AIR POWER STUDIES CENTRE

PAPER 74

Month Year

NETWORK-CENTRIC WARFARE: A PLACE IN OUR FUTURE?

By

Group Captain Peter Layton

About the Author

The ...

INTRODUCTION

Analysing a subject from a different perspective to those commonly employed can illuminate and make more comprehensible the chaotic phenomena experienced on occasion in the natural and the man-made world. Military forces are complex, complicated, societal organisations which must operate efficiently in the ultimate man-made condition of chaos: war. Considering military forces as systems, or as 'systems of systems', can offer a fresh dimension to our understanding of their operations. This approach, when entwined with the emerging network-centric warfare ideas emanating from the US, may have considerable utility in equipping us in better thinking about preparing military forces for waging armed conflict.

The French Revolution with the levee en masse, the organisational innovations adopted to make the best use from this universal conscription, and the progressive application of the technology of the Industrial Revolution to war have combined to introduce the logic of systems into the field of warfare. In the 19th century, as Shimon Naveh has recently observed: '… armies and military theoreticians found themselves in a new strategic reality governed by system dynamics'.[1] This concept has particular application to military theory in all its variants, and especially to the technologically most complex organisational creation of 20th century man: Air Forces. Modern air forces are astonishingly involved, heterogeneous, and intricate systems operating elaborate and fragile machines in an environment hostile to man, in combat against other similar machines operated by a parallel but opposed system.

Systems have been defined as a complex of interacting elements which can be considered as having three parameters:

a. the number of elements comprising the system,

b. the types of elements involved, and

c. the interaction between the elements.[2]

It is the last parameter which is the essence of a system, and makes the whole more than the sum of its parts. However, while it is the nature of the interaction between the system elements that determines the final product, this is influenced by both the number and the quality of the elements within the system. The system approach to analysing armed forces, and the key observation that element interaction is crucial, is being reinforced by recent developments in civilian information technology and the corresponding emergence of network-centric warfare ideas. The methods by which military force elements interact in the modern battlespace are being transformed by contemporary information technology.

Information technology is the centre-piece of the modern era, the determining feature of the Tofflers' so-called 'third wave' of human civilisation. Information technology

[1] Naveh, Shimon, *In Pursuit of Military Excellence: The Evolution of Operational Theory*, Frank Cass, London, 1997, p xiv. A dense book of complex ideas, this is one of the most important studies on operational level warfare in the past decade.

[2] von Bertalanffy, L., *General System Theory*, New York, 1975, pp 31-51.

is itself now undergoing a fundamental shift from platform-centric computing to network-centric computing. Significant research and development investment in the civil information technology sector has led to key technologies that have created the conditions for the emergence of network-centric computing.[3] The network is becoming the computer; with sufficient communication, engineers can now create any computer network topology they want, allowing a redefinition of the optimal computing architectures.[4] This shift is most obvious in the explosive growth of the Internet, intranets, and extranets.[5]

Network-centric computing operations are characterised by information-intensive interactions between large numbers of heterogeneous computational nodes on the network. Whether these interactions are focused on commerce, education, or military operations, there is 'value' that is derived from the content, quality and timeliness of information moving between nodes on the network.[6] This value increases as information moves toward 100 per cent relevant content, 100 per cent accuracy, and zero time delay - towards that elusive goal of knowledge dominance.

Applying Information Technology

The US Armed Forces have seized upon these developments in civilian information technology. In the US Joint Vision 2010, the emerging operational concepts are characterised as 'Network-Centric,' and the conception of future warfare described as 'Network-Centric Warfare'; US Joint Staff's papers assert 'the primary mechanism for generating increased combat power in 2010 will be networks of sensors, command and control, and shooters'.[7] While an understanding of developments in Australia's major ally is adequate reason to seek an understanding of the notion, network-centric warfare is as much a concept as an item of hardware. This system-based concept is useful for any size of force when preparing for, and waging, armed conflict. Indeed, in leveraging off commercial information technology developments, network-centric concepts may be particularly useful for those forces without a large budget.[8]

Network-centric warfare is a derivative of civilian network-centric computing, whose principles have been derived by observing successful businesses and their commercial experiences. Network-centric computing is being exploited by companies to provide a

[3] Internet users will recognise transmission control protocol/Internet protocol (TCP/IP), hypertext transfer protocol (HTTP), hypertext markup language (HTML), Web browsers (such as Netscape Navigator, and Microsoft's Internet Explorer), search engines, and JavaTM Computing. 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. Gilder, George, 'Metcalfe's Law and Legacy', *Forbes ASAP*, 13 September 1993. Article access index in http://www.seas.upenn.edu/~gaj1/ggindex.html.

[4] Gilder, George, 'The Bandwidth Tidal Wave', *Forbes ASAP*, 5 December 1994, Article access index in http://www.seas.upenn.edu/~gaj1/ggindex.html.

[5] Cortese, Amy, 'Here Comes the Intranet', *Business Week*, 12 February 1996, pp 76-84.

[6] 'Technology and the Electronic Company', *IEEE Spectrum*, February 1997.

[7] 'The Emerging Joint Strategy for Information Superiority,' Joint Staff J-6, Information briefing at http://www.dtic.mil/jcs/j6/education/warfare.html.

