the user's decision-making process, easy interaction, initiative and explanatory presentation skills, correlation of multi-events and representation of uncertainties and high confidence levels.

In order to develop this capability, we would need to automate the linkage and use all relevant information, provide machine reorganisation of patterns and trends, empower users to customise views and display formats, introduce natural language packages, provide explanation and circumstances that can be correlated using agents to discover relations, data fusion, advanced computing, traditional display and decision aids.

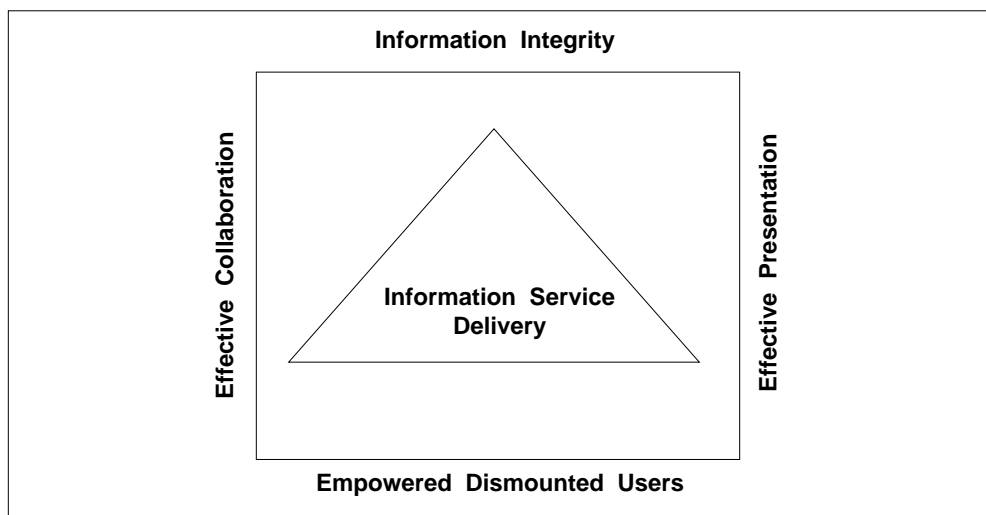
Empowered Dismounted Users

In the existing systems, the dismantled users are the least connected. What we require are the information services configured to dismantled foot soldiers, information appliances and devices embedded in weapons and clothing, hardware and software for small, unattended and mobile devices. Our existing systems are heavy, and consume high power. Their interfaces and presentations are not suitable for uncounted users. There is a need to improve size, power and weight, and develop interfaces, presentation formats, etc.

Ability to Support NCW Operations

Success in NCW operations is directly linked to the information service delivery. The ability to support NCW operations across the three Services would hinge around effective collaboration, information integrity, effective presentation and empowered dismantled users, as illustrated in Fig. 6.

Fig. 6: Assured Ability to Support Operations



Source: Marshh@ONR.navy.mil

These are further examined in the succeeding paragraphs.

Effective Collaboration

From an operational perspective, we should have the ability to achieve collaboration across any set of users, probably through software as agents of the users. This can be achieved by use of COTS products in tactical networks. The collaboration should be possible across the heterogeneous environments. The limitation of current COTS is that they need to be customised. The present level of distributed collaboration is ineffective and we are not geared for self-synchronisation in terms of basic technology blocks. What we require is to share critical information, solve tactical and strategic problems effectively, create interoperability amongst the collaboration tools of different types and maintain collaboration over networks.

Assured Information Integrity

In an NCW environment, the information should be available when needed, information should be trustworthy, current and of high quality. In

the existing system, security solutions are complex to use and generally bypassed by the users. One weak node can corrupt the entire network, applications are not designed secure from ground up, and the accuracy, currency and quality of information are not guaranteed. What we need are the transparent security measures to support NCW operations, end to end networkwide assurance up to application layer and assessment of intimation trustworthiness and quality.

The trust in the information systems can only be built through assessment of quality, tracking of uncertainties and following a rigid quality regime.

The transparent security measures need to be built using common encryption methods for all data rates and using trusted and rapid guards and filters. Network assurance would have to be achieved through intrusion monitoring, incidence handling and virus control. The trust in the information systems can only be built through assessment of quality, tracking of uncertainties and following a rigid quality regime.

