Annals of the Academy of Romanian Scientists
Series on Military Science
Volume 1, Number 1/2009

THE NETWORK CENTRIC WARFARE AND NETWORK ENABLED CAPABILITIES INFLUENCES ON C4ISR SYSTEMS

Professor Gruia TIMOFTE, PhD

Specifically, the present era of warfare, in which computers have been embedded in weapon platforms and communication systems, is at best only three-decades old. Today the computer is ubiquitous and embedded in almost every aspect of modern society's activity. This trend is well known as *information and communications technology* development.

Indeed, the first electronic and programmable computer, code-named Robinson, was invented in England in 1940. It was mainly used to break German codes. Just three years later, a computer named Colossus would debut with one thousand times more speed. However, by 1946, the primary role of the computer had shifted from wartime applications to scientific endeavors. International Business Machines (IBM) introduced the IBM Model 701—which initially was named the Defense Calculator—and almost immediately received eighteen orders for use in designing aircraft and jet engines and for other applications requiring repetitive operations.[1] To be sure, much of the ability to calculate was directed towards nuclear weapons research,[2] but it is also true that business management information systems and the invention of the software language validated the

[1] http://www-03.ibm.com/ibm/history/exhibits/701/701_intro.hthl

[2] Wineguard D., Akera A.,"A Short History of the Second American Revolution," *University of Pennsylvania Almanac*, v. 42, no. 18, January 30, 1996, p. 6.

notion that wartime inventions produce commercial applications. The exponential rise in the number of computers was not envisioned, particularly outside of the scientific community.

The emergence of solid-state devices and discrete components in the late 1960's would fuel the advance of battlefield communications for the next two decades. The tactical communications of that era were not automated in the sense that they contained any semblance of computers, programmability, or networking.

In 1965, the physical chemist Gordon Moore, co-founder of Intel, predicted that the number of transistors on an integrated chip would double every eighteen months. Moore predicted that this trend would continue for the foreseeable future. Moore and most other experts expect Moore's Law to remain valid for at least another two decades.

The personal computer (PC) arrived commercially in 1981, introduced by IBM. File Transfer Protocols (FTP and later TCP/IP)[3] were developed, and soon a seven-layer scheme for moving data virtually across a multi-computer network was realized. Indeed, it took the maturation of the Internet, in concert with a graphics scheme and the hypertext markup language (HTML), to realize the World Wide Web in the early 1990's. Before that time, very few people had an e-mail address or a website with which to identify themselves. There was no widespread use of e-mail during Desert Storm, but the exponential increase in the number of personal computers, electronic mail messages, and websites was about to begin two years later. The computing power increases to $1456x10^{12}$ operations per second with 129.600 processors. In Internet 1 of 5 people of the world navigates on this network, and the mobile phone number is over 4 trillion.

The era of Network Centric Warfare was about to dawn.

From a linguistic point of view, C4I was born in the 1990's. The computer at the corps and below, however, emerged in the late 1970's. By 1970, commercial phones were being converted to touch tone (dual tone, multi-frequency). These computer-driven switches not only provided familiar multi-frequency dialing, but they also provided precedence calling and alternate call routing (alternate route) features. This new switching system, along with a system of land and radio extension nodes, would become known as Mobile Subscriber Equipment.

Thus, observations over the hundred-year period from 1920 to 2020 show that technology continues to advance at an exponential rate, transformational

[3] http://www.cisco.com/univercd//cc//td/doc/cisintwk/ito_doc/ip.htm

technologies are paradigm shifts that were not envisioned inside of twenty-year increments, sourcing of investment in technology can alternate between the private sector and government, and war erupts at unpredictable intervals.

Bandwidth is a measure of the amount of data transmitted per unit of time. A recent article states,

"In World War I, the U.S military's communications capability was about 30 words a minute. In War World II, it was about 60. In Vietnam, it was a little over 100. By 2010, it is projected to be 1.5 trillion words per minute flowing around theater. That's the equivalent of the Library of Congress every minute. Buried in there somewhere is the information that a battalion, squadron, component or joint force commander needs".[4]

To achieve the commanders' needs, the C4ISR architecture must include next-generation technologies. Many of these technologies are, in fact, envisioned as part of the global information grid and the future combat systems. They are now programmed to be delivered in the 2013 to 2025 timeframe. What can never be predicted is a "disruptive" technology, the World Wide Web in the early 1990s, for example. Disruptive technologies' are those which produce new products in new ways. Initially, they may cost more and be less effective than the more mature, 'sustaining technologies.' But eventually, they become so much cheaper and better as to drive the older technologies out of the market.

