Network Centric Warfare in the Land Environment

Dr Carlo Kopp

The process of digitising and networking the modern military is as tortuous as was the case in industry a decade ago, with added complexities arising from technological needs unique to the military. As has been observed in the industry framework, digitisation and networking can produce large gains in productivity, and the same is true for military environments; but used as a force multiplier and in force protection are areas in which the greatest gains are realized. Indeed, military commanders now look to the networked force concept as crucial to fighting in the battlespace of today and the future.

On the global stage, armies continue to lag behind air forces and navies in this domain, reflecting in many respects the unique demands and needs of land warfare. Networking in air and naval environments evolved from air defence and this is the area where it is also best developed in land warfare overseas.

Australia is grappling with the early stages of transition into a networked environment. There has been much discussion but as yet little investment, doctrine development or conceptual thought, which is bound to change over the next decade, especially as more affordable hardware becomes available and installed in ADF platforms and facilities. Hardware and supporting software represent only a part of this picture, as the paradigm is much broader and deeper. Without a sound strategic, techno-strategic and doctrinal basis, the full potential of networking cannot be exploited.

Networking and digitisation are not a panacea and in themselves cannot substitute for combat capabilities, or indeed support logistical capabilities. The idea that combat capabilities can be downsized as networking is introduced is little more than heresay. What networking does provide is the ability to use what is available with greater effectiveness - accepting that the limits to combat effect will be constrained by the platforms, troops and logistical machine feeding them.

In considering the limits of networking and digitisation, it is also important to observe that the information being distributed within a network may or may not be correct. As with all digitised systems, the computer scientists' old adage of GIGO (Garbage In Garbage Out) applies. A sensor that misidentifies a target could well result in hundreds of force elements being simultaneously told that an opponent exists where there is none, or vice-versa. Networks are not a substitute for smart heads and commonsense.

In practice, networking links are used not only to distribute targeting data, situational awareness data and command directives, but also for position reporting of moving combat elements and combat identification to other friendly forces. In an era of standoff weapons and beyond visual range targeting, the latter is a key imperative.

The introduction of networking in air force and naval orders of battle is complex but technologically straightforward, as both arms rely heavily on aerial assets that permit large line of sight coverage, facilitating medium and high-speed wireless digital connectivity. A JTIDS/MIDS terminal on an AWACS or naval helicopter can cover a footprint ranging to 200 nautical miles, depending on platform altitude. Land forces using armour and low flying helicopters do not have this coverage. Another implicit obstacle armies face in introducing networking is in their dependency on formations of small platforms and units, unlike air forces and navies delivering combat effect using dozens, or at most hundreds, of larger and more complex platforms, each equipped with power and cooling to easily accommodate networking equipment. Equipping every armoured and soft-skinned vehicle and helicopter used by an army with networking modems represents a budgetary hit well in excess of that borne by air force or naval elements.

The approach followed by air forces and navies in introducing networking capabilities is therefore not a model well suited to armies; land arms must be more structured in how they plan and introduce such a capability. Put bluntly, to achieve similar effect armies must be smarter in terms of how they introduce networking, and must plan over much longer timelines given the larger inventories to retrofit.

Reconnaissance helicopters will be early candidates for the introduction of networking equipment as their basic role falls under the ISR umbrella.

The Connectivity Problem

The biggest technological challenge land forces face in implementing a robust networked force structure lies in providing high levels of digital connectivity between units, platforms and headquarters or other command elements.

Land forces in typical operations may be scattered over areas of hundreds of nautical miles, with a need to gather intelligence, and distribute intelligence and command directives to dozens or hundreds of fighting units that may be dispersed and concentrated over hundreds of thousands of square miles of terrain. For the network to be effective, it must function without interruption, even if force elements are on the move.

Conventional VHF, UHF and microwave land communications are limited to line of sight; indeed many existing types of equipment perform little better than the link between a mobile phone and base station. The more complex the terrain the more difficult this problem becomes.

While HF radio may be used, it demands bigger antennas and often has blind spots. Putting a complex encrypted spread spectrum frequency-hopping modulation on a radio carrier wave to provide for a digital network cannot change the physics of radio transmission.

