HISTORY AND EVOLUTION OF NETWORK-CENTRIC WARFARE

SANJAY PODUVAL

Know your enemy and know yourself; in a hundred battles
you will never know peril.

— Sun Tzu

The history of war is replete with instances of a player using superior knowledge garnered from various sources to gain a war winning advantage. The fact is that the more knowledgeable player has the advantage of being able to anticipate the opponent's moves and deployment patterns and is better poised to field to his assets to fashion the desired results. The "various sources" referred to are the extension of the eyes and ears into an adversary's domain which constitute the information deriving web. This, when properly coordinated and with proper security, timeliness and reliability, forms a war winning network. Referring to the "network," environment as a noun, means an interconnected group or system, while "to network" denotes the act of interconnecting. Networking is not novel; it has evolved over a period of time and its methods have changed. Network-centric operations deal with shaping networks to exploit the emerging environment to one's advantage. The fundamental philosophy of Network-Centric Warfare (NCW) is that the

* Wing Commander **Sanjay Poduval** is a Research Fellow at Centre for Air Power Studies, New Delhi.

The roots of today's NCW can be traced back to the time when telegraphy was introduced.

network makes the difference. The aim of this paper is to trace the roots of NCW in the context of the present. The paper also endeavours to highlight a few of the important features which have developed to enhance the speed, precision and lethality of operations.

TRACING THE ROOTS

Historically, every nation has sought to create a "usable military advantage" over its enemies and potential adversaries to create an asymmetric advantage in its favour. Therefore, providing fighting forces the most accurate intelligence, surveillance and reconnaissance information is nothing new to the military. The need to be connected with the troops has been an essential requirement since times immemorial. Information was passed by means of hand signals, smoke screens, drum beats, etc for tactical positioning. Visual communications had reached a peak by the end of the 18th century and were the primary means of communications for forward control. Large and small flags, heliograph and oil lamps with shutters for night communications were utilised. Skilled operators could signal from 8 to 12 words per minute.

However, the search for usable military advantage relied heavily on acquiring superior technology and instruments of warfare, besides devising superior military strategy and tactics. The roots of today's NCW can be traced back to the time when telegraphy was introduced. The British used wireless telegraphy extensively during the Second Boer War 1899-1902 in South Africa. Strategically, the telegraph was used for communication with the home government in London by submarine cable. In the theatre, the land line was used to control formations down to the level of divisions and occasionally lower later in the war. During the Boer War, the telegraph battalion's section laid 18,000 miles of telegraph and telephone cable. A total of 13,500,000 messages were handled in four years. It was also the first time a telegraph battalion provided technical and strategic communications for

the army when Gen French used telegraph and telephones to control artillery fire.[1]

Radio Communication

The Russo-Japanese War which broke out in the year 1904 as a result of the conflicting interests between St. Petersburg and Tokyo was probably the first war which exploited the newly introduced radio systems to communicate plans with their respective forces at sea. The radio equipment was more user friendly, less cumbersome and did not require a specialist for operation. The Japanese fleet commanded by Admiral Togo, had set up a system of continuous surveillance by carefully positioning their patrol ships at key locations. The success of Admiral Togo's plan relied on the premise that he would have maximum early sightings because of tactically positioned ships and, more importantly, swift early warning by radio. In short, the whole plan was based on the efficiency and speed of radio communication network without which the Russian ships commanded by Admiral Rozhestvenskiy could slip through. In the battle that followed, the Japanese fleet, because of better coordination between the ships and helped by Admiral Rozhestvenskiy's decision of a complete radio blackout, enabled the Japanese to have an information upper hand which resulted in a famous victory for Admiral Togo. The important issue here, even when networking was in its primitive stage, was that it was a double-edged sword. Had Admiral Rozhestvenskiy decided to disrupt the Japanese communication, which was very much possible, the outcome of the battle may well have been different.

The Japanese fleet, because of better coordination between the ships and helped by Admiral Rozhestvenskiy's decision of a complete radio blackout, enabled the Japanese to have an information upper hand which resulted in a famous victory for Admiral Togo.

The Austrians were probably the first to realise that this weakness was an excellent means of acquiring political and military intelligence which was

1. "The Second Boer War 1899-1902", http://www2.army.mod.uk/royalsignalsmuseum/displays/boer_war/index.htm

previously obtained through costly and dangerous espionage missions. In fact, when a political crisis arose in 1908 as result of the Austro-Hungarian Empire's annexation of Bosnia and Herzegovina, the Austrians intercepted and deciphered Italian radio traffic through their network and used this intelligence to shape their foreign policy.[2] This was perhaps the first time in history that the course of a military campaign conducted hundreds of kilometres away was followed move by move by technical means.