1. The Information Environment

The information environment is the aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information. The actors include leaders, decision makers, individuals, and organizations. Resources include the materials and systems employed to collect, analyze, apply, or disseminate information. The information environment is where humans and automated systems observe, orient, decide, and act upon information, and is therefore the principal environment of decision making. Even though the information environment is considered distinct, it resides within each of the four domains. The

[4] Rogers M., "C4I Interoperability for Our Warfighters," *Military Information Technology*, 7 iss.10 (December 31, 2003).

information environment is made up of three interrelated dimensions: physical, informational, and cognitive (Figure 1).[5]

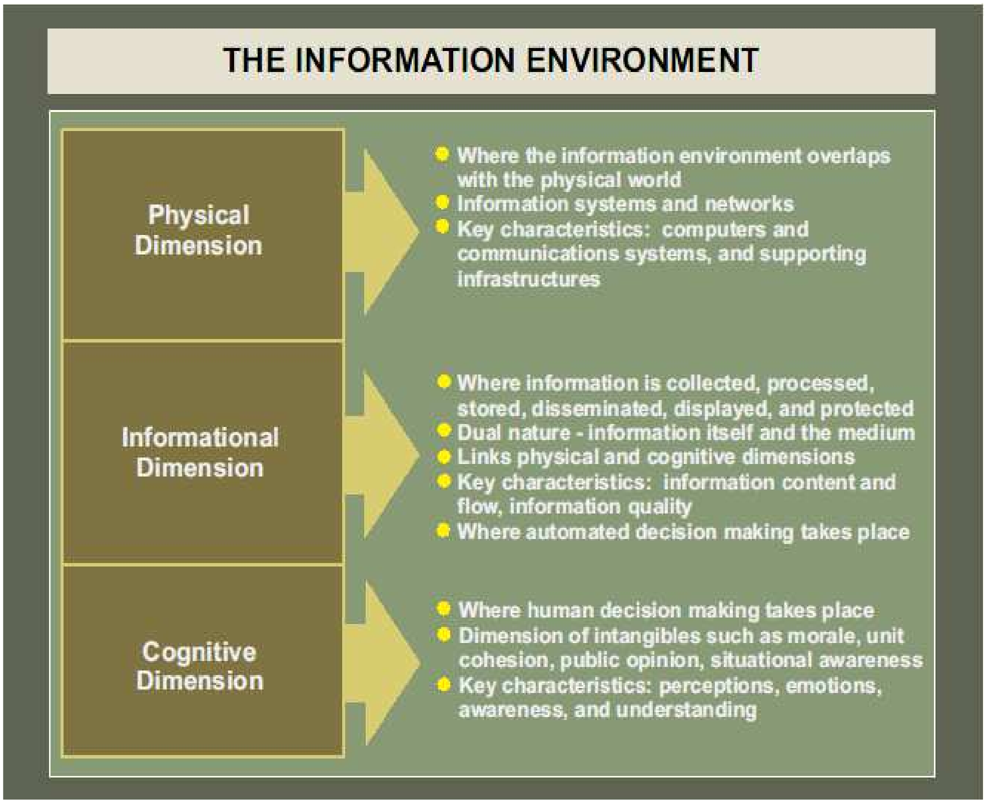
The physical dimension is composed of the command and control systems, and supporting infrastructures that enable individuals and organizations to conduct operations across the air, land, sea, and space domains. It is also the dimension where physical platforms and the communications networks that connect them reside. This includes the means of transmission, infrastructure, technologies, groups, and populations. Comparatively, the elements of this dimension are the easiest to measure, and consequently, combat power has traditionally been measured primarily in this dimension.

The informational dimension is where information is collected, processed, stored, disseminated, displayed, and protected. It is the dimension where the command and control of modern military forces is communicated, and where commander's intent is conveyed. It consists of the content and flow of information. Consequently, it is the informational dimension that must be protected.

The cognitive dimension encompasses the mind of the decision maker and the target audience. This is the dimension in which people think, perceive, visualize, and decide. It is the most important of the three dimensions. This dimension is also affected by a commander's orders, training, and other personal motivations. Battles and campaigns can be lost in the cognitive dimension. Factors such as leadership, morale, unit cohesion, emotions, state of mind, level of training, experience, situational awareness, as well as public opinion, perceptions, media, public information, and rumors influence this dimension.

Advancements in technology have enabled information to be collected, processed, stored, disseminated, displayed, and protected outside the cognitive process in quantities and at speeds that were previously incomprehensible. While technology makes great quantities of information available to audiences worldwide, perception-affecting factors provide the context which individuals use to translate data into information and knowledge.

[5] Joint Publication 3-13, *Information Operations*, Department of Defense, Washington, D.C., 2006, p.I-6.



THE INFORMATION ENVIRONMENT

Physical Dimension

- Where the information environment overlaps with the physical world
- Information systems and networks
- Key characteristics: computers and communications systems, and supporting infrastructures

Informational Dimension

- Where information is collected, processed, stored, disseminated, displayed, and protected
- Dual nature - information itself and the medium
- Links physical and cognitive dimensions
- Key characteristics: information content and flow, information quality
- Where automated decision making takes place

Cognitive Dimension

- Where human decision making takes place
- Dimension of intangibles such as morale, unit cohesion, public opinion, situational awareness
- Key characteristics: perceptions, emotions, awareness, and understanding

Figure no 1. Information Environment

There are criteria that define the quality of information relative to its purpose. The varying purposes of information require different applications of these criteria to qualify it as valuable. Additionally, each decision relies on a different weighting of the information quality criteria to make the best decision.