[8] An important part of network-centric warfare is Commercial Off-The-Shelf computers. The Intel family of CPUs we all now use cost some US$20bn to develop, that is about the same as the USAF's Northrop B-2 Spirit. If the RAAF cannot rationally aspire to operate the B-2, the Service's personnel can at least leverage off a product of a similar development budget (the Intel CPUs) to wage war more effectively and efficiently.

competitive edge in the commercial business sector; and in a similar manner, network-centric warfare seeks to attain an edge in warfare.[9]

Wal-Mart and Deutsche Morgan Grenfell are two firms that have made the shift to network-centric operations and gained significant competitive advantages by co-evolving their organisations and processes to exploit modern information technology. The characteristics of these 'big winners' is that they employ network-centric operational architectures that consist of a high-powered information backplane (or information grid), a sensor grid, and a transaction (or engagement) grid. The grids are supported by value-adding command-and-control processes, many of which are automated to achieve the necessary swiftness. These architectures provide the ability to generate and sustain very high levels of competitive space awareness, which is then translated into competitive advantage.[10] In the language of airmen rather than MBAs, the grid architecture gives excellent situational awareness which translates into more kills, and a longer life for friendly forces.

Information Grid[11]

The entry fee for network-centric warfare is a high performance information grid; it is the keystone of secure network-centric computing. The information grid is the fundamental building block which provides the infrastructure for receiving, processing, transporting, storing, and protecting information. The information grid is a 'network of networks' consisting of communications paths ('links' or 'pipes'), computational nodes, operating systems, and information management applications which enable network-centric computing and communications across the battlespace. The information grid can consist of both military and commercial communication capabilities and transmit multiple information types in multiple modes at multiple data rates. Voice, data, and video can be transmitted via point-to-point or direct broadcast.

A key requirement for an information grid is information protection; the grid must have embedded capabilities for Information Assurance to prevent intrusive attack and assure commanders that the information being presented is genuine. The combination of these capabilities enables the information grid to provide the warfighter with assured high speed access to the true information required to dominate across the tactical, operational and strategic levels of conflict.[12]

Sensor Grid

Sensor grids are composed of air, sea, ground, space and cyberspace based sensors. The elements compromising the sensor grids can include dedicated sensors, sensors based on weapons platforms, and sensors employed by individual soldiers, as well as

[9] Cerbrowksi, VADM A.K., USN, and J.J.Garstka, *Network-Centric Warfare: Its Origin and Future*, USNI Proceedings, January 1998, see http://www.usni.org/Proceedings/Articles98/PROcebrowski.htm. This is a seminal work on Network-Centric Warfare.

[10] Cerbrowksi and Garstka, *Network Centric Warfare*.

[11] Much of the following on the information, sensor and engagement grids is derived VADM Cerbrowksi's and John Garstka's *Network-Centric Warfare: Its Origin and Future*; the US J6 Joint Staff paper 'The Emerging Joint Strategy for Information Superiority', and a Network Centric Warfare Conference, presented by Charles Saffell, Rear Admiral, USN (Retired) and John Garstka, Joint Staff/ Directorate for C4 Systems, London, December 1998.

[12] 'The Emerging Joint Strategy for Information Superiority'.

embedded logistic support sensors. The information from the sensor grid is distributed across a force through the connectivity and computing capabilities of the information grid.

Ideally, the networked sensors create engagement quality awareness. This means that the time delays in passing track information to the platform firing the weapon (the 'shooter') must be short enough to allow accurate weapons engagement. Against relocatable land targets, delays of an hour or more may be acceptable if the target will not move in that period. Against naval vessels, lags of some minutes may be permissible as in this time a ship may not have moved outside the search radius of the seeker of a guided weapon (eg. an anti-ship missile) fired by the shooter using the target positional data passed from the sensor grid through the information grid to the shooter. However, for successfully engaging fast jet combat aircraft, time lags through the grids will probably need to be less than a quarter of a second, as aircraft very rapidly leave the small area an air-to-air missile searches after firing.

Abstractly, sensor grids can be viewed as a sets of 'sensor peripherals' (the actual sensor devices) with 'sensor applications' installed on the information grid to enable universal sensor recruitment, multi-mode sensor tasking and data fusion. Sensor grids can be persistent or transient. For example, a transient 'mission specific' sensor grid optimised to support the Suppression of Enemy Air Defences (SEAD) task while a strike package is within hostile airspace will have different elements than a sensor grid optimised to perform a long duration, air defence task.

Ideally, the operational architecture of a sensor grid could enable subsets of grid sensors to be dynamically tasked to support specific 'shooter' missions. The communications grid could dynamically match the optimum sensors to the most suitably positioned and equipped shooter. The size, composition and complexity of the sensor grid required to support a specific mission is a function of the level of battlespace awareness required to prosecute the mission. The number and types of sensors required to support a specific mission in a sector of the battlespace will increase or decrease as a function of the size and terrain of the battlespace, as well as the disposition of friendly and enemy forces in the battlespace. A few wide area sensors may suffice for sea surveillance over a large area, but in an urban environment a large number of local area sensors will be needed.