Air Defence Systems

Networking progressed many notches with the advent of radars. Radar was developed in great secrecy in Great Britain, and from 1937 to 1939, it developed into the core of the world's first integrated Air Defence (AD) System known as Chain Home (CH). This consisted of twenty-one 300-foot masts sited along the east coast of Britain, its coverage stretched from the Isle of Wight to the Scottish border, forming a network of radar defence, supported by Chain Home Low (CHL) Stations, which were able to detect low flying aircraft.[3] Following the outbreak of World War II, they were put into action during the Battle of Britain. The Chain Home System was complemented by Ground Control Intercept (GCI) radars which vectored the air defence fighters on to the hostile aircraft formation. In addition to the control of air defence fighters, Britain had set up a defence system which brought all the weapons available into play.

Chain Home radar stations, which could 'see' an enemy raid, in some cases while it was still over France, were positioned all along the coast. The raid was reported to Fighter Command Headquarters (FCHQ) where it was passed down to the Group Headquarters, which further passed it on to the Sector Control Rooms affected by the plot. The entire system was meshed for information sharing in both directions. The height of the raid was provided by Observer Corps posts once the raid came within visual sighting range. The sector controller then knew exactly where the enemy were and alerted the

2 Bartholomew Lee, "Radio Spies," http://www.trft.org/TRFTPix/spies9eR2006.pdf

3. See http://www.radarpages.co.uk/mob/chl/chl.ht m

balloon sites in possible target areas to put up a balloon barrage. The balloons forced the German pilots to fly their bombers higher, which made bombing more difficult and also ensured that the intruding aircraft were in the radar envelope for as long as possible. The sector controller also forewarned the anti-aircraft gun sites along the route of the raid of the ensuing raid so that they were ready to fire when the enemy came within range. Most importantly, the sector controller could scramble fighters from his sector airfields and vector (direct) them towards the incoming raid. In order to vector the defending fighters on to an incoming raid, the controller had to know exactly where they were. The last link in the defence system, keeping track of the Royal Air Force (RAF) fighters, was Direction-Finding or D/F radio stations. These also reported to their local Sector Control Room. The RDF information was crude by modern standards, but was more than sufficient to give bearing and range information on an incoming raid. This information was transmitted to all other sectors in the command to keep the "big picture" spread throughout the system. By doing this, the loss of a single Sector Control Room did not destroy Fighter Command's ability to function as an effective defence. As a result of this deployment, when the German offensive actually began on August 12, 1940, the German bomber pilots, much to their surprise, found that the British fighters systematically placed themselves in advantageous positions and managed to time their confrontation over the English Channel. Winston Churchill summed up the effect of the battle and the contribution of the Fighter Command with the words, "Never in the field of human conflict was so much owed by so many to so few."

The Kammhuber Line

In 1940, Col, later Gen Josef Kammhuber was tasked to build a night air defence for Germany in 1940, which came to be known as the Kammhuber Line.[4] Initially, the Kammhuber Line involved an extensive network of searchlights, radars, and night fighters based in occupied France, Belgium, and Holland, covering approach routes of the British bombers. Early on, searchlights illuminated each

4. Air Vice Marshal J.P.R. Browne and Wg Cdr M.T. Thurbon *Electronic Warfare*, Vol IV (Ritna Books).

bomber as a Messerschmidt Bf-110 or Junkers Ju-88 night fighter assigned to that area closed in for the kill. In 1941, a radar-controlled master searchlight was introduced which made the Kammhuber Line even more effective by locking onto bombers automatically and illuminating the target with a pale blue guide beam that manually directed searchlights could pick up.

Radar-directed searchlights gave way to a more elaborate system of search and tracking ground radar and radio stations, known collectively as the "Himmelbett" system. A Himmelbett station consisted of a Freya radar for early warning with a range of 60 to 150 km, a Würzburg radar for plotting bombers, and a second Würzburg radar was utilised for guiding the fighter aircraft. Each Himmelbett zone or "box" had a radius equal to the range of the Würzburg tracking radar (about 43 km wide and 34 km deep). These boxes were the building blocks of the improved Kammhuber Line. Target range, altitude, speed, and bearing data were sent to a ground control station that directed the fighters towards the British bomber stream. RAF bombers flying into Germany or France had to cross the Kammhuber Line at some point, and the Freya radar operators would detect them and direct Würzburg radars to illuminate the plane. All position reports were sent to the Himmelbett Control Centre thereby allowing controllers in the Himmelbett Centre to get continuous updates on the positions of both planes. The second Würzburg radar controlling the German fighters would direct them to intercept the now illuminated bomber. Thus, each night fighter was like a spider at the centre of an invisible web of beams.

The Bekaa Valley Conflict

Over the years, command, control and communications capability progressed steadily, improving the operating picture provided to commanders at various levels. The Bekaa Valley conflict carried this further. The conflict, known for bringing Electronic Warfare (EW) to the fore and the innovative use of Unmanned Aerial Vehicles (UAVs) in the battlefield was also important in the manner in which the more intangible network was used to decisive war-fighting advantage.