The finite amount of time and resources available to obtain information must be considered. Whether decisions are made cognitively or pre-programmed in automated systems, the limited time and resources to improve the quality of available information leaves decision making subject to manipulation. Additionally, there are real costs associated with obtaining quality information — that is, information well-suited to its purpose — such as those to acquire, process, store, transport, and distribute information.

Network Centric Warfare and Network Enabled Capabilities

The network centric approach to warfare is the military embodiment of information age concepts. Studies have shown that networking enables forces to undertake a different range of missions than non-networked forces, by improving both efficiency and effectiveness of operations.[6] NCW involves collaboration and sharing of information to ensure that all appropriate assets can be quickly brought to bear by commanders during combat operations.[7] Objectives of NCW include the following: self-synchronization, or doing what needs to be done without traditional orders, improved understanding of higher command's intent, improved understanding of the operational situation at all levels of command, increased ability to tap into the collective knowledge of all U.S. (and coalition) forces to reduce the "fog and friction" commonly referred to in descriptions of fighting.[8]

Key elements for implementation of NCW include the following: refine the rules and theory of NCW through simulation, testing, experimentation, and combat experience; apply NCW theory enterprise-wide in military organizations; accelerate networking in the joint force; accelerate deployment of network centric concepts and capabilities; experiment with network centric concepts to develop new ways to conduct NCW; address challenges of using NCW with coalition forces; develop appropriate doctrine and tactics for NCW.

Technologies that Support NCW. Some observers have said that the price of entry into NCW operations is the construction of a network of sensors. For example, aircraft and other platforms become sensors as they are given new capabilities to communicate and combine data, and many weapons are no longer considered simple munitions, but also become part of the system of sensors, as they are guided to their targets until they explode.

[6] Dr. Kimberly Holloman, Evidence Based Research, Inc., "The Network Centric Operations Conceptual Framework," *Presentation at the Network Centric Warfare 2004 Conference*, Washington, D.C., Jan. 20, 2004, [http://www.oft.osd.mil/library/library.cfm?libcol=2].

[7] U.S. Department of Defense, *Report on Network Centric Warfare*, 2001, [http://www.defenselink.mil/nii/NCW/ncw_sense.pdf] , and Ret. Admiral Arthur Cebrowski, Speech to Network Centric Warfare 2003 Conference, January 2003, [http://www.oft.osd.mil].

[8] "Fog" is the term that describes the uncertainty about what is going on during a battle, while "Friction" is the term that describes the difficulty translating a commander's intent into battlefield actions.

*Network Architectures***.** NCW is highly dependent on the interoperability of communications equipment, data, and software to enable networking of people, sensors, and manned and unmanned platforms. Parts of NCW technology rely on line-of-sight radio transmission for microwave or infrared signals, or laser beams. Other parts of the technology aggregate information for transmission through larger network trunks for global distribution via fiber optic cables, microwave towers, or both low altitude and high-altitude satellites. The designs for this technology must enable rapid communications between individuals in all services, and rapid sharing of data and information between mobile platforms and sensors used by all military services. The architectures must also have the ability to dynamically self-heal and re-form the network when one or more communications nodes are interrupted.

- *Satellites.* Satellites are crucial for enabling mobile communications in remote areas, as well as for providing imagery, navigation, weather information, a missile warning capability, and a capability to "reach back" to the remote HQ for added support. The Global Positioning System (GPS), consisting of 28 navigation satellites, helps identify the location of forces, as well as target locations for launching weapons, such as cruise missiles. However, despite the growing number of military satellites, up to 84 percent of the satellite communications bandwidth provided to the Operation Iraqi Freedom (OIF) theaters was supplied by commercial satellites.[9]

Radio Bandwidth. Digitization of communications is a key part of the programs associated with military force transformation. Digital technology makes more efficient use of spectrum bandwidth for communications than do analog technology. However, since 1991, there has been an explosive increase in demand for bandwidth, due to efforts to speed up the delivery of digital information. Defense officials remain concerned about whether the radio bandwidth supply available through military systems will grow adequately to keep up with increasing military demand in the future.

Unmanned Vehicles. Unmanned Vehicles, also known as Unmanned Aerial Vehicles, Ground Vehicles, and Underwater Vehicles, are primarily used for the surveillance, however their mission is evolving to also include combat.[10]

Computer Processor Chips. Gordon Moore's Law of Integrated circuits predicts that every 18 months, computer chips evolve to become twice as dense and twice as fast for about the same cost, meaning they become almost 4 times as

[9] Jefferson Morris, "GAO: DOD Needs New Approach to Buying Bandwidth," *Aerospace Daily*, Dec. 12, 2003; "DISA Chief Outlines Wartime Successes," *Federal Computer Week*, June 6, 2003.