Effective Information Presentation

It would be crucial to tailor information to suit specific needs in appropriate formats and requisite amplification with drilled down menus. In the existing systems, the presentations are dry, non-intuitive, unintegrated and do not highlight uncertainties as assessed by the decision support systems. What we require is the reflection of user decision processes, meaningful man-machine interaction, correlation of multiple events and a fair idea of uncertainties and confidence level presented to all sections of users.

The user decision processes can be reflected by using high end tools viz. machine recognition, more rigorous processing, and empowering users to customise views, use of natural language tools, explanation for machine recommendations and use of software agents to correlate reports .The

uncertainties and confidence presentation can be enhanced by using high end computing.

Empowered Dismounted Users

The foot soldier is the key to conclude operations. Therefore, information services need to be configured for infantry, devices embedded in weapons or clothing and miniaturised. Today, infantry is not connected to the network, systems are bulky, power intensive and unsuitable for mobile users. Thus, minimisation of size, weight, small power budgets is critical. The devices need to plug into networks.

PROCESS FOR BUILDING NETWORK-CENTRIC CAPABILITY

Our armed forces need to co-evolve concepts of operation, tactics, techniques and procedures, develop new materials and technologies and review the existing organisational structures. Each Service needs to identify IT capabilities required for NCW operations, assess current operational limitations vis-à-vis what systems are available, and assess and forecast technology needs of the NCW operations. The Services along with the Defence Research and Development Organisation (DRDO), and industry, should also plan and institute RD&D in this area. A similar approach followed by the US DoD to develop NCW capability through industry collaboration is illustrated by two case studies of NCW initiatives at Oracle and Boeing, in the succeeding paragraphs.

CASE STUDY: NCW ARCHITECTURE BY ORACLE CORPORATION, USA

Oracle Corporation, known for its enterprise applications and data base solutions, has been working with the DoD to develop NCW architecture. A brief overview of the NCW solution described in the company's White Paper is presented in the succeeding paragraphs. The key features of the globally aware battlefield pictures highlighted in the White Paper are:

(a) Common operational picture.

- (b) Connecting amongst all sensors, platforms and operators.
- (c) Self-synchronisation amongst underwater, land and air elements.
- (d) Enhanced ability of individual combat units and reduction in the fog of the war.

The architecture addresses the following basic issues:

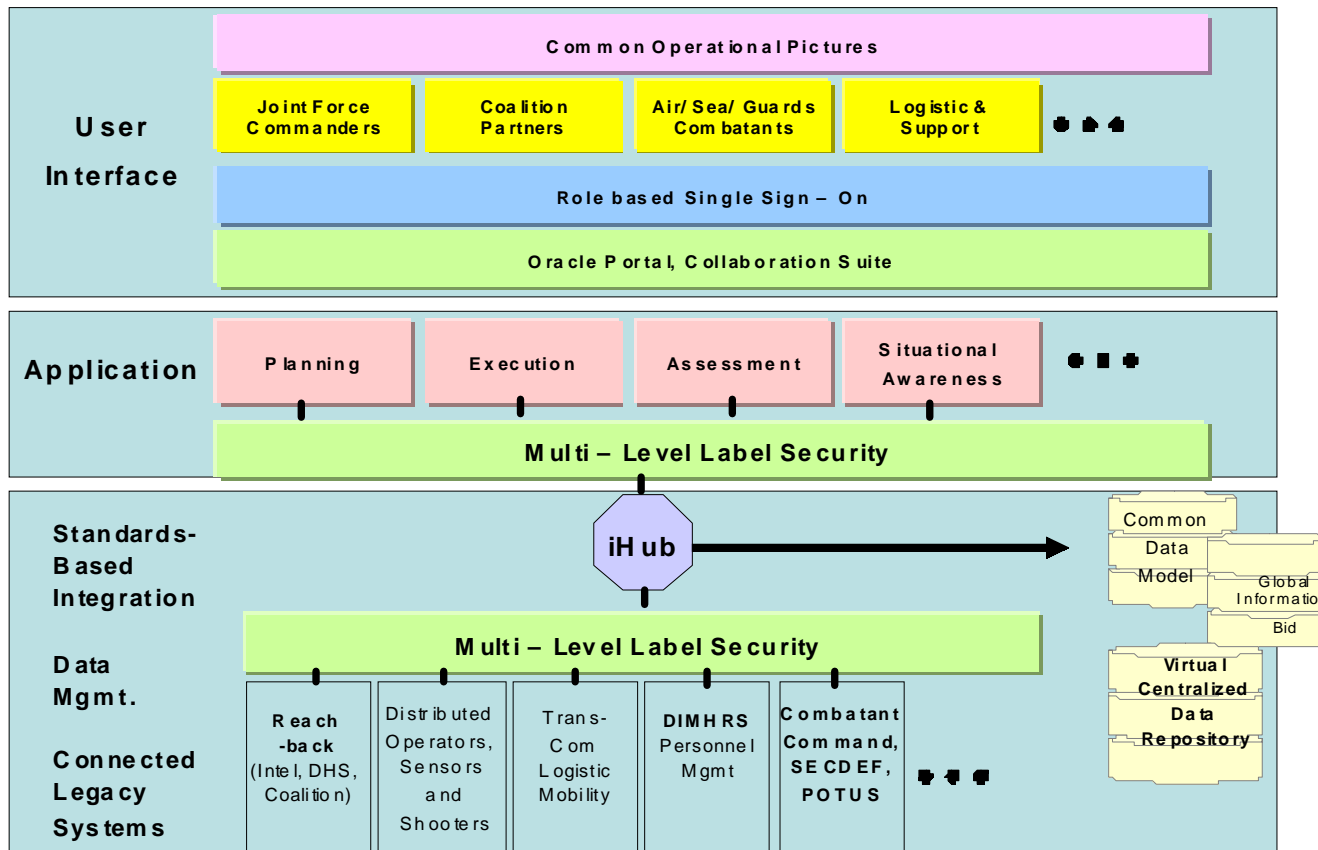
- (a) How to best use IT.
- (b) How to build IT infrastructure.
- (c) How to organise forces to learn and leverage use of IT.
- (d) How to keep boots on the ground and take advantage of forward persistence and presence.
- (e) How to preempt and enter the OODA loop of the enemy and keep the enemy off balance. There is talk of a “ten-minute” “kill-chain” by General John Jumpee of the US Air Force Chief of Staff i.e. eliminating the enemy within 10 minutes of its appearing in the battle zone.

The NCW architecture proposed by Oracle is presented in Fig. 7 and is built around the following.

- (a) Multi-level data security.
- (b) Legacy systems integration.
- (c) Community of Internet data sharing.
- (d) Geospatial data representation
- (e) Global data management.
- (f) Complex analysis and data fusion.
- (g) Rapid adaptive development
- (h) Collaboration
- (i) Configurable user interfaces

This new architecture and framework are based on Oracle’s experience of providing network-centric IT solutions to large corporations, including its own IT infrastructure. Thus, organisations with capabilities, experience and offerings like Oracle’s can be the right partners in new initiatives. They can work alongside the Services, DRDO or other peer industry teams engaged in such initiatives to cut down effort, expense, uncertainties and timeframe.

Fig. 7: NCW Architecture



Source: Building a Network-Centric Warfare Architecture, Oracle White Paper

CASE STUDY 2: NCW COLLABORATION BY BOEING CORPORATION, USA

Boeing staff writer Brad Grimes has predicted that the market for network-centric defence systems will hit \$ 200 billion over 10 years. Boeing expects to capture half of the new NCW business. Boeing has increased its stake of the business to \$ 7 billion a year, up from \$ 1 billion annually.

Last year, Boeing and Science Application's International Corporation won a \$ 15 billion contract to begin work on the future combat systems (FCS) programme. This will be a networked system to link soldiers with both manned and unmanned ground and air platforms and sensors.

Boeing is working on the following four categories of systems:

- (a) Battle communication networks.
- (b) Intelligence, surveillance and reconnaissance.
- (c) Integrated command and control and FCS.
- (d) Global situational awareness.

Boeing is also a part of a team from Lockheed Martin to compete for the US Navy's mobile users objective system, a narrow band tactical satellite communication system. Boeing has an integration centre in Anaheim and is planning a similar centre in Aclington to demonstrate network-centric operations in action.

An initiative is under way to form an industry consortium comprising Accenture, Cisco Systems, General Dynamics, IBM, Northrop, Raltheon, etc., to define the communication protocols.

Boeing has a strategic architecture group working with the DoD. The strategic focus is on interoperability of existing and new platforms and to make battlespace entities, including platforms, units, sensors and shooters "net ready."