It was the first combat operation involving the use of the modern Airborne Early Warning and Control system (AEW&C) aircraft, the E-2C Hawkeye.[5] It could scan three million cubic miles of air space, monitor over 200 aircraft simultaneously and control up to 130 separate air-to-air engagements at ranges up to 250 miles.[6] This capability enabled the Israeli Air Force (IsAF) to detect Syrian aircraft as they took off, allowing it to determine how many hostile aircraft were inbound and from which direction. The Israelis also used F-15s in the rear as "mini-AWACS" to help manage air-to-air engagements. The integration of these systems ensured a high level of situational awareness. The Israeli aircraft were vectored to the 'blindside' of Syrian MiGs which had only nose and tail threat warning receivers. They also effectively neutralised the Syrian radar and communication systems, leaving them isolated and vulnerable to AWACS directed attacks from F-15s and F-16s. The result was chaos within the Syrian formations.

The Bekaa Valley conflict provided the first example of warfare in real-time in which air reconnaissance and distribution of its results to attacking forces was carried out almost simultaneously.

Another technological innovation was the use of UAVs. They were used not only as decoys but also as intelligence gathering platforms for finger printing the Surface-to-Air Missile (SAM) radar frequencies and streaming almost 'real-time' video to the E-2C Hawkeye and to the command and control centres on the ground. The SAM complexes were neutralised as soon as they were switched on. They were targeted by surface-to-surface missiles or by anti-radiation missiles launched from F-4 Phantoms. Overall, the Bekaa Valley conflict provided the first example of warfare in real-time in which air reconnaissance and distribution of its results to attacking forces was carried out almost simultaneously in rapid succession, closely coordinated by AWACS and ground stations using

5. Frank J. O'Brien, *The Hungry Tigers: The Fighter Pilot's Role in Modern Warfare* (Blue Ridge Summit, Pa.: Tab Books, 1986).

6. David M. Russell, "Lebanon Proved Effectiveness of Israeli EW Innovations," *Defense Electronics*, October 1982.

secure and reliable communication and video links in an electromagnetic intense environment.

A magnified version of this was evident in both the Gulf War of 1991 and Iraq War of 2003. The shift in focus from the platform to the network is obvious. The emphasis now is to view actors as part of a continuously changing ecosystem rather than as independent entities.

THE WEB AS WE KNOW IT

Network-centric warfare can trace its immediate origins to 1996 when Admiral William Owens introduced the concept of a "system of systems" in a paper of the same name published by the Institute National Security Studies. Owens described it as the serendipitous evolution of a system of intelligence sensors, command and control systems, and precision weapons that enabled enhanced situational awareness, rapid target assessment, and distributed weapon assignment. As a distinct concept, however, NCW first appeared publicly in a 1998 US Naval Institute Proceedings article by Vice Admiral Arthur K. Cebrowski and John Gartska. "Network-Centric Warfare: Its Origins and Future." It described a new way of thinking about military operations in the information age and highlighted the relationship between information advantage and competitive advantage. Given the short period of time that has transpired since then, there has been an enormous amount of progress in getting the fundamental tenets of network-centric operations understood.

The term "network-centric warfare" broadly describes the combination of emerging tactics, techniques, and procedures that a fully or even partially networked force can employ to create a decisive war-fighting advantage. Network-centric warfare is an information superiority enabled concept of operations that describes the way forces will probably organise and fight in the information age. NCW generates increased combat power by networking sensors, decision-makers, and shooters to achieve shared awareness, increased speed of command, high tempo of operations, increased lethality, and greater survivability.

NCW TODAY: A BIRD'S EYE VIEW

The utility of networked information produced by integration of radars, communication systems, AWACS, Joint Surveillance Target Attack Radar System (JSTARS), etc is beyond dispute. NCW today envisages the integration of information from all sensors and making it available, as required, wherever required, to the authorised recipients. The objective is to provide a very high level of situational awareness that will, in its wake, lead to greater efficiency in the prosecution of war. The availability of information is not intended to be a one-way street, but field units can also demand information in real-time and vice versa. With an effective network, the geographic location of the controlling authority becomes irrelevant. It could occupy a permanent/relocatable location, immaterial of where the battle is being waged. With good situational awareness and communications, quick decisions can be arrived at, transmitted and implemented. This is a considerable advantage. A few of the factors which have ensured that NCW plays a prominent role in today's conflicts are discussed below.

NCW today envisages the integration of information from all sensors and making it available, as required, wherever required, to the authorised recipients.

Advancements in Information Technology

Armed forces are going through a transformation due to advancements in Information Technology (IT) in a network-centric enterprise. Though the concept may be relatively new and still developing, many commercial organisations have achieved considerable success by tapping their potential. For example, Wal-Mart, originally had a central purchasing department. But when the decision was made to share information directly with suppliers, instead of a central organisation, the need for this part of the organisation went away. Costs were reduced and performance increased. This shift to point-of-sale scanners to track weekly store sales enabled it to price goods at less than the prevailing rates.

The growing importance of IT in warfare will also change the way intelligence agencies support conventional conflicts.