[10] Adam Herbert, "New Horizons for Combat UAVs," *Air Force Magazine*, Dec. 2003.

powerful every 18 months. Industries that use computer technology rely on Moore's Law as a guide for investing in future technology systems.

Nanotechnology. New materials developed through nanotechnology may eventually change battlefield equipment in ways hard to imagine. Weapons may become smaller and lighter, and new miniaturized network sensors may detect, locate, identify, track, and target potential threats more efficiently. However, other countries are also making advances in nanotechnology. In 2000, 18 countries from Asia produced nearly 25,000 Ph.D. graduates in fields related to nanotechnology while the United States produced fewer than 5,000.[11]

Software. Software is an important component of all complex defense systems used for NCW. Many observers of the software industry believe that globalization of the economy dictates a global process for software development.

However, technology is only one of the underpinnings of NCW. Other observers state that NCW requires changes in behavior, process, and organization to convert the advances of Information Age capabilities into combat power. Through new uses of NCW technologies, rigid constructs are transformed into dynamic constructs that can provide new and advantageous flexibility for actions in combat. Sometimes, however, people may initially not fully utilize the capabilities of the new systems because they are not yet comfortable with the required changes in behavior.[12]

Advantages of NCW. Emerging literature supports the theory that power is increasingly derived from information sharing, information access, and speed. This view has been supported by results of recent military operational experiences showing that when forces are joint, with comprehensively integrated capabilities and operating according to the principles of NCW, they can fully exploit the highly path-dependent nature of information age warfare. Some resulting military advantages of NCW operations include the following:

(1) Networked forces can consist of smaller-size units that can travel lighter and faster, meaning fewer troops with fewer platforms and carrying fewer supplies can perform a mission effectively, or differently, at a lower cost.

(2) Networked forces can fight using new tactics. During OIF, U.S. Army forces utilized movement that was described by some as "swarm tactics." Because networking allows soldiers to keep track of each other when they are out of one another's sight, forces could move forward in Iraq spread out in smaller

[11] CRS Report RS20589, *Manipulating Molecules: The National Nanotechnology Initiative*.

[12] Frederick Stein, Senior Engineer, MITRE Corporation, *Presentation on Network Centric Warfare Operations*, 4th Annual Multinational C4ISR Conference, McLean, Virginia, May 6, 2004.

independent units, avoiding the need to maintain a tight formation. All units know each other's location. If one unit gets into trouble, other independent units nearby can quickly come to their aid, "swarming" to attack the enemy from all directions at once. Benefits may include the following: (1) fewer troops and less equipment are needed, so waging war is less expensive; (2) it is harder for an enemy to effectively attack a widely dispersed formation; (3) combat units can cover much more ground, because they do not have to maintain a formation or slow down for lagging vehicles; (4) knowing the location of all friendly units reduces fratricide during combat operations; and (5) swarming allows an attack to be directed straight into the heart of an enemy command structure, undermining support by operating from the inside, rather than battling only on the periphery.

(3) The way individual soldiers think and act on the battlefield is also changing. When a unit encounters a difficult problem in the field, they radio the Tactical Operations Center, which types the problem into an online chat room, using Microsoft Chat software. The problem is then "swarmed" by experts who may be located as far away as the Pentagon.[13]

(4) The sensor-to-shooter time is reduced. Using NCW systems, soldiers in the field have the capability to conduct an "on site analysis" of raw intelligence from sensor displays, rather than waiting for return analysis reports to arrive back from the continental United States.[14]

Information Overrated. Some observers state that Information Age technology is making time and distance less relevant, and that information increases the pace of events and the operational tempo of warfare.[15] However, other observers believe that networking for information exchange is not a sufficient substitute for combat maneuver, and that information superiority and situational awareness are not the most significant components of combat power. As in a chess game, these observers believes is knowing the next move to make that is the key to success in battle, for example, through correct analysis of an anticipated enemy movement and tactics.[16]

[13] Joshua Davis, "If We Run Out of Batteries, This War is Screwed," *Wired Magazine*, June 2003, [http://www.wired.com/wired/archive/11.06/battlefield.html].

[14] U.S. Department of Defense, Office of the Secretary, *Unmanned Aerial Vehicles Roadmap*, 2002-2007, Dec. 2002.

[15] David Alberts, John Garstka, Frederick Stein, *Network Centric Warfare*, DOD Command and Control Research Program, Oct. 2003, p. 21.

[16] Edmund Blash, USAR, "Network-Centric Warfare Requires a Closer Look," Signal Forum, *Signal Magazine*, May 2003.

Other observers also state that huge information resources may be overrated as an asset for creating effective military operations, and that important military decisions may not always lend themselves to information-based rational analysis. Some of the issues raised by these observers include:

(1) Quantitative changes in information and analysis often lead to qualitative changes in individual and organizational behavior that are sometimes counterproductive.

(2) Reliance on sophisticated information systems may lead to management overconfidence.

(3) An information-rich, opportunity-rich environment may shift the value of the information, redefine the mission objectives, and possibly increase the chances for perverse consequences.