Boeing is not attempting to define the global information grid and build new platforms and equipment to plug into this grid. Instead, the approach is to build the grid by using current capabilities and focussing on an open architecture. Building a common and open architecture into systems and

platforms is essential to support the information superiority vision of the DoD.

The result is that each node can share information with other nodes, allowing for more pertinent and accurate data to be available to each decision-maker, whether from a command centre or on the battlefield.

The concept of the common and open architecture is indeed becoming increasingly important. The FCS programme, joint tactical radio system (JTRS) and family of advance beyond line of sight terminals (FAB-T) programme each support a common architecture. Boeing, as the lead system integrator on the FCS programme, is tasked with defining the open architecture requirements for subsequent army platforms and systems. Engineers from the strategic architecture organisation are working alongside FCS programme personnel to ensure an effective, network-centric approach.

Within the Boeing Integrated Defence Systems organisation, representatives from the strategic architecture organisation are key members of each of the business strategy councils representing interests as diverse as missile defence to aerospace support to precision engagement requirements.

As brought out above, a key tool to demonstrate a network-centric environment is the Boeing Integration Centre (BIC). The BIC can be linked to other developmental laboratories across the country to demonstrate the efficacy of a network-centric environment. The labs communicate in real time to simulate warfare scenarios in a network-centric environment. According to the strategic architecture team, implementation of network-centric capabilities is already under way.

ROADMAP FOR BUILDING INDIA'S NCW CAPABILITY : RECOMMENDATIONS

The following are the outlines of a suggested NCW capability development roadmap.⁶

(a) Develop Capability in Stages: This would involve efforts and actions to recognise constraints for changing concepts, doctrines, need to

6. Brad Grimes, "Boeing : Network-Centric Operations Worth \$200 Billion," July 4.

accommodate legacy systems, budgetary constraints, technology limitations, etc.

(b) **Coordinate Concept Development and RD&D Efforts:** It is extremely necessary to experiment with state-of-the-shelf technology, development of models, war games, etc.

(c) **Guide Development:** It would be extremely critical to address the need to move beyond the existing requirements documents to make meaningful inroads into NCW. There is also a need to establish concept driven programmes.

The Services need to examine and access the current level of transformation from a paper-based work environment to a paperless work environment and give this activity the highest priority. Unless this transformation takes place, no meaningful progress would be possible.

(d) **Create a Focussed Strategic**

Programme and Steps for Developing a RD&D Plan on the Following Lines

- Create NCW task force, including experts from industry.
- Develop a vision for NCW infrastructure.
- Develop NCW taxonomy. Collaborate at inter-Service level.
- Identify gaps in technology which can impede NCW vision.
- Bring in collaboration at the national level amongst agencies to work out priorities, time lines, requirements, roadmaps, operational concepts, doctrine, etc.

The approach to develop this capability, in time varying steps, is given as follows:

(a) **Step 0:** Get off the ground by creating a thought leadership, faster ownership to the senior management, and create a critical mass of competencies. The Services need to examine and access the current level of transformation from a paper-based work environment to a paperless work environment and give this activity the highest priority. Unless this transformation takes place, no meaningful progress would be possible to evolve a network-centric operations blueprint. It is also necessary to

examine the level of in-house expertise, what is available from the DRDO and what needs to be collaborated with industry.

- (b) **Step 1:** Examine and assess current operational doctrine, existing legacy systems, gateways across IP-nets and the mediators for operational information sharing.
- (c) **Step 2:** Develop new doctrine for coordinated operations across the selected operations across the selected mission areas, create IP appliquéés for selected non-IP networks, create sensor grids, create non-satcom radio relay networks with limited dynamics, create federated management approach and structure for selected sub-grids and distributed agents for information access services.
- (d) **Step 3:** Develop new doctrines for integration across selected missions, create communication grid based on the network backbone, heterogeneous computing agents, and build automation system management functions.
- (e) **Step 4:** Create C⁴I for the grid embedded in operations, mission driven network adaptation, self-synchronised execution and an integrated battle force command.

In conclusion, NCW is inescapable and inevitable for India to establish and sustain a credible military posture. However, this transformation is extremely complex and challenging in terms of technology, doctrine and change in mindset. The NCW programme would require large funding, extensive collaboration and buy-in from higher management at the national level. The armed forces need to create the thought leadership and steer this programme. ■