By providing information directly to suppliers, Wal-Mart eliminated the platform-centric purchasing department at each store, thus, reducing operating costs and improving control over its stock. Sharing information to reduce its sales cost below the industry average enabled Wal-Mart to exploit its already dominant position in the retail sector.

This has been made possible because IT is undergoing a fundamental shift from platform-centric computing to network-centric computing. The significant investment the IT sector makes in Research and Development (R&D) and product development (in some cases up to 18 per cent of sales) has led to key technologies that have created the conditions for the emergence of network-centric computing. This shift is most obvious in the explosive growth of the internet, intranets, and extranets and the development of Transmission Control Protocol/Internet Protocol (TCP/IP)[7], Hypertext Transfer Protocol (HTTP)[8], Hypertext Mark-up Language (HTML)[9], Web browsers (such as Netscape Navigator, and Microsoft's Internet Explorer), search engines, etc. These technologies, combined with high-volume, high-speed data access (enabled by the low-cost laser) and technologies for high-speed data networking (hubs and routers) have led to the emergence of network-centric computing. Information "content" now can be created, distributed, and easily exploited across the extremely heterogeneous global computing environment ideal for business and being adapted to suit the requirements of the defence forces.

The growing importance of IT in warfare will also change the way intelligence agencies support conventional conflicts. New technology will collect real-time

7. TCP provides reliable, ordered delivery of a stream of bytes from one programme on one computer to another programme on another computer. IP handles lower-level transmissions from computer to computer as a message makes its way across the internet.

8. HTTP is an application-level protocol for distributed, collaborative, hypermedia information systems. Its use for retrieving inter-linked resources led to the establishment of the World Wide Web.

9. HTML is the software which allows one to move around the web by clicking special text called hyperlinks identified by mark-up tags.

intelligence for fast changing tactical engagements, but the communications systems available at present are far too slow for disseminating these high-tech indications and warnings. Faster means of delivering—and protecting—raw collection are being devised, so that real-time intelligence can be sent directly to shooters without detouring through multiple echelons of military intelligence analysts. Super-high-speed free-space laser communications links will be the technological cornerstone of future military satellite communications.

Compressing the Time Factor in the OODA Loop

The Observation, Orientation, Decision and Action (OODA) loop identified during the 1970s by US Air Force strategist John Boyd, is an abstraction which describes the sequence of events which must take place in any military engagement. The opponent must be observed to gather information, the attacker must orient himself to the situation or context, then decide and act accordingly. The OODA loop is fundamental to all military operations, from strategic down to individual combat and has been an inevitable part of reality since the first tribal wars centuries ago, as it is fundamental to any predator-prey interaction in the biological world.

At a practical level, what confers a key advantage is the ability to stay ahead of the opponent and dictate the tempo of engagement to maintain the opposition off balance. The quest to reduce timelines has been central to war-fighting which entails operating inside the OODA loop. In effect, the attacker forces his opponent into a reactive posture and denies him the opportunity to drive the engagement to an advantage. The impact of reduction in timelines for tactical purposes fully emerged in Operation Iraqi Freedom (OIF) during the unsuccessful but audacious attempt on April 7, 2003, to decapitate the Iraqi leadership. The strike was especially noteworthy for the way it saw information on the whereabouts of the Iraqi dictator, which emerged at very short notice, transmitted rapidly to Allied air planners and then to the B-1B. "We confirmed the co-ordinates and then it took about 12 minutes to fly to the target and release the weapons," said Lt Col Frank Swan, the weapons systems officer on the aircraft. The crew had previously been tasked with attacking

Throughout history, military leaders have recognised the key role of information as a contributor to victory on the battlefield.

an airfield in western Iraq.[10] It is noteworthy that the OODA loop which took 3-4 days during Operation Desert Storm, was reduced to just 45 minutes during OIF. In effect, the player with the faster OODA loop, all else being equal, will defeat the opponent with the slower OODA loop by blocking or preempting any move the opponent with the slower decision cycle attempts to make.

Information Superiority

Throughout history, military leaders have recognised the key role of information as a contributor to victory on the battlefield. Commanders have always sought—and sometimes gained—decisive information advantage over their adversaries. The writings of both Sun Tzu and Clausewitz reflect the key role of information in warfare.

While network-centric operational concepts are being adopted and applied by different nations, the evolving concepts are underpinned on the understanding that information will play a critical role in increasing the military effectiveness. Technological advances in recent years have vastly increased the capability to collect, process, disseminate, and utilise information. Airborne and space-based sensors are, for example, capable of providing real-time pictures of increasing dimensionality (hyper spectral) and resolution. Perhaps the most significant advances have come in the technologies related to the distribution of information. The ability to broadcast information, distribute it to a large audience, or to deliver it in a more focussed manner (narrowcast), even to individuals on the move, has dramatically increased. The sharing of information across an organisation and its partners affects and influences all aspects of an operation.