Engagement Grid

Air, sea, ground, space, and cyberspace based 'shooters' form the engagement grid. When cued by the sensor grid information distributed by the communications grid, the engagement grid can apply effects at precise places and times. As with the sensor grids, the engagement grids can be envisioned as a set of 'shooter peripherals' with 'shooter applications' installed on the information grid. These 'shooter applications' consist of software for command and control, and for weapon employment.[13] As with sensor grids, engagement grids could be persistent or transient. For SEAD support of a strike package operating inside hostile airspace for an hour, only a transient grid able to engage targets when they threatened friendly assets may be necessary.

[13] Cerbrowksi and Garstka, *Network Centric Warfare.*

However, for long term air defence of a critical high value asset a persistent grid may be essential to allow engagement continuously day or night for a protracted period.

The combination of the grids allows the massing of effects from sea, land, air and cyberspace shooters to give better depth of fire, faster reaction times, increased lethality and a higher probability of kill.[14] The networked sensors can allow the shooters to have a common operational picture allowing the networked shooters to undertake cooperative engagements.[15] The correct target can be engaged, at the right place, with the minimum effort and minimum risk to friendly forces.

Command Grid

Applying the US network-centric warfare concepts, a modern military joint force can be considered as a system composed of a communications grid, a sensor grid and an engagement grid. However, the term communications grid is potentially misleading, as it includes by implication the command functions. From a conceptual viewpoint it may be preferable to include a fourth ‘command’ grid.

The command grid would principally be the province of human decision makers but could include knowledge based, artificial intelligence, software applications that acted as command advisers able to recommend courses of actions. Including a command grid would allow the useful Boyd’s loop of Observe, Orient, Decide, Act (OODA) to be incorporated as functions alongside the virtual, electronic, grids. The sensor grid would observe, the communications grid (which includes data fusion and dissemination) would orient, the command grid would decide and the engagement grid would act. To achieve a mission, the grids must interact and exchange information.

The girds are inherently virtual and can be standing, or created on order, to meet the command and combat situation as required. Even from an established grid system,

[14] Undertaking SEAD tasks with network-centric warfare concepts can give increased combat power compared to platform-centric methods. The High-speed Anti-Radiation Missile (HARM) is used to suppress or destroy enemy Surface-to-Air Missile (SAM) sites. With platform-centric operations, few kills are achieved; the HARM will suppress the SAM sites and sharply reduce friendly aircraft loss rates as has been operationally demonstrated many times. However, this is because SAM site operators adjust their behaviour; the sites will stay through the duration of the war and consequently, aircraft must carry HARMs throughout the entire campaign. Through co-evolution of networked systems, organisation and doctrine, better battlespace awareness and force utilisation is gained, as every time a SAM radar transmits the network can locate and match a shooter to the target almost instantaneously; with all shooters part of an engagement grid, almost all sites can be destroyed in a short time period. This operational architecture integrates a mission specific sensor grid and a mission specific engagement grid to enable precision engagement of SAM targets even after the SAM radar has ceased transmitting. ‘The Emerging Joint Strategy for Information Superiority’.

[15] The US Navy’s Cooperative Engagement Capability (CEC) employs network-centric concepts to increase combat power. Traditionally, each ship’s radar would build incoming missile tracks independently, on the basis of what it saw. The CEC architecture increases combat power by networking the sensors, command and control, and shooters of a Battle Group’s platforms to develop a sensor grid and an engagement grid. The mission specific sensor grid embedded in CEC generates a high level of battlespace awareness by fusing data from the multiple sensors to create a consolidated high accuracy track unobtainable with stand alone sensors. Passing this track to all ships in the Group permits each ship to engage a target on the basis of what other ships see, thus extending the battlespace and the engagement of incoming targets in depth with multiple shooters with an increased probability of kill. ‘The Emerging Joint Strategy for Information Superiority’.

different quality services can be provided to meet the needs of different users. A high level commander will only need broad positional information on friendly and hostile force location, but over the whole theatre. Conversely, an air defence commander using Cooperative Engagement Capability will need near-real time, highly precise hostile aircraft track data, but only covering the small area in which the engagement is taking place.

Overall Architecture

Conceptually, the command, information, sensor, and engagement virtual grids overlay the operational theatre. The various force elements, which could range from individuals and single platforms to battle groups, would each be nodes on one of the grids able to receive, act on, or pass forward data as appropriate.

The own force nodes within any grid overlaying the non-linear battlespace would be most dense in the friendly regions, and be clustered around important assets or areas. The grid networks would extend from the rearward, friendly domains into the depths of hostile territory. Deep in the hostile domain, the nodes would be more sparse and dispersed, with connectivity back to other nodes in friendly territory a major issue. The hostile force would probably mirror image this visualisation of friendly force deployment, with hostile force elements located throughout the battlespace but clustered around areas perceived as critical centres of gravity in own force territory.

In the network-centric warfare system, modern information technology can enhance force element interaction to levels not previously experienced. Air, sea, land, space and cyber force elements can be linked and operate as a single networked system with a single operational aim. This integrated, tightly-coupled, force concept is perhaps a step beyond the current concepts of joint forces, which focus more on command issues in determining whether or not a force is joint.