It is important to observe that all connectivity solutions in the networking game must be designed around the expectation that opponents will actively jam networks and invest effort in destroying larger and more valuable networking nodes. Networks are potentially a shared single point of failure for any digitised force, and the payoff in jamming them and destroying airborne and surface based relay nodes is very high. While contemporary network technology like JTIDS/MIDS has good jam resistance, the game in question is one of kiloWatts of jam power, antenna sizes and bandwidth to frequency-hop in. A determined opponent possessing Digital Radio Frequency Memory (DRFM) technology, now being marketed by Russian manufacturers, is in the position to severely degrade a network that is not designed from the outset to cope.

While much of the debate on the ISR element of a networked force remains focused on technological sensors, Special Forces troops connected into a network can provide a unique 'wetware' element to an ISR constellation, capable of divining information which many current sensor technologies cannot divine.

Network Centric Warfare

Armoured vehicles represent viable platforms for carrying networking relay equipment, as they are well protected, and have the power and cooling to support such systems without difficulty. The intended infantry support role of the Army's new M-1A1 ABRAMS tanks makes them a natural candidate for early introduction of networking equipment.

The US Army and US Marine Corps have relied heavily on the use of satellite terminals to provide backbone connectivity between larger formations, exploiting the large US DoD satellite communications constellation. Local hubs then connect to platforms and fighting units using digital radio links over shorter distances.

This model is an expensive one, and is ill suited for smaller defence forces without the budget to fund extensive satellite constellations, or the need to operate on the global scale. Another problem in its own right is the available capacity over a SATCOM link. There are two viable and practical technological solutions to this problem, but both are immature and will require further development investment to integrate them into force structures.

The first of these is the 'pseudo-lite' (pseudo-satellite), which is a long endurance UAV carrying a digital and voice communications relay package. A pseudo-lite can be put on station over an area of operations, and orbit for many hours providing connectivity to force components within its line of sight. If the UAV is equipped with additional antennas and relay equipment, it also offers the potential to connect to other UAVs within the line of sight, extending the network footprint.

The model is not a new one. During the Vietnam war US forces relied often on US Air Force EC-135 Combat Lightning and EC-130 airborne communications relays, which orbited areas of operation to provide wide area VHF/UHF coverage and links to central headquarters elements, although primarily for supporting air force operations. A UAV based pseudo-lite is essentially a much cheaper robotic solution to the same problem, with the potential for much greater coverage footprint if the UAV station altitude is well above 40,000 ft.

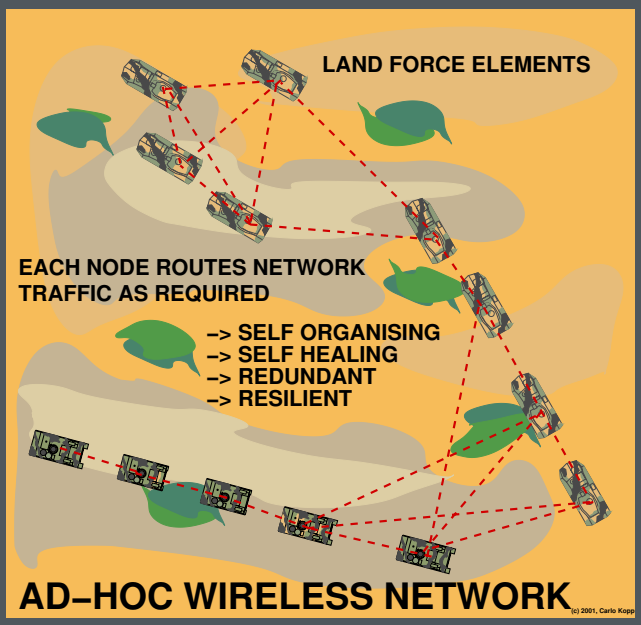
At this time there is no off-the-shelf high capability product in this category. The US have funded some initial work on the AirBorne Communications (ABC) communications payload for the RQ-4A Global Hawk, intended to provide a High Altitude Long Endurance UAV based multi-service solution, relaying digital and voice communications.

Given Australia's weakness in SATCOM capabilities, a HALE UAV based pseudo-lite solution is an attractive model, especially if a system can be produced that is capable of addressing the needs of all ADF users. Such a solution will be much cheaper and more flexible than a satellite system, but more than token numbers of UAVs will be required, making it a potentially large and expensive undertaking, that being a challenge in its own right.

