AIR POWER STUDIES CENTRE

PAPER 65

Month Year

CONTROLLING AUSTRALIA'S INFORMATION ENVIRONMENT OR DECISION SUPERIORITY AND WAR-FIGHTING

By

Air Vice-Marshal Peter Nicholson

About the Author

The ...

INTRODUCTION

Our new strategic guidance requires the most important capability development priority to be the 'knowledge edge'; that is, the effective exploitation of information technologies to allow us to use our relatively small force to maximum effectiveness. The knowledge edge is described functionally in the 1997 Strategic Review as intelligence; command arrangements and command support systems; and surveillance of our maritime approaches.[1] This is a very conventional categorisation in the light of emerging technology and operational concepts. So, the knowledge edge can be characterised in ways in which it might be applied across all levels of war and in terms of its components or elements.

The subject of 'Controlling Australia's Information Environment' will be treated in the context of the use of armed force at all levels of war, but especially at the operational level, in fighting campaigns that will be referred to as war-fighting. Specifically, this paper will examine the application of our new theatre war-fighting concepts (in essence, joint operational doctrine) to controlling our information environment.

The Getting of Wisdom

A hierarchy of data, information, knowledge and wisdom is created by successive analysis and assessment of the lower elements to add value to levels of understanding. At the lowest level, *data* is collected from sensors or other sources (for example, a radar detection of an aircraft). The next level, *information*, is produced by processing data to associate different or successive observations to enable conclusions to be made about behaviour, and perhaps predictions to be made about future behaviour (for example, successive radar detections are combined to form a track). Further analysis of information including association with other data and information provides a deeper understanding of this behaviour called *knowledge*. In the military context, knowledge enables the understanding of what is happening, where, and probably how the activity is taking place. Knowledge is the level of understanding needed to comprehend what has happened and make reasonably confident predictions about future behaviour. Following the previous examples, knowledge would be exemplified by analysis of track history, track origin, aircraft identification, flight path parameters and so forth, to deduce that an air attack was in progress and to identify the likely targets. The final level of understanding postulated is termed *wisdom* which relates to why events are taking place and enables a complete mental picture to be formed of adversary behaviour.[2]

On this hierarchical scale, the more conventional notion of *intelligence* fits somewhere between information and knowledge. The common complaint of commanders that they wish to know what is about to happen from their intelligence

[1] Department of Defence, *Australia's Strategic Policy*, Canberra, December 1997, pp 56-60.

[2] Sometimes, the idea of a hierarchy includes the conventional notion of *intelligence* as the result of analysis of information. Thus, intelligence is seen as an intermediary step between information and knowledge. See for example, Murphy, Lt Col Edward F. *et al.*, 'Information Operations: Wisdom Warfare for 2025', in *Air Force 2025 White Papers*, Volume I, Air University, Maxwell AFB, Alabama, 1996, p 3.

specialists rather than what has happened in the past underlines the reluctance of the intelligence function to predict future events. This substantiates the view that intelligence is more than information but not quite knowledge. Indeed, our conventional notion of intelligence may now be outmoded and perhaps should be discarded in favour of a term which describes the function - gaining a complete understanding of the enemy's behaviour. This is not the only conventional notion which does not fit the paradigm of warfare in the next millennium.

The tasks at the lower levels of understanding, gathering and analysing data, can be largely performed by machines. However, there is some point in the continuum between what we are calling information and knowledge where the complexity of the assessment task cannot be replicated by machines. Despite the advances in artificial intelligence, expert systems and the use of techniques such as neural networks and fuzzy logic, technology has not yet been able to replicate human reasoning. This is particularly true for the association of apparently unconnected items of information, the ability of the mind to make cognitive leaps and intuitive deductions. The consequence of this is that physical or electronic action on data or information can be used to influence the lower levels of understanding but the higher end will require influencing the assessment and evaluation process of the adversary's mind; that is, successful knowledge warfare will require attacking his decision making process.