Network-Centric Warfare

In this modern age of manoeuvre war that seeks to defeat an opponent’s military forces by guile and cunning rather than frontal attrition battles, friendly forces seek to operate inside an opponent’s OODA loop. To allow this, the hostile OODA loop can be degraded by friendly force attacks and be prevented from operating optimally. The efficient and timely operation of a hostile OODA loop can be thwarted by attacking an opponent’s command, communications, sensor and engagement grids by physical, electronic and psychological means.[16]

The physical and psychological means are the traditional methods of the warrior, but the electronic means of jamming and deception can now be combined with

[16] Seeking to operate within an enemy’s decision loop is a valid goal, but the real focus is on our actions once inside, not just on the blind pursuit of faster response times. The networked organisation’s great advantage is that the processing and distribution of data are sped up considerably and this should translate into increased time for commanders to analyse and contemplate the most appropriate response. The goal is not to shorten our decision-making loop, but to lengthen it, and, by doing so, improve the quality of decisions and effectiveness of friendly force actions. Otherwise, we may generate two suboptimal decisions to an opponent’s one. Barnett, Thomas P. M., ‘The Seven Deadly Sins of Network-Centric Warfare’, *USNI Proceedings*, January 1999, pp 36-39.

information warfare, cybernetic warfare and transnational infrastructure warfare. The visualisation of a miliary force as a system comprised of command, communications, sensor and engagement grids allows an appreciation of the utility, impact, and integration of the disparate and dissimilar means of attack modern technology has made possible.

Attacks can be considered as being focussed against a specific grid's vulnerable elements, or to prevent the interaction between the elements. Each grid system is a small, single system within a larger system of systems, and hence grid interaction may be a most profitable focus of attack. Taking the broad view, the aim of these physical, electronic and physiological attacks is to cause a systemic failure within the opposing military system. This systemic failure will allow us to impose our will upon the enemy; the Clausewitzian aim of war.

Waging Netwar

During combat, friendly forces must maintain the integrity of their own system while attacking the hostile system. Friendly forces must focus, not on simply destroying individual force elements in attrition style battles, but in attacking the interaction between the elements; that is disrupting the network by shock.[17] The four grid construct allows a hostile military system to be conceptually divided into constituent elements and the interactions examined to determine where force may be best applied to have the desired effect to meet the strategic goals. In different situations, different grids or parts of grids will be the preferred place for the attack to focus on; for example, if an adversary only has a few sensors but a large number of shooters then the sensor grid may be a profitable avenue of attack.

One of the first modern networked systems was the UK Air Defence system which defeated the Luftwaffe in the Battle of Britain. In retrospect, the Luftwaffe should have concentrated its attack on the RAF on the Chain Home radar stations, the system's sensors, rather than attempting to destroy the much more numerous fighter aircraft, the engagement grid, for which the radar warning information was critical. The Luftwaffe focussed on destroying platforms, rather than conceptualising the RAF air defences as a system and designing an attack to prevent the interaction between the radars and the overall system. The Luftwaffe had overlooked the need to take a systemic approach to air defence.[18]

More surprising perhaps was the RAF response to the rising attrition suffered by Bomber Command squadrons after 1941 from the steadily improving German night air defence systems. Bomber Command began to use sophisticated electronic attack methods which degraded, but did not physically threaten, radar target detection and tracking, and wireless communications; additionally the Command eventually sought to shoot night fighters down by providing escort fighters. The RAF may have found

[17] Naveh, Shimon, *In Pursuit of Military Excellence: The Evolution of Operational Theory*, p 16.

[18] This failure in thought was not perhaps surprising as the Luftwaffe took some years to realise that an integrated, networked system was essential for air warfare. The Luftwaffe in the early stages of World War II possessed individual elements: radars, fighters, communications and commanders at least as good as and in some cases better than the RAF's but did not link them into a system. See Alan Beyerchen, 'From Radio to Radar', in Williamson Murray and Alan Millet (ed.), *Military Innovation in the Interwar Period*, Cambridge University Press, 1996, pp 265-299.

physical attack of the German sensor grid, the radar sites, more useful in reducing attrition as the sensors could be easily located, were relatively few and vulnerable to air attack weapons.[19]

Indeed, there has been a gradual application of Suppression of Enemy Air Defences (SEAD) techniques over the least 50 years in an attempt to reduce losses of attacking aircraft to hostile air defence systems. SEAD concepts take a systemic approach to defeating an opposing system and use a variety of tools and methods to engage a system's command, communication, sensor and engagement grids to defeat an opponent's OODA loop.

A comparison of loss rates between those air forces using SEAD doctrines and methodologies and those who have not is illuminating. The Argentine Air Force and Naval Air Arm suffered unsustainable losses of more than ten per cent a mission while attacking ships defended by the Royal Navy's integrated air defence system; this attrition determined the war's outcome. By comparison the loss rates of the Israelis in the Bekka Valley campaign and the US forces during Desert Storm were some four orders of magnitude less.

The difference in attrition rates indicates that attention to SEAD can reduce losses to insignificance. While air defence equipments have steadily improved since World War II, the loss rates to defensive systems sustained by air forces embracing SEAD has steadily declined. SEAD may be a harbinger of 21st century network warfare concepts which seek to engage and defeat an opponent's military system, not individual platforms.