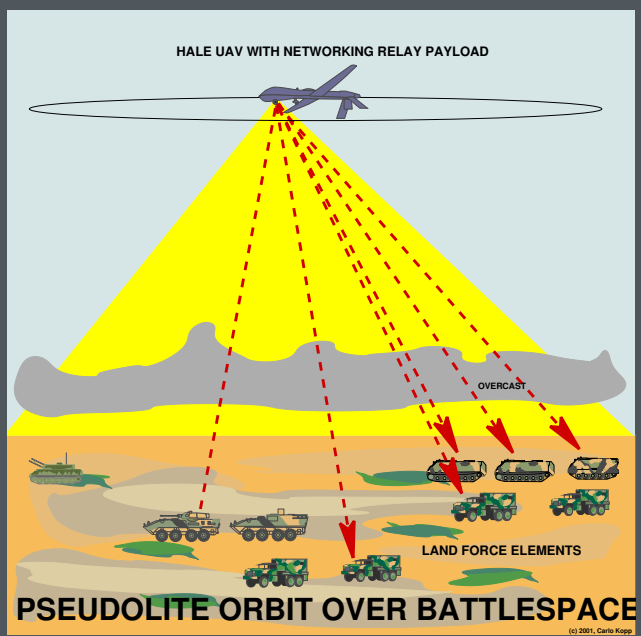
The top end solution of using a large HALE UAV with a 500 nautical mile diameter coverage footprint and half a tonne of relay equipment does not preclude the use of a much smaller single-Service capability for the Army alone. However, any such system will still demand tens of kilograms of relay equipment payload, electrical power and cooling, and hours of endurance at 20,000 ft station altitude which still puts it in the category of well sized and well priced equipment.

From a robustness and resilience perspective the pseudolite model involves inherent tradeoffs. Smaller numbers of larger and higher flying HALE UAVs are invulnerable to shorter ranging air defence weapons, but exposed to long range SAMs and top tier fighters such as the widely used Su-27/30, and with smaller numbers attrition is a major issue. Smaller and lower flying UAVs are exposed to area defence SAMs and larger guns, but deployed in larger numbers some attrition can be absorbed without a major loss in capability.

Network Centric Warfare in the Land Environment



Ad hoc wireless networks are self organising, self healing radio networks in which every station functions as a relay for its peers, as required. This technology is reaching commercial viability but has yet to be seen in a full scale military application, despite the large investment in the DARPA GLOMO program. A military wireless network would require smarter networking equipment which incorporates the ad hoc routing capability in addition to the digital radio modem used otherwise.



Pseudolites are long endurance UAVs equipped with satellite-like but shorter ranging voice and digital communications relay payloads. While they do not provide the continent scale footprint of satellites, they are very much cheaper and given the short transmission distances involved, can be used for high capacity digital links.

The second technological solution to the connectivity problem is also immature and involves the use of 'ad hoc networking' protocol technology.

Ad hoc networks are self-organising networks with no defined structure, in which every node in the network acts as a relay as required. Packets of digital data hop from node to node across the network until they arrive at their destination, exploiting the line of sight proximity between individual nodes, and creating effectively the illusion of a fixed terrestrial network. Rather than directing digital traffic to a large airborne or orbital relay, the ad hoc network diffuses the traffic across a large number of small mobile ground based relays.

The ad hoc networking model is well suited to land warfare, especially with large formations, or groups of smaller formations, as the logistical chain connecting formations provides opportunities to carry ad hoc networking equipment on vehicles. Even relatively low powered wireless nodes can exploit line of sight, often in complex terrain. If helicopters are equipped with ad hoc networking nodes, their additional coverage can add further robustness to the system.

In practical terms an ad hoc networking system would involve fitting all armoured vehicles, all helicopters, many trucks and 4WDs with digital radio modems incorporating an embedded ad hoc router software package. The cost of the technology would differ little from the cost of more conventional radio modems, as the additional functionality is mostly in embedded software which determines how and where to relay incoming packets of digital data.

Perhaps the greatest strength of the ad hoc networking model is its resilience to attrition, as the traffic flows across large numbers of small routing nodes. As the network protocols are self-organising, destruction of platforms carrying such nodes would typically see traffic transparently routed around the lost node in a matter of tens of milliseconds or seconds.

As with airborne UAV-based technology, ad hoc networks are immature and not available as yet off-the-shelf as military spec rated products. The US DoD funded a major early research effort under the GLOMO (GLObal MObility) program during the late 1990s, but few of the projects led anywhere. The US has a major investment in SATCOM technology, and more recently the aerial refuelling tanker based ROBE project, both of which provide much of the capabilities needed and both have soaked up much of the available funding. While there has been considerable research in commercial applications of ad hoc technology, these are unusable for military applications as the commercial wireless 802.11 hardware used is highly vulnerable to jamming.