The Utility of Knowledge

Knowledge, or even wisdom, is not an end in itself. Rather, it is how that knowledge is exploited to achieve the military objective which is important. Knowledge of the adversary and of oneself has always been important in warfare. Knowledge of the enemy is an understanding of the threat posed by him - understanding his capability, his intention and his motive. Understanding his capability is to have knowledge of his force preparedness and force structure, and in some definitions, the modernisation state of his force.[3] Knowledge of his intent introduces the predictive element, extrapolating from past behaviour to estimate what his actions are likely to be in the new situation. Understanding his motive may provide clues to why he is pursuing that course of action and enable a more indirect and subtle means to counter him. This may be the future kernel of knowledge warfare - changing the adversary's will, influencing his motive through controlling his perception of what is happening and why.

Knowledge or the lack of it exerts influence at all levels of war and across the spectrum of conflict pervading every engagement, operation, campaign and war. At the strategic level, all sources of knowledge available to the government will be used to determine which instruments of national power will be brought to bear to deal with an adversarial state or any non-state group which poses a threat to national security. Data and information will be gleaned from many sources within and external to the government covering a wide range of indicators, including economic, financial and commercial fields, as well as social, cultural and religious aspects. But ultimately, the

[3] The most encompassing description of operational capability is that propounded by former US Secretary of Defense Frank Carlucci who defines it as the combination of *readiness*, *sustainability* (which together define preparedness), *force structure* and *force modernisation*. The notion of force modernisation captures the idea of upgrading capability through incremental improvement of sub-systems throughout the life of type of the weapon system.

grand strategic decision - whether or not to engage the adversary and what combination of means available should be used, including the military instrument - will be a political decision. Political decisions are based on judgements formed from perceptions; that is, they could be loosely described as knowledge based. It may be important, even crucial, to influence or change the adversary's political decision making process, to cause a change to his grand strategy through successful knowledge warfare at the strategic level. But that is not the purpose of this dissertation which will concentrate on the operational level of war and how we could endeavour to control Australia's information environment for the purposes of successful war-fighting.

To do this, we will look at our new theatre war-fighting concepts which provide the theoretical framework for campaigns to defend Australia and its interests. The key precept of this joint operational doctrine is called *decisive manoeuvre*. Decisive manoeuvre is 'the conduct of synchronised operations … to defeat the adversary by positioning in time and space the most appropriate force to threaten or attack critical vulnerabilities, thereby unhinging the centre of gravity and obtaining maximum leverage'.[4] This can only be accomplished successfully if we adhere to several core concepts. In turn, these are enabled by four supporting concepts, the most important of which is termed *decision superiority*.

In addition to examining some of the operational concepts made possible by technological advances, such as decision superiority, it is also necessary to consider the organisational adaptation and response if we are truly to reap the rewards of a full blown Revolution in Military Affairs. The Air Force of tomorrow might look nothing like the one we know today.

Decision Superiority

Decision superiority is achieved when we can make and implement more informed and more accurate decisions at a rate faster than the adversary. For decisive manoeuvre to succeed, not only must our decision cycle be faster than the adversary's, the quality of those decisions must be superior and they must be implemented in the required time-frame. Like all other aspects of warfare, achieving decision superiority necessarily involves a close interaction with the enemy. We are concerned not only with our own, but also *his* decision making process. The objective can be accomplished if we can force him to make *bad* decisions as well as allow him to make good decisions but too slowly. This is a considerably more subtle approach than the usual adage to 'get inside the enemy's decision cycle'.

There are several discrete and to a large extent independent steps in achieving decision superiority which provide a convenient means of analysis. The process begins at the start of the knowledge cycle with the collection of data and its transformation through analysis into information which will ultimately provide battlespace awareness. Battlespace awareness requires a variety of complementary sensors which will detect, or have a high probability of detecting, events and activity through both passive and active means. Whenever the enemy emits radiation (transmits) in his efforts to gain battlespace awareness, we should be able to detect

[4] Australian Defence Force Warfare Centre, *Decisive Manoeuvre: Australian War-Fighting Concepts to Guide Campaign Planning*, Interim Edition, January 1998, pp 1-3.

that he has transmitted, localise the source of the transmission, classify the transmitter and identify it. In addition, in parallel and perhaps concurrently, we must seek to detect through active means platforms that do not transmit.