Towards the Integrated Force

Visualising war as a clash of opposing systems each comprised of four grids overcomes the boundaries imposed on concepts, operational employment and force structures by Service- or environment-centric views. Armies emerged in prehistoric times, navies during feudal times and air forces during the industrial era; in the post-modern era, though, the three are being progressively integrated under the Joint Service paradigm. The environmental framework is similarly becoming less useful as all three services seek to achieve their missions by increased use of air vehicles. Air forces can no longer be defined solely or simplistically by their use of the air. Although as a former US Deputy Assistant Secretary of Defence noted:

The integrated battlespace can provide more flexibility for all of the forces in the theatre of operations and will enhance the contribution of air power. However, the independent status airmen have historically accorded air power should disappear as integrated operations are made possible. The tighter knitting of the operational environment will demand a revisiting of air power doctrine to accommodate the possibilities available in the integrated battlespace. Air power will continue to grow as an instrument of national power, but at the same time the independence which

[19] Streetly, Martin, *Confound and Destroy: 100 Group and the Bomber Support Command*, MacDonald and Jane's, London, 1978.

characterised air power and airmen will fade in the common vision of battlespace management.[20]

The inherently different capabilities of air elements compared to surface elements allows each to bring different capabilities essential to the overall military system. In the engagement grid, the air shooter elements could make use of their speed and range of action to provide limited duration, wide area coverage, or rapid reinforcement of focal areas. Conversely, surface force shooter elements able to undertake long duration, point operations would focus on providing focal area coverage. In a similar manner, for the sensor grids, air elements could use the positional advantages from high altitude assets to provide short duration, wide area surveillance, reconnaissance and target acquisition coverage; while surface elements would provide long term, focal area coverage.

Each Service element can bring useful and unique capabilities to each of the four grids, but each capability must be able to 'plug and play' in the larger joint force arena. Plug and play applies as much to human beings as to machines.

The system approach can embrace and integrate not only the contribution of the three Services but also that of extra-Service organisations. The armed forces are making increasing use of the civilian infrastructure for support tasks as diverse as providing intelligence to repairing damaged equipment. The systems approach allows the wide diversity of civil activities that directly and indirectly form part of the defence capability to be conceptually incorporated from an own force, and a hostile force, viewpoint.

In a similar manner to the combination of the three services into a joint force, the contributions of the civilian agencies and contractors can be conceptually integrated into the appropriate grid. In so doing the importance, vulnerability and fragility of civil elements is perhaps highlighted. The contemporary emphasis on the blurring of the military-civil divide has made the civilian component relatively more important, but also more subject to attack (by any means) as part of any effort to degrade an armed force's effectiveness.

The concept of an integrated force combining and coupling a large array of disparate military elements and civil organisations is an evolution beyond joint force concepts which primarily focus on the contributions and involvement of only the three Services. The open systems concept of network-centric warfare usefully unites all battlespace participants into an integrated force able to focus on a single operational aim.

Organisational Change

In the commercial environment, co-evolution of organisational structures and processes has been the key to exploiting changes in information technology. The military can both exploit civilian information technology developments and undertake

[20] Frostic, Frederick, 'The New Calculus: The Future of Air Power in Light of Its Growing Qualitative Edge', in Hallion, Richard P., *Air Power Confronts an Unstable World*, Brassey's (UK) Ltd, 1997, pp 223-224.

military specific equipment developments, but organisational change is still necessary to gain the maximum benefits from technical changes. The formation of independent air forces is perhaps the ultimate expression of optimum technology exploitation requiring organisational restructuring.

Network-centric computing allows new types of organisations and processes with new types of relationships. There is the potential for virtual and almost instantaneous collaboration between all the individuals on a net, which could be a complete organisation spanning several continents and time-zones. Information, not people, is moved to achieve a close-knit team able to self-synchronise on the organisational aim. Moreover, everybody on the net can have access to the same information at the same time. This contrasts to hierarchical structures, where there is an inherently preferential treatment for the larger, or more senior, members so that low level subordinates or small elements always work with superseded information.

A networked organisation has the potential for enhanced speed of command and staff learning compared to more traditional structures.[21] Information can go up, down and sideways in an organisation at the speed of light, although benefiting from this requires a strong common, shared rule set, intent and doctrine amongst all the members of an organisation to be truly effective. Network concepts can allow teamworking and networking across functional lines, but require present J6 staff to move from simply providing information technology to working closely with operators who will use this to achieve strategic outcomes. In itself, this raises the question of who will provide and keep operating the various nets and grids. Previously careers were based on platforms; but now, careers may be based on net creation, maintenance and operation, making appropriate career paths and long term training requirements worthy areas of analysis.

Network-centric computing both forces, and empowers, matrix management with uncertain impacts on command during combat. In commercial experience, network-computing leads to flatter organisational structures with a broader participatory base, and an emphasis on self-managing teams created on an ad hoc basis to deal with specific problems and drawn from across the whole organisation.[22] However, the business of war is so terrible that a strong hierarchical system has developed to control and direct it. This system, owing much to Frederick the Great, may not be as appropriate to the 21st Century as it was to the 18th Century and change may be needed. Since Frederick's time communications technology has gradually made irrelevant the need for a commander to be physically at the same battlefield as his soldiers. Indeed with battlespace having replaced battlefields the whole concept of directly commanding subordinates face-to-face has been altered completely.