The key factor in warfare that will prove decisive is the ability to acquire and move information rapidly and deny the enemy the ability to do the same, or at

10. "What Went Right"?, *Jane's Defence Weekly*, April 30, 2003. http://www.oft.osd.mil/library/library_files/article_63_Jane.doc.

the same pace. Information processing will become central to the outcome of future battle scenarios. While information has always played a major role in any past conflict, establishing information superiority/dominance over the enemy will become a major focus of the operational art in the future. Information systems will be required to collect data in a form that is directly interpretable and useable by the shooter because one of the key elements of this information dominance will be sensor-to-shooter fusion. Conventional tactics effectively used in conjunction with information gathering assets and high speed networks will be crucial to victory in future conflicts.

The key factor in warfare that will prove decisive is the ability to acquire and move information rapidly and deny the enemy the ability to do the same, or at the same pace.

C4ISR

Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) is the domain where information gathered is converted to actionable knowledge. This forms the central nervous system of a defence organisation. The key technologies in information age warfare are remote-sensing, communications and computer technologies. One of the main steps and something many nations are now trying to implement, in becoming an efficient military at waging warfare is bringing all elements of C4ISR and weapon systems into a common actionable network. The trend started with the US operations in Afghanistan when the predator UAV armed with Hellfire missiles controlled by operators in Nellis Air Force Base in California were able to identify, track and shoot the vehicle carrying Al Qaida operatives in Yemen on November 3, 2002.[11]

The military's ability to move data from the reconnaissance platform to the weapon system able to take action, the so-called sensor-to-shooter sequence, generally required at least 80 hours in Operation Desert Storm, as imagery

11. Chelsea Emery, "Unmanned-Flight Technology Takes Off," Reuters. http://www.usatoday.com/tech/news/techinnovations/2003-11-17-drone-flight_x.htm

from a satellite or reconnaissance aircraft had to be analysed, identified as a target, turned into hard-copy, and intensively studied by the aircrew before a weapon could be dropped accurately. In Operation Enduring Freedom, the personnel of land-based Special Operations Forces (SOF) identified a Taliban troop concentration, relayed the target coordinates to the Combined Air Operations Centre in Saudi Arabia and received permission to call in an air strike. Before calling the strike, the exact coordinates of the enemy were again determined using the Global Positioning System (GPS), and the coordinates were transmitted to a loitering B-52 bomber which again used GPS to guide bombs onto the target. The whole operation was completed in less than 20 minutes of the original identification of the target. Similarly, Predator UAVs have been able to transmit live video pictures to waiting AC-130 gun ships, which were able to attack moving targets.[12] These operations taking place at short notice, against time critical targets illustrate the importance of amalgamation of C4ISR assets. This is particularly relevant in today's context where non-state actors present dispersed and fleeting targets. Technologically, the challenges are in integrating present day platforms to provide one coherent picture of the battlespace, reducing the need for operator intervention between systems of basic technical data.

Reach and Richness

Historically, one was forced to choose between a rich information exchange with very limited reach (e.g. face-to-face discussion aided by graphics, maps, etc) or a restricted information exchange that had a wider reach (e.g., memos, dispatch). This choice was forced because in the past the economics of information dictated an inverse relationship or a trade-off between the richness of the information that could be exchanged and the number of individuals it could be exchanged with. As the state-of-the-art in information technology advanced, military communications progressed from runners to smoke signals and signal flags to telegraph to radio to telephone to video

12. David A. Fulghum, "Intel Emerging as Key Weapon in Afghanistan," *Aviation Week &Space Technology*, March 11, 2002, p. 24.

teleconferencing to a fully functioning collaborative work environment. The explosion of information and communications technologies has dramatically altered the richness and reach of information. The key variables are the state-of-the-art IT and its underlying economics. As individuals and organisations have become better able to extend their reach, they have begun to focus on the quality of reach as well as the quantitative aspects of reach. It has only been within the last decade or so that individuals and organisations have been able to provide high quality information to those who need it and in the manner they need it.

The quality of reach and richness was clearly evident in the video Teleconferencing (VTC) between Gen Wesley K Clark, Supreme Allied Commander Europe (SACEUR) and North Atlantic Treaty Organisation (NATO) leaders from 19 counties during the Kosovo conflict. They would collectively view the results of the previous day's bombings over a secure transmission environment and go over the plans for the coming day. The meeting seemed like a normal one except that the participants were hundreds of kilometres apart. [13]

Common Operating Picture

A Common Operational Picture (COP) is a single identical display of relevant (operational) information (e.g. position of own troops and enemy troops, position and status of important infrastructure such as bridges, roads, etc.) shared by more than one command. A COP facilitates collaborative planning of operations and assists all echelons to visualise the development of threats by integrating pictures from all information gathering sensors. It facilitates commanders at lower formations to act without intervention from the 'top'. This has the effect of making operations smoother, faster and less confusing. This is analogous to a pride of lions attacking their prey. Each member operates in a manner to augment the actions of the other, in effect making the result superior to the sum of the different parts.

13. Micheal Ignatiff, *Virtual War* (New York: Metropolitan Books Henry, Holt and Co, 2000), p. 102

The real significance of NCW is the value addition it provides to the required range of participants engaged in prosecuting a mission.