Interoperability. Some question whether the U.S. military can achieve true network and systems interoperability among all services.

Bandwidth Limitations. Some observers question whether communications bandwidth supply can be made adequate to match growing future military needs. When the supply of bandwidth becomes inadequate during combat, military operations officers have sometimes been forced to subjectively prioritize the transmission of messages.

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 that may eventually threaten U.S. global technical superiority and undermine current NCW advantages. The Gartner Group research firm has reported that corporate spending for offshore information technology services will increase from $1.8 billion in 2003 to more than $26 billion by 2007, with half of the work going to Asian countries such as India and China.[17]

Key Military Programs

In 2004, Pentagon officials used a “Net-Centric Checklist” during department wide reviews of high technology programs to ensure the inclusion of network centric capabilities for military platforms (Table 1). The checklist consists of approximately 84 questions that program managers must answer showing how their systems meet NCW requirements.[18]

[17] Paul McDougall, “Optimizing Through Outsourcing,” *Information Week*, Mar. 1, 2004, p.56.

[18] CRS Report for Congress, Order Code RL 32411, *Network Centric Warfare: Background and Oversight for Congress*, Congressional Research Service, Washington, D.C., 2006, pp.15-20.

Net Centricity. The Net Centricity program is intended to support information technology activities for network-centric collaboration. Horizontal Fusion is a component that determines how quickly military and intelligence community programs can be extended to a net-centric operational environment. Facility is a component that tests interoperability of key systems in an end-to-end manner, including the Joint Tactical Radio System (JTRS) and the Global Information Grid Bandwidth Expansion (GIG BE) programs.

Air Force Advanced Tactical Targeting Technology (AT3). The AT3 system combines information collected by an airborne network of sensors to identify the precise location of enemy air defense systems. The system relies on coordination of information from different systems aboard multiple aircraft.

Air Force Link 16. Tactical Data Links are used in combat for machine-to-machine exchange of information messages such as radar tracks, target information, platform status, imagery, and command assignments.

Navy Cooperative Engagement Capability (CEC). The CEC system links Navy ships and aircraft operating in a particular area into a single, integrated air-defense network in which radar data collected by each platform is transmitted on a real-time (i.e., instantaneous) basis to the other units in the network. Each unit in the CEC network fuses its own radar data with data received from the other units. As a result, units in the network share a common, composite, real-time air-defense picture. CEC will permit a ship to shoot air-defense missiles at incoming anti-ship missiles that the ship itself cannot see, using radar targeting data gathered by other units in the network. It will also permit air-defense missiles fired by one ship to be guided by other ships or aircraft.

Army Force XXI Battle Command Brigade and Below (FBCB2). FBCB2, used with Blue Force Tracker computer equipment, is the U.S. Army's main digital system that uses the Tactical Internet for sending real-time battle data to forces on the battlefield. The computer images and GPS capabilities allowed tank crews to use Blue Force Tracker to pinpoint their locations, even amid Iraqi sand storms, similar to the way pilots use instruments to fly in bad weather.

Joint Tactical Radio System (JTRS). The software-based JTRS Program offers a way to bring together separate service-led programs into joint software defined radio development effort. JTRS is a family of common, software-defined, programmable radios that are intended to interoperate with existing radio systems and provide the additional capability to access maps and other visual data by allowing the war fighter to communicate directly with battlefield sensors.

Joint Unmanned Combat Air Systems (J-UCAS). The J-UCAS program combines the efforts conducted for a common architecture to maximize interoperability. All four military services are developing and fielding Unmanned

Aerial Vehicles for tactical purposes and the rate of acquiring these systems greatly exceeds expectations of just a few years ago.

Table 1

Program ($)	**2003**	**2004**	**2005**	**2006**	**2007**	**2008**	**2009**
Horizontal Fusion (mil.)	-	-	206,422	207,815	210,864	222,126	226,586
GIG Evaluation (mil.)	-	-	7,800	8,200	8,600	9,100	9,500
AT3 (mil.)	11,023	5,815	-	-	-	-	-
LINK 16 (mil.)	50,535	70,481	141,012	218,743	228,009	161,909	153,606
Navy CEC (thousands)	106.020	86.725	103.452	-	-	-	-
Army FBCB2 (thousands)	59.887	47.901	23.510	-	-	-	-
JTRS (thousands)	95.790	259.990	249.880	-	-	-	-
J-UCAS (mil.)	667,307	380,105	1043,498	986,156	-	-	-

NNEC is the Alliance's cognitive and technical ability to federate the various components of the operational environment, from the strategic level (including NATO HQ) down to the tactical levels, through a networking and information infrastructure.[19]

From a strategic and operational perspective, the aim is the enhancement the mission effectiveness through the connection of a number of sensors (or collectors), decision makers, and effectors – they may be weapons or anything else –, to ensure the best flow and use of information all along the chain of command. The Figure 2 is just one illustration of these tenets, in the specific case of a Time Sensitive Targeting scenario which stress a few ideas:

[19] Ruud v. Dam, *NATO Network Enabled Capabilities*, Presentation at AFCEA Symposium, Paris, 2006.