The detection capability needs to at least span the communications, data transfer and active illumination (radar) portion of the electromagnetic spectrum; that is, from the low HF (high frequency) to the K band (3 megahertz to 30 gigahertz). The physics of transmission and the curvature of the earth preclude remote, long-range detection of emissions or active illumination of targets except by high frequency ionospheric refraction. This leads us to the inevitable conclusion that the sensor must be either space-based or carried to the area of interest by another platform. While direction finding can be accomplished in most cases with only a single detection, spatially fixing the location of the emitter is a trigonometric problem which requires at least two and probably several detections, from either a moving sensor or a second sensor. Platform movement relative to the target and successive detections at intervals sufficient to provide a triangular fix, is the common technique using a single platform which has been highly refined electronically in the synthetic aperture radar. However, much greater potential is available, especially for Australia's situation, in the second method of *multi-static detection*. This exploits burgeoning information technologies associated with onboard or distributed processing and high speed, high capacity data transfer.

A fruitful area for multi-static detection techniques which has been long exploited is of course the use of acoustic sensors for underwater target detection and fixing. The usual method is to lay a sonar buoy field across the path of a submarine and by triangulation plot its track through the field. While passive detection ranges are relatively short - a few kilometres at best - active methods have the potential for detection of submarines over scores or even hundreds of kilometres. Fixed, passive arrays are useful for barrier or focal point detection tasks, but open water detection and tracking requires a mobile platform. Detection and tracking of aircraft at acoustic frequencies is also proving feasible using fixed arrays on target approaches or where intruders can be channelled by placement of surface-to-air missile systems. What we need in the future is the application of multi-static illumination and detection techniques at radio frequencies.

Australia's geographic circumstances predicate a surveillance system with enormous coverage. This immediately suggests a move to space-based sensors but economic realities deny us an independent, full coverage, sovereign capability although we must take full advantage of information obtained from our major ally, the United States. An alternative for wide area coverage is over-the-horizon radar but this does not provide the resolution for accurate tracking and is strongly dependent on ionospheric conditions which can be problematic because of diurnal, seasonal and solar effects. An operational concept which immediately seems feasible is to use the combination of a limited space-based capability and over-the-horizon radar to provide cueing for other sensor packages. Because of time and space considerations, these sensors should be mounted in aircraft in order to provide rapid response and broad area coverage. Some weapon systems to meet this requirement will enter the inventory in the next few years, notably a new generation airborne early warning and control aircraft. But there is a clear requirement for long endurance, high altitude, long range unmanned

aerial vehicles to carry sensor packages and to provide data linking with other platforms.

In determining the type and mix of sensors needed for situational awareness, it is important to note the difference between detection of an activity, and repeated observation and tracking of the event or platform. Detection is not likely to require the same degree of resolution required for tracking nor the same intensity of observation or revisit rate. So detection of an event by a less precise, wider area sensor can be used to cue the deployment of a higher accuracy, more focussed sensor for subsequent tracking.

Many features of the surveillance system required to provide battlespace situational awareness are also necessary for targeting and, increasingly, information technology will allow manipulation and control of surveillance sensors for this purpose. Clearly a very sophisticated sensor management and tasking system is a prerequisite for multiple use of the sensor suite for surveillance, reconnaissance and targeting.

Information Management

The wide variety and types of information sources available requires processes in place to synthesise incoming data to present the best possible information in an easily comprehensible fashion without overloading the commander, staff or the communications information system. However, it is most important that the technology is the means employed and does not become the ends in itself by 'automating a stubby pencil'. The decision making and battle management *process* must be designed to identify the initial information requirements, present this in a coherent manner, allow it to be evaluated to become knowledge, and permit interaction between the automated functions and the human elements. This process is well established and regularly tested in the air component and the joint theatre headquarters but it would be prudent to ensure it is constantly examined and refined.[5] We must assume that the adversary will have an equally effective process in place, so this may be a fruitful avenue for knowledge attack and would certainly represent a capability edge if accomplished.