With timelines in the conduct of war getting compressed, it has become necessary to speed up the pace of conflict to put the adversary at a disadvantage. The aim is to provide a high level of situational awareness collaboration, and a shared common mechanism, leading to greater efficiency and speed. A COP enables its users to receive and transmit near real-time situational updates to all systems connected to the shared network, thus, maintaining operational relevance in a push- pull fashion across the network. It also enables commanders to share critical information in a secure, distributed data network, reinforced by commonly understood procedures, training and policy.

Value Addition

The real significance of NCW is the value addition it provides to the required range of participants engaged in prosecuting a mission. Military operations in support of Operation Enduring Freedom highlighted the emergence of near-real-time information sharing as a source of war-fighting advantage. The source of power was not new platforms, but rather the networking of the legacy platforms with SOF. The extent to which ground-based SOF were able to share precision information with AWACS and attack aircraft was unmatched in military operations. It represented an order of magnitude increase in value addition in terms of information sharing over what had been previously demonstrated anywhere in the world in combat operations.

In air-to-air combat, a major contributor to enhanced survivability and lethality is an increase in shared situational awareness and enhanced situational understanding. With audio-only communications, pilots and controllers must share information generated by onboard sensors about opposing forces as well as their own position and status via voice. Communicating the minimum essential information required to take offensive or defensive actions takes time, and the resulting situational awareness can often differ significantly

from reality. In contrast, when data links are employed on fighter aircraft, digital information on friendly and opposing forces is shared instantaneously, adding value, and enabling all participants to share a common tactical picture. This improved information position constitutes a significant information advantage vis-à-vis an adversary fighting with voice-only communications. This information advantage, in turn, enables a cognitive advantage in the form of dramatically increased shared situational awareness and enhanced situational understanding. The result is that pilots flying data link-equipped aircraft can achieve much higher levels of shared situational awareness and understanding on a timeline previously unachievable with voice-only communications. They can translate these advantages into increased survivability and lethality.

THE GREY AREAS

Net-centricity has shown great promise but is still in its infancy. NCW is not a panacea, nor can it ever be. It has a number of limitations, and the intention here is to view these broadly and leave the analysis under a magnifying lens for later.

Cyber Space: The New Frontier

The attack on Estonia's paperless government was the most publicised event in the recent past. The borders were quiet, there were no incursions or air space violations but Estonia was still under attack; banks were under siege, communications were down and government machinery was unable to function properly. This was because the country was attacked by botnets[14] through its least protected border – the internet. The salient aspect of these

14. A botnet or robot network is a group of computers running a computer application controlled and manipulated only by the owner or the software source. Generally, botnets are a group of computers infected with th e malicious kind of robot software, the bots, which present a security threat to the computer owner. Once the robot software has been successfully installed in a computer, this computer becomes a zombie or a drone, unable to resist the commands of the bot commander. The owners of the zombie computers usually are unaware that their computers and their computers' resources are being remotely controlled and exploited by an individual or a group of malware runners.

types of attacks is that it cannot be traced to a particular nation or computer. The intrusions into the systems are through the so-called 'back- doors'. Once infiltrated, finding the attacker is complicated because of the array of electronic screens available to mask the intruder's locations. This was the first time that a botnet threatened the national security of an entire nation. The digital invasion is new and something which most countries are trying to grapple with and find solutions to overcome the potential threat.

Queuing Up

Metcalfe's Law states that the "utility" of a network increases with the square of the number of nodes in the network: ten nodes (platforms) permit a hundred possible connections, a hundred nodes ten thousand. Unfortunately, this law is not particularly relevant to the behaviour of networked military forces. Metcalfe's Law presents a possible best case scenario for distribution of information collected by sensors on platforms in a military system. At best, it is an indicator of gains in situational awareness, assuming the data being distributed is valid, timely and relevant. The real limits to capability gains in networked systems arise from the decision-action phases of the OODA loop. Networking can accelerate operational tempo by speeding up the observation and orientation phases of Boyd's OODA loop. Unfortunately, the bounds on the capability of the 'system of systems' are imposed by the decision and, especially action, phases of the loop.

The decision phase sees a commander exploiting knowledge acquired in the observation-orientation phases, and conferring as required with his superiors and subordinates to determine the best choice of action. In the action phase, the commander must deploy his assets and effect the engagement. Both of these phases of the loop, in mathematical terms, are queuing systems. The commander must wait for others to respond, and must marshal and position assets to engage. All of these events involve one entity waiting for another, in effect queuing up.

The mathematical model which constrains such systems is Amdahl's Law, like Metcalfe's Law, a defining equation in the computer industry. The reality

Amdahl defines is simple: increasing the number of assets in the system increases the achieved work or effect at best only by the number of assets added. The actual improvement is limited by the queuing effects seen in marshalling and positioning assets to perform engagements.