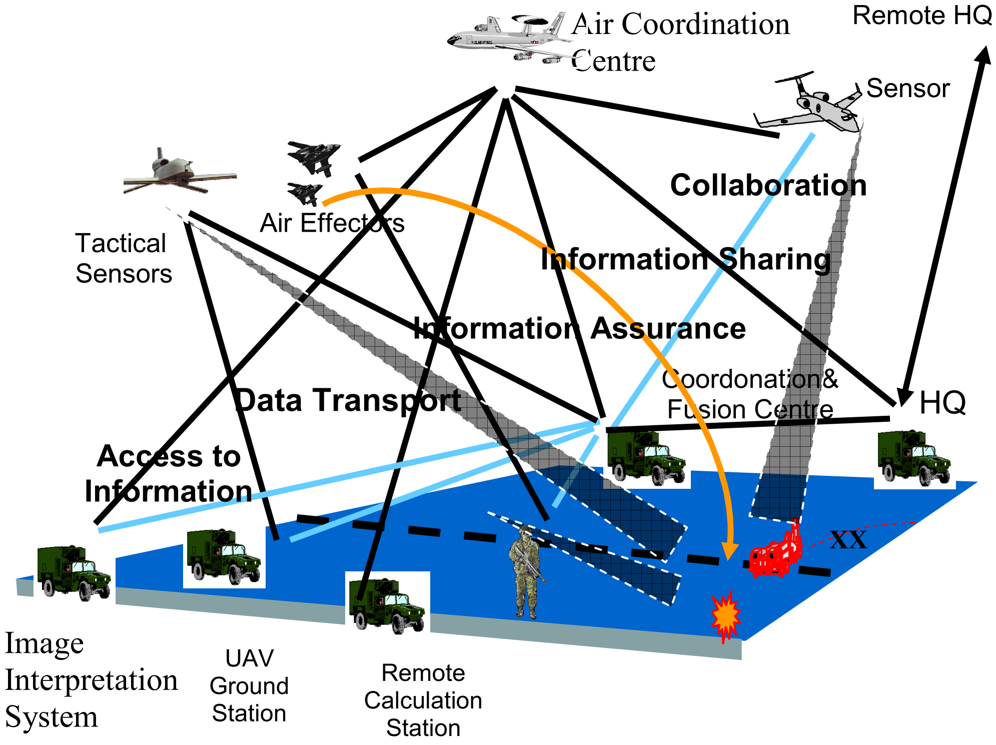


Figure no 2. NNEC Fundamentals

The first one is to emphasize the reach for NNEC as global, which means it should be available in any location that the Alliance deems suitable, within or beyond the area of responsibility. The recent experiences of operations conducted by the Alliance underline the need for expeditionary forces, and NNEC has to enable and support this key requirement.

The second idea to point out that the capability encompasses all levels of action, from the tactical to the strategic level. The recurrent request from the operators to have a reach back capacity shows clearly that the expected flow of information has to go back and forth through all levels in order to allow the appropriate situational awareness and command and control.

NNEC aims to support the full range of missions, from peace support to high level intensity conflict, including humanitarian relief or other kind of missions. Moreover, NNEC must support the ability of a coalition to interact and cooperate with non-military elements of the environment, as implied in an Effect Based Approach to Operations. It becomes obvious that NNEC is not just about Command and Control, but is an opportunity to enhance the linkage between the various capabilities that are needed by a coalition to conduct an operation.

2. C4ISR System

The C4ISR "system" is not to be regarded as a single system, but rather as a distributed system-of-systems (Figure 3) where each system is producing and/or consuming services. A cornerstone in the service-oriented concept is the separation of the producers and consumers of functionality. The services are not necessarily produced for a single particular purpose; they are instead produced independently of the consumers and are made generally available for any authorized consumer to use.

The systems-of-systems concept also means that services and information residing in existing and new systems are integrated and aggregated. Thereby services and information with a higher value are created. Neither the infrastructure nor the technical systems producing the services need to be new systems, even though new systems may of course also be included. Existing legacy systems can be integrated into the service environment by means of encapsulation. The C4ISR solutions are completely scalable; services and capabilities can be further developed and the range of services and systems can be extended over time in an evolutionary fashion.

C4ISR is the integration of doctrine, procedures, organizational structures, personnel, equipment, facilities, communications, and intelligence to support a commander's ability to command and control across the range of military operations. C4ISR provides commanders with timely and accurate data and systems to plan, monitor, direct, control, and report operations.

Command and Control System — the facilities, equipment, communications, procedures, and personnel essential to a commander for planning, directing, and controlling operations of assigned and attached forces pursuant to the missions assigned.

Communications System - an assembly of equipment, methods and procedures and, if necessary, personnel, organized to accomplish information transfer functions. A communication system provides communication between its users and may embrace transmission systems, switching systems and user systems.

A communication system may also include storage or processing functions in support of information transfer.