Data and information is electronically collated, stored, manipulated and presented in a Command Support System. To be effective, this will be a distributed system in a wide area network comprising several local area networks including the theatre and component headquarters with links down to other local area networks at the Wings and Squadrons, laterally to other components, and up to the strategic level. Modern information gathering capabilities will inevitably overload both the commander and the communications system if all information is presented, so it must be managed such that only knowledge that is both timely and appropriate is presented to those who need it. This management is facilitated by a 'pull' system whereby the user seeks the information required from databases distributed over the system rather than the opposite 'push' arrangement from the sources to the user.

[5] Australian Defence Force Warfare Centre, *Joint Military Appreciation Process*, Interim Edition, January 1998.

From the earlier discussion of the point in the hierarchy of understanding where human interaction becomes the more important component, it is evident that data and information management should be automated to the greatest extent possible up to this point, and limited in quantity from this point on. Otherwise, the crucial decision making process could be swamped in a flood of incomprehensible information. An obvious area for improvement in the future is the development of automated decision support aids to reduce, by aggregation and summary, the amount of information passing to the human operatives. The likelihood is that this will be accomplished by presenting information in visual form so that it can be rapidly comprehended by the humans in the chain and intellectually 'bundled' for comparison and integration with other knowledge packages for decision making. The principle should be that humans should be able to concentrate their attention on those aspects or 'knowledge bundles' that machines are unable to digest and automate everything else to the greatest extent possible. We must not become over-reliant on the information system presenting all pertinent information. Even under extreme pressure from time, superior commanders, system degradation and adversary disruption, the commander must have the wherewithal to make decisions rapidly.

To this point, the discussion of information management addresses our own processes and is part of knowledge of oneself or own forces. But we must also consider the likelihood that the adversary will attempt to degrade our internal processes, especially the automated functions and the flow of information in electronic form, in order to reduce our knowledge of own capabilities.

Information Security and War in Cyberspace

Our Command Support System is clearly a target for attack by the adversary as are the communications links between the local area networks. While both can be physically attacked, the more dangerous threat comes from undetected intrusion of the computer system and disruption of its operation, or corruption of the data it uses. The lexicon of the techniques used are redolent of the information revolution itself - viruses, logic bombs, Trojan horses, trapdoors - and are as pervasive and dangerous in the civilian arena as the military.[6] The outcome of an information attack might simply be a massive overload of the computer and communications system, and the most worrying aspect yet to be resolved is recognition that an attack is underway. The first level of threat is simply disruption of the information system which, while destroying or rendering useless data and information, will probably be obvious, if not as an attack, at least as a system failure. The second and more subtle threat is a partial distortion of data and information which is not recognised as an attack and which leads to misunderstanding and false knowledge. This is one form of attack on the internal decision making process which if successful can lead to a situation of decision inferiority.

Computer networks designed for other than command and control functions are also vulnerable to attack. These include the computer aided aircraft maintenance management system which will eventually hold all information concerning aircraft serviceability and maintenance history, the equipment supply tracking system, the

[6] Correll, John T., 'War in Cyberspace', *Air Force Magazine*, Volume 81, Number 1, January 1998, pp 32-36.

personnel management system, and so on. Again both the separate databases and the links between them could be attacked, but corruption of the data is unlikely to significantly degrade decision making so attacking the communication system may be a more likely prospect. In any case, entry to the widely distributed network is becoming increasingly easier. The situation is likely to worsen in the future because '…current trends indicate that public telecommunications and the Internet will merge [and] many of today's networks will likely be absorbed or replaced by a successor…infrastructure capable of providing integrated voice, data, video, private line and Internet based services.'[7]

All US services have established an Information Warfare Centre or something similar to oversight what is becoming known as information operations, but responsibilities are dispersed in the traditional staff structure between intelligence, operations and communications (J2, J3 and J6). In contradiction of the tenets of the Revolution in Military Affairs, so ardently espoused, these organisations have failed to respond and adapt to the introduction of new technology and operational concepts. In addition, the US military appears to be concentrating on information security rather than other aspects of knowledge warfare. For example, the USAF has raised the 609th Information Warfare Squadron which concentrates almost exclusively on protection and reaction to computer attack.