[21] The US Army's Force XXI automates the generation and distribution of battlefield information, orders, and related message traffic. The heart of Force XXI is called the Appliqué: a computer terminal in each vehicle which gives a constantly populated map of the battlefield and status reports on mission assignments, logistics, and environmental factors. The Appliqué and its servers are linked by a tactical Internet covering 1000-plus users per brigade over constantly shifting network topologies. In March 1997, the Army Experimental Force equipped with Appliqué exercised at the National Training Centre; its performance demonstrated that network-centric computing, compared to traditional means, can halve the time required to plan and conduct operations. http://www.ndu.edu/sa98ch15.htm

[22] Bikson, Tora, 'Organisational Trends and Electronic Media', *American Archivist,* Number 58, Winter 1994, p 51.

General Zinni commanded the 1998 *Desert Fox* operations from Florida, half a world away from his combat units, while his component commanders were spread across the Middle East. Network-computing permits such virtual headquarters and while they have vices they also have virtues, especially when a force is deficient in numbers of educated and trained staff. As the geographically dispersed, virtual management structure trend will be accelerated by network-centric warfare, there is a real need for experimentation during command post and live exercises to determine the optimum command and organisational structures.

Force Development

With a network centric approach, development plans for future forces need to embrace a system of systems approach where the focus is not on platforms, but on nodes. Instead of considering platforms as autonomous stand-alone entities, equipment and platforms should now be treated as nodes of a network. The ability to connect to the information grid now emerges as a primary source of combat power with 'plug and play' interfaces between platforms and the information grid critically important. Connectivity becomes a determinate of combat effectiveness.

This approach alters the present methodology when considering force structure development. The existing force structure thinking is platform-centric with the existing processes tailored to trading off platform A against platform B: is the Eurofighter better than an F/A-18E/F? In a network centric approach, the comparison would be between rival network concepts. System A will be played off against system B in the process of determining force structure balance of investment plans. System architectures will be the new currency in force planning.

However, in comparing the rival system options, all three parameters of a system will need to be considered; that is the number of elements, the quality of each element and the interactions between them. Traditionally, quality has been considered the critical factor in air combat success. With network warfare's systems approach, though, numbers are also important.

Network-centric computing is governed by Metcalfe's Law, which asserts that the 'power' of a network is proportional to the square of the number of nodes in the network.[23] In a basic form, this law merely captures the exponential rise in the value of any network device, such as a telephone, with the rise in the number of other such devices it can access. The 'power' of network-centric computing comes from the information-intensive interactions between the large numbers of heterogeneous computational nodes in the network. CEOs now march to the beat of Metcalfe's Law by connecting hundreds of millions of workers to local, wide area and corporate intranets.[24]

A formation of fighter aircraft can be considered as a small closed system. Applying Metcalfe's Law this four aircraft formation when networked would be potentially 16

[23] Gilder, George, 'Metcalfe's Law and Legacy', *Forbes ASAP*, 13 September 1993. Bob Metcalfe is the inventor of Ethernet, a pioneer of Arpanet and the founding father of the networking era. Article access index in http://www.seas.upenn.edu/~gaj1/ggindex.html.

[24] Beach, Gary, Publisher's Note, *CIO Magazine*, 1 April 1998, http://www.cio.com/archive/040198_publisher.html.

times more effective than a non-networked formation. The individual aircraft elements of a non-networked formation would need to be considerably more capable to be able to be as effective in combat as the networked formation. This simplistic application of Metcalfe's Law intuitively reflects current experiences where fighter formations using JTIDS networks on exercises are proving significantly more capable than non-JTIDS networked formations. Similarly, fighters and AEW&C aircraft working together as a system, even with only voice communications, are vastly more effective than fighters operating outside of an integrated system. The pilots of the Bf-109s flying escort missions against Spitfires commanded and controlled by the UK's embryonic Intergrated Air Defence System (IADS) during the Battle of Britain would have doubtlessly understood the benefits of the systems approach to air combat.

It is important though to stress that the system parameters of numbers, quality and interaction are all important; quality cannot be ignored with a focus solely on numbers and interactions. Chasing a single parameter at the expense of the others may, depending on the situation, be misguided. The key remains creating value from the emergence of the new types and kinds of relationships in a network. This value is derived from the content, quality and timeliness of information moving between the network's nodes. Thomas Barnett could be correct when he states that 'network-centric warfare's bottom line must be that no node can be worth more than the connectivity it provides'.[25]

Affordable Force Structures

The goal of superior quality has dominated Western air combat developments since World War II and allowed Western air forces to usually prevail against less sophisticated opponents.[26] However, superior quality has come at a steadily accelerating price tag; aircraft costs have been rising at five to ten per cent annually. The next generation of Western air combat aircraft, exemplified by the F-22, F/A-18E/F, Rafale and Eurofighter, are reaching the limits of affordability for most nations.