As with pseudolite, ad hoc networks are a technology that is exceptionally well suited by its basic design for smaller defence forces, and specifically armies.

By the same token, neither have developed as rapidly as hoped – since the US industrial base has soaked up much of the available investment funding to produce more conventional technology optimised for US service needs.

Australia has a good expertise base in smaller UAVs, ad hoc networking and airborne digital datalinking.

However, this expertise is scattered across academia, portions of industry and specific groups in DSTO. Without robust early investment by Defence into developing this technology base into real products, the long-term outlook is that the ADF will continue to struggle with solving the connectivity problem – in a world where most off the shelf technology will be built around the US model and its unique idiosyncrasies.

Deconfiction and combat identification of ground forces is a persistent problem, accounting for often significant combat losses over the last six decades. While the public debate has focussed on recent incidents involving combat aircraft striking ground forces, the historical record shows this problem to be a feature of every larger and more complex campaign, with infantry-on-infantry, tank-on-tank, and helicopter-on-armour 'friendly fire' incidents well documented. Networking equipment can much reduce opportunities for such incidents.

NCW in the Land Environment

The ISR Problem

Networks without advanced digitised sensor systems to feed them with raw information are of limited use - the power of NCW derives largely from its ability to rapidly transmit and distribute large volumes of digitised information produced by a pool of Intelligence Surveillance and Reconnaissance (ISR) systems. Without ISR, NCW systems are blind and without NCW, the inherent speed of digitised ISR systems cannot be exploited.

In the land warfare context Australia is in a poor position when it comes to investment in ISR systems. The RAAF and RAN can both exploit the large ISR investment inherent in the JORN and Wedgetail programs, but there is no equivalent program to support land warfare oriented ISR capabilities. The long running JP129 project aims to cover these needs, but in scope, scale and impact cannot compete with the JORN and Wedgetail programs.

The US ISR constellation provides valuable lessons on what to do and what not to do. Owned and operated largely by the US Air Force, the US system is the most comprehensive and powerful in existence. It is also most inhomogeneous, and in effect is an accretion of a large number of what used to be independent programs developed over a 30-year period. While the US Air Force plans to standardise much of the technology and systems in the constellation within the next generation of the technology, especially in the MC2A program, over the next two decades the US will continue to operate a menagerie of systems, glued together by digital networks.

At the most fundamental level, a contemporary ISR constellation relies on a handful of key sensor technologies. High resolution Synthetic Aperture Radar provides all weather mapping capabilities, supplemented by Focal Plane Array imaging chips operating in the infrared and visible TV bands. Electronic Support Measures (ESM) receivers, Emitter Locating Systems (ELS) and Signals Intelligence receivers (SIGINT) are used to collect, identify and geolocate hostile radio and radar emitters. Ground Moving Target Indicator (GMTI) radars can track and often identify or classify moving targets such as vehicles, armour and rotating radar antennas.

It is important to note that technological ISR capabilities exist in parallel to 'wetware ISR capabilities'. A SAS reconnaissance team on the ground provides a unique ISR capability that can do things technological ISR cannot at this time. To generalise the model of networked ISR, we must include human observers as sensors connected to the network.

While the core technologies underpinning the ISR revolution of the 1990s are common, the apertures supporting the sensors, and the platforms carrying them, differ widely. While a surveillance UAV, fighter recce pod and internal FLIR on a fighter might all share the same type of thermal imaging array chip, the picture quality will vary enormously with the quality of optics, stabilisation of the optical platform, and operating altitude of the carrying platform.

The Australian Army faces some unique challenges in sourcing the kind of real time or near real time ISR output required to support operations on a modern battlefield. In the US architecture, the JSTARS, Rivet Joint and UAVs provide ISR output for both US Air Force battlefield interdiction and close air support operations, as they provide the same for Army and Marine Corps land operations. No such wide area capability exists for the ADF - while JP129 and DEF 224 Bunyip aim to address these needs, neither program is funded on the scale required.

In practical terms the ADF needs a two-tier architecture to provide networked ISR for Army, but also Air Force operations. The upper capability can be partly addressed by the planned HALE UAV (eg Global Hawk), but a big hole remains in planning given the absence of a long range high power SAR/GMTI surveillance and target acquisition radar program in the class of the JSTARS and its smaller EU equivalents. Mobile ground targets require high power X-band radars and there are practical limits as to what any medium sized or larger UAV can deliver. Practical options do exist: the new US MP-RTIP modular radar planned for JSTARS upgrades, MC2A, later Global Hawks and other platforms would be a suitable candidate.