The mathematical bottom line in NCW is a very simple one: networking can permit a significant improvement in operational tempo where a shortage of targeting information is the bottleneck. For example, attacking strategic and *in situ* battlefield targets like deployed armoured divisions or airfields whose targeting information is already known; networking the force will not dramatically increase the combat effect because the number of aircraft and ordnance delivered will produce the desired result. However, networking produces its greatest gains in combat during battlefield strike and close air support operations, especially against highly mobile and fleeting ground targets. In such an environment, where the opponent is continuously on the move, networking can produce spectacular gains since the bottleneck limiting force capability lies in the flow of targeting information to strike aircraft.

Overconfidence about the Effectiveness of NCW

Proponents of NCW say that shared situational awareness enables collaboration and self-synchronisation and enhances speed of command, which increases mission effectiveness. Critics, however, are concerned that dangerous assumptions are being made by military planners about how future forces will benefit from "information dominance" to such a degree that fewer soldiers will be needed, or that forces will not require as much protection because they will be able to act ahead of enemy action. They believe that the doctrine of "see first, act first" that underlies Network-Centric Operations (NCO), may be flawed because the tempo of operations may outpace the ability of forces to assess and respond. While a network may provide better access to information, usually about the activities of one's own side, that information may not be complete and may not necessarily enable an accurate understanding of the situation. For example, if NCO are intended to make wars short in duration, then inferior adversaries are likely try to draw

There is no substitute for good human judgement, as yet, and making best use of a powerful NCW apparatus requires exactly that.

forces into a protracted conflict of lower intensity, and will seek to win merely by avoiding defeat by simply denying a target for the weapon systems.

Training for Operations in a Computer Battlefield

Wars have traditionally been conducted in tangible space, but information warfare, in addition to occurring in tangible space on the ground, at sea and in the air, is conducted even more in intangible space such as in electromagnetic fields. It is not only a battlefield in which guns and bombs proliferate, but also a "computer battlefield" in sheltered laboratories and control rooms where manipulated bits and bytes can create an equal amount of chaos. One of the main steps and something many nations are now trying to implement in becoming an efficient military at waging information warfare, is bringing all branches of the military into an information network. One must not forget that electronic war is conducted by the people against the people. The combat personnel are not only the warriors who charge enemy lines for face-to-face struggles, but sometimes are the operating technical personnel who sit in front of computers and instruments where vital information and real-time communication is shared. They stand at the first line in electronic warfare and in the resistance against C4I systems. Combat personnel must, therefore, be familiar with the technical and operational aspects of the weapons and equipment in their hands and must be very well trained in their operation. They must be able to understand accurately the combat plan and resolutely and flexibly utilise weapons and equipment to wipe out the enemy. To successfully absorb NCW into a defence force, it is vital that personnel not only have appropriate practical skills, but also a proper understanding of the limitations of the machinery. There is no substitute for good human judgement, as yet, and making best use of a powerful NCW apparatus requires exactly that.

Seamless Connectivity

Provision of digital seamless connectivity between combat platforms is a major technical challenge which cannot be understated. While civilian networking of computers can largely rely on cabled links, be they copper or optical fibres, with wireless connectivity as an adjunct, in a military environment centred on moving platforms and field deployed bases, wireless connectivity is the central means of carrying information and the area is most vulnerable to interference.

The fact that military networks and civilian networks co-mingle provides another set of vulnerabilities which must be addressed, for example, during Operation Iraqi Freedom, US and coalition forces reportedly did not execute any computer network attacks against Iraqi systems, even though comprehensive Intelligence Operations (IO) plans were prepared in advance. US officials may have rejected launching a planned cyber attack against Iraqi financial computers because Iraq's banking network is connected to the financial communications network also located in Europe. Consequently, according to Pentagon sources, an information operations attack directed at Iraq might also have brought down banks and ATM machines located in parts of Europe.[15]

Many nations are now on a 'networking spree', trying to interconnect their old and new systems on a common grid with the help of optical fibre cables, copper wires, data links *et al*. The success of NCW is dependent on the ability of these systems to communicate with each other. But since there is no standardisation of architecture, software and protocols followed, each system poses a new set of challenges which impedes or prevents the smooth transfer of information even after all efforts are made to overcome them.

Information Overload

The information age has forever changed the nature of warfare. Commanders are no longer hindered by the slow delivery of information in which to

15. Charles Smith, "US Information Warriors Wrestle with New Weapons," NewsMax.com, March 13, 2003 http://www.newsmax.com/archives/articles/2003/3/12/134712.shtml .