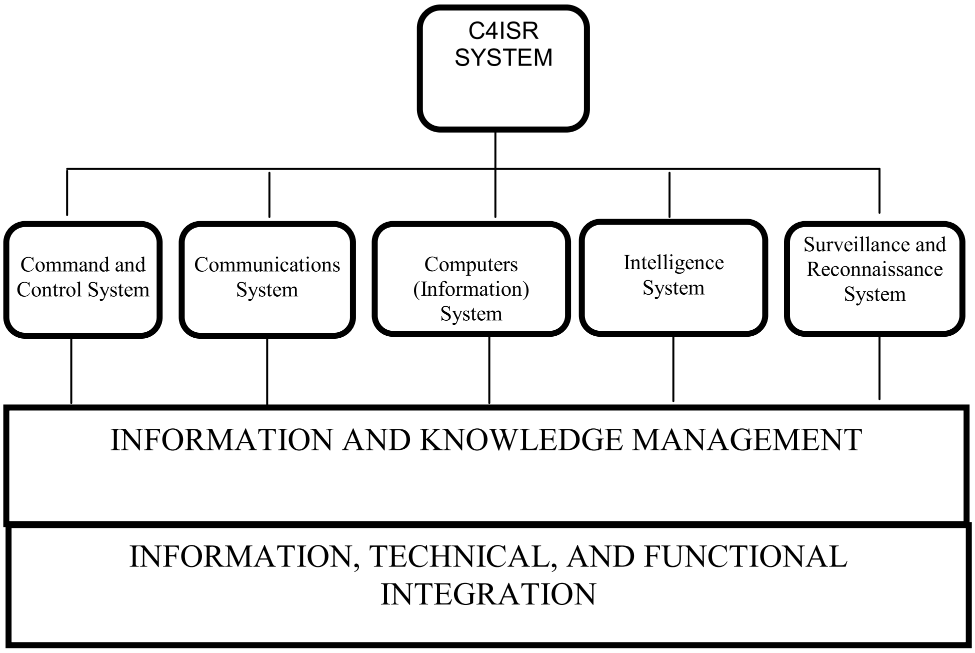

C4ISR SYSTEM
Command and Control System
Communications System
Computers (Information) System
Intelligence System
Surveillance and Reconnaissance System
INFORMATION AND KNOWLEDGE MANAGEMENT
INFORMATION, TECHNICAL, AND FUNCTIONAL INTEGRATION

Figure no 3. C4ISR System Structure

Information System represents an assembly of equipment, methods and procedures and, if necessary personnel, organized to accomplish information processing functions. Examples of information system are: command and control information system, management information system, office automation system. An information system may also transfer information in support of the processing functions, for example, over a local area network interconnecting a number of computers, which are part of the information system.

Intelligence System — any formal or informal system to manage data gathering, to obtain and to process the data, to interpret the data, and to provide reasoned judgments to decision makers as a basis for action. The term is not limited to intelligence organizations or services but includes any system, in all its parts, that accomplishes the listed tasks.

Intelligence, Surveillance, and Reconnaissance — an activity that synchronizes and integrates the planning and operation of sensors, assets, and processing, exploitation, and dissemination systems in direct support of current and future operations. This is an integrated intelligence and operations function.

Sensor System - an assembly of equipment, methods and procedures and, if necessary, personnel, organized to detect persons, objects, phenomena or activities and record, process, and possibly transfer the information. A sensor system may use one or more sensors of one or more techniques.

The main advantages of the networks-of-networks approach are:[20]

• Combined use of different networks leading to improved efficiency and a reduction of equipment and operational costs, as compared to traditional vertically integrated networks ("stovepipe networks").

• The networks-of-networks can be dynamically composed depending on where network resources are needed for the moment.

• Due to the distributed network architecture and packet-based transmission there is no single point of failure. If a piece of equipment is damaged, others continue to operate and joint communications are maintained using alternative paths. If all connections to other networks are lost, sub-networks are formed that may operate autonomously and later be reconnected. The networks-of-networks approach puts special requirements on infrastructure functionality like routing, addressing, mobility, quality of service, and security. In order to fulfill these requirements it is advantageous to make use of IP version 6.

The basic idea behind the *service-oriented architecture* is to avoid large "stovepipe" systems, designed only for a specific purpose, and instead make it possible to combine individual systems into systems-of-systems. This means that the individual systems, that may be geographically distributed, are used as modular building blocks that are interconnected. The output of these building blocks is made available as generally accessible services permitting the blocks to be combined in different ways. Among the advantages with such an approach are a more cost efficient use of systems, and the possibility to adapt to the needs of the particular situation by reconfiguration in real time of the building blocks into so-called situation-adapted systems.

The system has two main parts: Services and Infrastructure. The Services part includes services for Communication & Collaboration, Situation Information, Information Operations, Command & Control and Engagement Support. The

[20] *C4ISR for Network-Oriented Defense*, White Paper, Ericsson, Stockholm, 2006, pp.6-7, 16-18.