In terms of platforms, a palletised package in an AP-3C weapon bay, emulating the US Navy 'Hairy Buffalo' P-3B trials, would be a viable choice, and this could be transplanted into a future AP-3C replacement. Existing proposals such as the MMSS package for the AP-3C could be adapted. However, none of this will materialise as long as there is a focus on single-Service investment agendas.

NCW
in the Land Environment

Unlike smaller navies and air forces which can equip most of their platforms with dozens of ship-sets of networking equipment and achieve full fleet coverage, armies face a major challenge in introducing fleet wide networking equipment due to the significantly greater numbers involved. Equipping the Army's ASLAV and M113 fleets would require hundreds of systems.

The lower tier of an ISR architecture could be addressed with a wide range of available UAV-based, or crewed aircraft-based systems. The market offers a diverse range of thermal imaging, optical imaging, high-resolution radar, electronic recce and signals intelligence payloads. However, as with upper tier needs, a joint service architecture must be adopted from the outset. There are important synergies between Army and Air Force needs that can be exploited but there must exist a shared understanding of what these needs are and a serious commitment to grow capabilities.

The Architectural Problem

Given a pool of sensor platforms and a collection of warfighting elements – be they equipped with wheels, tracks, rotors, wings or boots – a major issue arises in the manner in which they are networked. Is the networking architecture a hierarchical system? Is is a peer-to-peer system? Is priority accorded to networking command and headquarters elements first? Is priority accorded to networking 'shooter' elements first?

The global trend has favoured the introduction of networking to connect command elements first, and once this is addressed robustly, networking of combat elements follows.

There are good reasons for pursuing this 'top-down' approach, in particular the need for commanders to rapidly gain access to ISR data to support decision-making. Coordinating large formations and tasking components of these cannot be done in a bottom-up fashion. Accordingly, a model in which networking is introduced first at divisional level, then at brigade level, and so on is the best strategy to pursue, and one which delays the large dollar investments at a unit level, as networking equipment will continue to decline in cost over time.

The current aim in US NCW development is, however, more ambitious and involves direct and indirect 'sensor to shooter' links. This model has worked well for the US Air Force, employing primarily 'smart' guided weapons. Armies that rely to a much greater extent on 'dumb' direct and indirect fire weapons are less able to exploit this model. Nevertheless, there are important benefits in being able to directly download via network targeting coordinates into the fire control computer of a tank, attack helicopter or artillery piece. Introduction of more precision guided munitions, especially indirect fire munitions, is a necessary prerequisite to properly exploit 'sensor to shooter' link technologies.

The pursuit of a top-down model in the introduction of NCW capability in the Australian Army does not preclude early introduction of some 'sensor to shooter' capability in combat elements, but the pragmatic reality is that universal availability of 'sensor to shooter' capabilities across the Army force structure must be a long term goal rather than short term goal. Clearly 'sensor to shooter' links to tanks, light armour, attack helicopters and artillery batteries must take precedence over wearable computers and helmet mounted head-up displays for infantry. A viable model may well be to introduce 'sensor to shooter' to some elite combat formations, to develop a doctrinal and experience basis for broader usage.

A consideration in Low Intensity Conflict and similar counter-terrorist operations is the utility of networking for Special Forces elements, exploiting them as a 'wetware ISR element' but also providing them with access to remote HUMINT resources in real-time. This is a unique area where networking has considerable potential.

The issue of 'peer-to-peer' networking vs 'hierarchical' networking is less easily exposed, as the hierarchical and peer-to-peer relationships between sources and consumers of networked data can exist regardless of whether the networking technology itself is structured around a hierarchical or peer-to-peer network topology. Indeed, many networking technologies concurrently use internal mechanisms that are peer-to-peer and hierarchical in function concurrently - the Internet protocol suite being an example.

It is important that the topological structure of the networking technology is not understood to be the structure to be followed in the model used for distributing networked information. The latter must be functional, not patterned after the digital hardware used.

In summary, the Australian Army faces key challenges in providing connectivity, providing ISR capabilities and developing a robust architecture in its quest to become a networked 21st Century force. While these challenges are in many areas difficult, they are not insurmountable.