The proliferation of sensors in the battlefield has created what some call "data overload", where large inflows of real-time data can overwhelm users, and jeopardise the decision-making process.

make decisions that impact military operations. They are now, in fact, affected by a problem exactly opposite in nature—information/data overload. The proliferation of sensors in the battlefield has created what some call "data overload", where large inflows of real-time data can overwhelm users, and jeopardise the decision-making process. Effective engagement of a target requires location and identification of the target, which must be accurate and precise, along with other critical information such as target vulnerability (e.g. thickness of armour or fortification), speed, direction of movement, and time of sighting. Practically any one of these information pieces, if it is delayed, would only constitute bits of traffic on the electromagnetic (EM) highway. Waiting to get all the information of the target before taking a decision may actually hamper time critical decisions. The best operations picture is the enemy of the optimum one. The US Department of Defence is examining using new "data fusion" centres, which would use special software to filter out battlefield data not required by war-fighters. Also, to make sure that radio frequencies in use don't encounter interference, the US Air Force Electronic Systems Centre is working to design a universal tool which is intended to manage all radio communications traffic in tactical situations.

IS KNOWLEDGE WARFARE NEXT?

Collection, organisation and analysis of information generate knowledge. Rudimentary decision-making is already being performed by machines. Modern fuses, in cluster bomb units, for example, have basic IF, THEN, ELSE logic built in. In the case of a smart bomb, it is sufficient to know when and under what conditions to detonate. In battle, knowledge is power and is the domain of the decision-maker. In this information age, net-centricity has ensured an abundance of information. However, mere collation and

storage of information does not mean actionable intelligence. The information available should be distilled to provide the required intelligence. Considering the amount of intelligence available at present, it will be a stupendous task for operators to derive the required intelligence as it would entail coalescing information from myriad sources collected not just a few hours earlier but perhaps also spanning a few days, weeks or even months. It is possible that intelligent systems capable of doing so may be developed to derive the requisite intelligence from available information.

Right now, technology serves primarily the observation and action elements of the OODA loop. Sensors help observe targets while communications speed decisions to subordinate units or weapon systems for appropriate action. But it may not be long before technology aids begin helping commanders orient their observation tools and participate in the decision-making process and perhaps take part in the action itself. The research into artificial intelligence for the past twenty years is a step in this direction. Knowledge-based systems need to be different from the conventional ones which follow a strictly prescribed sequence of steps and operations. These systems need to be able to 'reason' and handle imprecise and fuzzy data. This, at present, is a tall order. Knowledge is represented by a set of rules and facts representing concepts and ideas. Therefore, a knowledge-based system requires an inference engine that provides reasoning and has an interface with the user. Some progress has been made in this direction for identification and prioritisation of threats, selecting and timing of counter-measures, including carrying out evasive manoeuvres – these systems, however, are still in their embryonic stage at best. But because of all the work being done on knowledge systems these days, it is quite possible that the rapid advances of information systems and information technology will give rise to a knowledge age and also to knowledge warfare. The information age won't go away, any more than the industrial age or the agrarian age has gone away. They're still important aspects to society, but they've been supplanted in importance by new conditions. Knowledge is liable to be the next revolutionary condition, but its Desert Storm-like manifestation is still a way off.

While information has always played a major role in any past conflict, establishing information dominance over the enemy will become a major focus of the operational art in the future.

CONCLUSION

The effectiveness of NCW has greatly improved over the years mainly due to development in IT. The increasing dependence on the electromagnetic spectrum can be gauged from the fact that in Operation Desert Storm a 500,000 force was supported with a 100 megabit per second (Mbit/s) of bandwidth. In OIF, about 350,000 war-fighters had more than 3,000 Mbit/s of satellite bandwidth, which is 30 times more bandwidth for a force 45 percent smaller.[16] The critical factor in warfare, that will prove decisive is the ability to acquire and move information rapidly and deny the enemy the ability to do the same, or at the same pace. Information processing will become central to the outcome of future battle scenarios. While information has always played a major role in any past conflict, establishing information dominance over the enemy will become a major focus of the operational art in the future. One of the key elements of this information dominance will be sensor-to-shooter fusion. Information systems will be required to collect data in a form that is directly interpretable and useable by the shooter. Conventional tactics effectively fused with space-based assets and high speed networks providing information superiority/dominance over the adversary will be crucial to victory in future conflicts.

The wars of tomorrow will increasingly be fought in cyberspace. Thus, intelligence services will need an increasing proportion of tech-savvy talent to track, target and defend against adversaries' IT capabilities. Cyber wars will be played out on landscapes of commercial IT; intelligence agencies will need new alliances with the private sector, akin to existing relationships between nation-states and will have to confront awkward problems such as: performing intelligence preparation of cyber battlefields; assessing capabilities and intentions of adversaries whose info-weapons and defences are invisible;

16. Lt. Gen. Harry D. Raduege Jr "Net-Centric Warfare Is Changing the Battlefield Environment", Defense Information Systems Agency" http://www.stsc.hill.af.mil/crosstalk/2004/01/0401

deciding whether there is any distinction between cyber defence and cyber intelligence; and determining who in the national security establishment should perform functions that straddle the offensive, defensive and intelligence missions of the uniformed Services and intelligence agencies.

Network-centric warfare between equals is akin to a chess game where situational awareness alone is not power and neither is pure knowledge by itself. The movement of pieces in anticipation of the opponent's move is more important than the power and position of the pieces. In NCW, knowing the move to make in relation to an anticipated enemy movement is the key.