Infrastructure part includes a Control Layer, a Convergence Layer and a Connectivity Layer.

The Communication & Collaboration services provide functionality for communication and information sharing. Situation Information services involve gathering, processing and dissemination of situation information. Information Operations include services for assessment and influence on other parties' situation information and also for protection of the own situation information. Command & Control involves services for decision support and order handling. Engagement systems and effectors are connected to the C4ISR environment and are involved in the information flow and controlled by Engagement Support services.

The Control Layer contains functionality and support services that are used to give all the services mentioned above the required characteristics and features such as security, mobility, and accessibility. The Convergence Layer ensures that connectivity can be accomplished in a unified manner based on the Internet Protocol and different types of fixed and wireless networks, belonging to the Connectivity Layer, can be used.

3. New Requirements for C4ISR Systems

The Institute for Electrical and Electronics Engineers (IEEE) defines the term architecture as "the structure of components, their relationships, and the principles and guidelines governing their design and evolution over time."[21] The Framework is careful to differentiate between an architecture description and an architecture implementation. The description means the "blueprint," while the implementation means the real-world capabilities and assets in the field. The Framework does not address how the blueprint-to-implementation process takes place. The Framework does, however, divide a architecture into three views—the operational, systems, and technical views defined as follows:

- Operational Architecture View—a description of the tasks and activities, operational elements, and information flows required to accomplish or to support a military operation.

- Systems Architecture View—a description, including graphics, of systems and interconnections providing for, or supporting, war fighting functions.

- Technical Architecture View—the minimal set of rules governing the arrangement, interaction, and interdependence of system parts or elements, whose

[21] *C4ISR Architecture Framework Study,* (Washington, D.C.: U.S. Department of Defense, 18 December 1997), p.15.

purpose is to ensure that a conformant system satisfies a specified set of requirements.[22]

The main lessons learned and conclusions for the future development of C4ISR systems are as follows:[23]

- The existing switching systems were designed to support a bandwidth requirement of 93% voice, 7% data and 0% video;

- The transmission systems, based on land line-of-sight vans, were limited in the bandwidth;

- The Mobile Subscriber Equipment does not have the flexibility to "trade-off" between voice and data; at the same time it was not fully deployed (in terms of time, distance, operations tempo);

- A division main command post has only a data rate of 512 Kbps; command post installation varied from 45 to 60 minutes for initial operating capabilities;

- Legacy systems were not able to interoperate at all times;

- Great difficulties were created by combining legacy systems, commercial systems and items being designed for the military agencies;

- the Army Battle Command System encompasses 8 specialized command and control to ensure the ability to provide a clear, accurate and common view of the battle space;

- a Joint Common Database was created to display notional overlays, friendly unit locations, specific enemy equipment, facilities and individuals, logistic information, adjacent and higher units, unmanned air vehicle activity, cruise missile speed and direction at fight, weather conditions, mobility, etc.;

- Spectrum management was a major concern at all levels;

- The communications platforms for mobile operations were not updated;

- Communications systems were not provided to support commanders with time-sensitive situational awareness and battle command on the move capabilities;

- In 2004, data requirements per individual soldier rose over one hundred per cent since Desert Storm;

- A major flaw in joint and coalition systems was the lack of interoperability;

- Tactical satellites provided on the move capabilities of the force, but the quantity was insufficient to equip every unit;

[22] DoD Architecture Working Group, *DoD Architecture Framework Study*, (Washington, D.C.: U.S. Department of Defense, 9 February, 2004), vol 1. pp.2-4.

[23] Cogan K., Lucio R., Network Centric Warfare Case Study, Volume II: *A View of C4 Architecture at the Dawn of Network Centric Warfare*, U.S. Army War College, Carlisle Barrackis, Pennsylvania, 2006, Chapter 4-5.

- Collaboration tools were used between small groups of users due the network limitations;

- There were many commercial operating systems, but little interoperability or commonality.

During the OIF some measures were taken to modernize the systems (War-fighter Information Network Tactical, Joint Network Node, Command Post of the Future), to adjust equipment to the exponential increase in bandwidth requirements, to shorten the acquisition cycle from 10 to 3 years or less, increase the transmission capacity from 1024 Kbps to 8192 Kbps, etc.

Five principal components of the C4ISR were named for 2010 and beyond:

▪A robust multi-sensor information grid providing dominant awareness of the battle space to commanders and forces;

▪Advanced battle-management capabilities that allow employment of globally deployed forces faster and more flexibly than those of potential adversaries;

▪An information operations capability able to penetrate, to manipulate, or deny an adversary's battle space awareness or unimpeded use of his own forces;

▪A joint communications grid with adequate capacity, resilience, and network-management capabilities to support the above capabilities as well as the range of communications requirements among commanders and forces;

▪An information defense system to protect own globally distributed communications and processing network from interference or exploitation by an adversary.

These recommendations have already been promulgated for a full range of hardware and software technologies. It can be assumed that some of those technologies will be applicable to next-generation networks and C4ISR systems.