The impact of rising costs is to force down the numbers of aircraft being acquired to replace the existing aircraft. From a systems perspective, the quality of the new aircraft must be sharply more than the aircraft replaced to compensate for the decline in numbers. Both quality and numbers are important. Arguably, only the F-22 is such a remarkable advance to compensate for one F-22 replacing two F-15 aircraft in the USAF, although regardless of superior performance a single aircraft can only be in one place at one time. The numerically small but advanced Me-262 fleet was overwhelmed by the large numbers of technically inferior P-51 and P-47 fighters.

Network-centric warfare has the potential to provide a system incorporating lower cost, less sophisticated aircraft which is more effective than one emphasising small numbers of highly sophisticated aircraft. However, system design needs to be carefully considered to achieve the most cost-effective result. Depending on the

[25] Barnett, 'The Seven Deadly Sins of Network-Centric Warfare'.

[26] The major exception was the USAF's and USN's problems handling the North Vietnamese IADS which were not solved until the systems approach, that is SEAD, was adopted.

system architecture, the high cost of a sophisticated fighter aircraft fleet option may simply only be spread across a larger number of less advanced equipments; the system cost could as a whole be the same or higher than the platform-centric approach.

Cost attribution in a network architecture system can be difficult, as defining where an open system starts or finishes is inherently difficult. It is a truism that everybody wants to use the information grid but no one wants to pay for it or to have the costs associated solely with their program. Moreover, with a system approach the desired operational effectiveness cannot be obtained without the whole system; if some elements are not acquired the system may be completely ineffective in some situations.

The network-centric approach can also improve affordability by allowing sharing of information amongst the various elements of a system. In the current generation of aircraft, each aircraft carries a suite of complex avionics equipment. Each current aircraft is an autonomous system with internal command, communications, sensor and engagement grids. By expanding the network on an aircraft to include off-board elements each individual aircraft need not all carry a full suite of avionics.

Avionics typically constitute some 50 per cent of the cost of a modern combat aircraft so there are significant costs involved in carrying individual avionics suites on each aircraft. If avionics can be carried on only some aircraft and shared across a networked formation, the overall cost of a formation could be sharply reduced. Extending the concept, if the information that avionics traditionally provide can be data-linked over long distances to the aircraft the sources of the information could be quite remote, or even surface or space-based. This concept means that aircraft may not be able to operate autonomously in some situations, but this situation is already apparent under the platform-centric approach where air combat aircraft are vastly more effective when supported by aircraft such as AEW&C.

The systems approach of the network centric warfare concept may be essential to allow the air forces of smaller nations to remain in the air combat business, for at least the next generation of fighter aircraft. Without it, nations which cannot afford to maintain effective air combat forces may need to embrace asymmetric strategies, accept defeat in circumstances where a hostile nation can employ or threaten to employ effective airpower, retreat from high technology participation in an alliance, or focus on providing manpower not capital intensive armed forces. However, the network-centric warfare concept is complex and sophisticated, and is not easy to implement; there is no such thing as ‘turnkey’ netwar.

Problems with Netwars

Like all things in life there are problems and deficiencies in network-centric warfare. Inherent in network warfare is the potential for compromise - the more data you share, the greater the chance of compromise. To be a full part of the net means revealing your location in some way; it may be wise not to do everything in the ‘open’. There may be some virtues in keeping some elements from the net, and retaining tight hierarchical control of certain critical need-to-know elements. Every cola has an ‘uncola.’ The uncola of Metcalfe’s Law is Beach’s Law of Vulnerability: the number

(N) of devices an organisation has connected via nets results in (N squared) the risk of having data corrupted. [27]

There is inherent in network-centric warfare the need to accept the electronic representation of battlespace given by the communication grid as reliable. Thomas Barnett makes a telling point when he remarks that:

> I am concerned that [network centric warfare] will drive all participants to an over reliance on the common operating picture as a shared reality that is neither shared nor real. That gets me to the question of the common operating picture's 'realness', for it suggests that the picture will be less a raw representation of operational reality than a command-manipulated virtual reality.[28]

The dangers of micro-management are evident in the network-centric warfare concept but may be minimised by commanders looking only two command levels down, and learning to practice information sufficiency rather than seeking information overload. Higher level commanders should always be focussing on a force's future moves and not be sidetracked by the demands of the moment to interfere with lower level subordinates' handling of current activities. However, a possible gain from network-centric warfare is that with a shared picture the command chain could avoid the need to be constantly asking questions to ascertain the activities being undertaken and results obtained. The common picture may give commanders more faith in subordinates, not less.

Coalition warfare poses particular challenges as multi-national forces will need to connect into other nation's grids at all levels. Questions of security immediately arise with concerns of unauthorised individuals or nations 'surfing' classified national-only nets. There is also the concern over accepting a common picture, to which all have contributed, as an accurate picture. If one nation's forces engage a civilian target because the information provided to the net by another country's sensors was in error, which nation will feel the weight of international opprobrium? Will nations be comfortable authorising national forces to launch weapons based on net data of uncertain origin and veracity? Future rules of engagement will need to specify whose information on the various grids can be trusted to base engagements upon; the air defence JTIDS system may force this issue sooner rather than later.

A major criticism of network-centric concepts is that they are irrelevant in the 'operations other than war' which form the majority of the crises that military forces are involved in. However, there may be considerable utility in many such scenarios, if military forces can act as 'node connectors,' (rather than 'node destroyers') to assist crisis stricken regions. The military networks can act as a Network Central for the wide array of national and multi-national agencies that respond to complex humanitarian emergencies and international crises. The military information technology power could generate the 'Observe, Orient' portion of Boyd's decision loop for the non-military organisations who ultimately will take the lead in deciding

[27] Gary Beach, Publisher's Note, CIO Magazine, 1 April 1998, http://www.cio.com/archive/040198_publisher.html

[28] Barnett, 'The Seven Deadly Sins of Network-Centric Warfare', p 39.

and acting. Network-centric systems could allow the establishment of an information umbrella in a crisis situation to boost the transparency of everyone's actions.[29]

Bandwidth Dilemmas

There is a technical issue hidden within the shift from platform-centric computing to network-centric computing. Progress in the computer industry has ridden the revelation in 1979 by Intel co-founder Gordon Moore that the density of transistors on chips, and thus the price-performance of computers, doubles every 18 months. Every seven years, the performance of CPUs increases by an order of magnitude and thus computers get continually smaller, and more capable, at a remarkable rate. However, in network-centric computing, the computer is the network and this makes communications the key. Moore's Law is no longer the driving force of progress in information technology; instead it is bandwidth.[30]

Bandwidth is communications power: the capacity of an information channel to transmit bits without error in the presence of noise. In fiber optics, in wireless communications, in new dumb switches, in digital signal processors, bandwidth will expand from five to 100 times as fast as the rise of microprocessor speeds. Bandwidth is now doubling at least every year and should continue to do so for the next 20 years, with possibilities emerging from biological engineering after that. Over a ten-year period, this means a hundredfold rise in computer power and at least a thousandfold rise in bandwidth.[31]

The most important short-term contributor to the tides of bandwidth is asynchronous transfer mode but the ultimate source of bandwidth expansion is the immense capacity of optical fiber.[32] Wireless bandwidth capacity is doubling every nine months, but fundamental limits exist which will ultimately constrain the communications bandwidth available for mobile users while fixed, or relocatable, network user nodes linked by fibre-optic cable will have no restrictions. This difference will markedly impact the design of the command, communications, sensor and engagement grids both internally and their interconnections to the other grids.

In planning and conducting network-centric operations, warfighters will need to have an insight and understanding into the bandwidth costs of their activities. The broad dictum that a video conference link costs a Headquarters 16 telephone links indicates that trade-offs will need to be made when choosing interconnections on the nets.

Commercial Influences

A major tenet of network-centric warfare is that the concept's implementation can leverage significantly off commercial products to reduce costs. Broadly, the maximum use should be made of Commercial Off-The-Shelf (COTS) hardware and software with the military only funding developments of items able to give the

[29] *ibid*. p 39.
[30] Gilder, George, 'The Bandwidth Tidal Wave', *Forbes ASAP*, 5 December 1994, Article access index in http://www.seas.upenn.edu/~gaj1/ggindex.html.
[31] Gilder, George, 'Feasting on the Giant Peach', *Forbes* ASAP, 26 August 1996. Article access index in http://www.seas.upenn.edu/~gaj1/ggindex.html.
[32] Gilder, 'The Bandwidth Tidal Wave'.

friendly force a competitive advantage in being able to use information more efficiently than by using a COTS product. There is an assumption that an adversary can also use COTS products and access civilian information resources, but with the selective development of unique software applications, the friendly force can process and act on the same information more effectively and faster.

However, the advances possible by leveraging off the rapid increases in COTS technology are all dependent on the market. Development timelines are influenced by profit opportunities and are dependent on investment cycles as constant investment is necessary to keep laws like Moore's functioning. To develop the Intel family of CPUs has required an investment of more than $20 billion.[33] Gordon Moore himself has questioned whether the pace of microchip progress can continue in the face of wafer factory costs rising toward $2 billion for a typical 'fab'. He has pronounced a new Moore's Law: The costs of a wafer fab double for each new generation of microprocessor. The technology to implement network-centric warfare is, for smaller nations at least, hostage to commercial developments.

Conclusion

There is a new fashion in thinking about armed conflict. From the US has emerged the idea of network-centric warfare enshrined in the new US Joint Vision 2010. The network-centric concept is based on the current wave in commercial information technology, but has utility beyond simply enhancing military equipment.

When combined with insights from viewing armed forces as complex systems, network-centric warfare concepts can aid in thinking about preparing and waging armed conflict. These ideas have particular importance for airmen because they can be found embedded in past air power practises, can guide force development, and could yet make the next generation of fast jet aircraft affordable. The concepts have considerable potential to re-invigorate airpower application, while simultaneously lessening the independence of air forces as the trend towards service and extra-service force integration progressively strengthens.

A military force can be considered as comprising four interconnected, grids: command; communications; sensor; and engagement. These grids can be visualised as overlaying the battlespace from the friendly rear areas to deep into hostile territory. Each grid is a system of interacting elements having three parameters: the number of elements, the types of elements, and the interaction between the elements. The last parameter is the essence of a system, and makes the whole more then the sum of its parts. Viewing military forces as a 'systems of systems' provides a unique perspective on the complex business of waging war and preparing combat forces.

[33] *ibid.*