Information security is much more than a military problem because there are several national infrastructures in an advanced information society such as Australia which are vulnerable to strategic attack which might not be recognised in time for adequate protection measures to be put in place.[8]

Despite our best efforts to improve information security, knowledge assurance can probably never be guaranteed and best protection is likely to come from the development of systems and architectures which are sufficiently robust to function during and after malicious intrusion.

Information Attack

An advanced, information age adversary is vulnerable to attack on his information systems. Knowledge attack is the obverse of the coin of knowledge assurance. Determining how his systems interact will give clear pointers to his decision making process which should be the objective of future attacks. Understanding our own information system vulnerabilities will provide insight to methods and techniques of attack on the enemy's systems. But more and more the emphasis should be on degrading the interaction between the data available on the adversary's system and the human who analyses and interprets that information.

A major problem in the future will be how to deal with a non-developed adversary or non-state player who is not reliant on information technology and chooses to engage in asymmetric warfare. Decision superiority remains the key to success but the

[7] *ibid.,* p 34.

[8] The Marsh Commission identified eight critical US national infrastructures: information and communications, electrical power systems, transportation, oil and gas delivery and storage, banking and finance, emergency services, water supply systems, and government services (Correll, 'War in Cyberspace', pp 32-36).

sensors needed for our battlespace situation awareness may need to be different, including for example a greater proportion of human intelligence sources and with less reliance on electronic detection. An adversary who does not use computers which can be 'hacked', or who does not communicate using terrestrial or space-based bearers which can be intercepted, is largely invulnerable to information attack. Equally, however, his decision cycle time will be long and his knowledge of our force capability and disposition are likely to be limited. So in this situation we must ensure we play to his weaknesses not his strengths. In particular, we must ensure we identify exactly what are our intelligence requirements - what do we need to know - and put in place a collection mechanism to obtain the data we need together with the processing and analysis to transform this into information and knowledge.

While a less developed adversary might lack the infrastructure and capacity to operate as a modern information age force, he might well have access to other tools to circumvent his lack of capability. For example, by keeping the conflict or impending action at crisis level he will attract media attention, and through their reporting he will most likely be able to gain most of the knowledge he needs about our operational capability and disposition. He will also be in a position to manipulate political perception of events and through his influence on public opinion even control political reaction.[9] An open democratic society is at a decided disadvantage in dealing with an unscrupulous, authoritarian adversary.

A final aspect of information attack is encompassed by what we have traditionally called electronic warfare. Like all dimensions of warfare there is both a defensive and an offensive element to electronic warfare. The defensive element includes threat warning, counter-measures and jamming to electronically protect an aircraft threatened by an adversary weapon system. The offensive part includes detection and jamming of his defensive systems typically to open the way for a strike package to their target. However, in the new paradigm of knowledge warfare, we can look at electronic warfare capabilities as diminishing the enemy's situation awareness by denying, degrading or deceiving his observation of activity in the battlespace. There is a closely coupled and highly geared relationship between our own and the adversary's situation awareness in this situation. First we must know of his activity in the battlespace - the surveillance capability detailed earlier - then we must look to ways of decreasing the probability of him detecting our activity. Some of this will be accomplished through physical means by reducing the signature of our platforms - reduced infra-red emissions, the use of radar absorptive materials, the application of a whole range of stealth technologies, and so on. Some will be achieved using electronic means but because at present these are likely to be predominantly active means, he will become aware of our efforts. And some will be by threatening or attacking his collection platforms. There is a clear need for improved electronic capability to counter adversary collection effort which is undetectable by him or so ambiguous in origin as to not be attributable. The point is that any decrease in his situational awareness will enhance our decision superiority.

[9] No where is this more evident than at present in the Gulf where Saddam Hussein has garnered Arab support by appearing to defy US threats while at the same time diminishing political and electoral support for action against him in the US itself.

Precision Strike

No matter how good our decision superiority, common sense, war-fighting experience and prudent planning all point to the need to complement this by simultaneously degrading that of the adversary. This can be accomplished both by reducing his situation awareness and by degrading his internal processes. We have already seen the present capability deficiency in electronic and defensive means of diminishing his situation awareness and this points to the requirement to physically attack or threaten his collection capability - his surveillance radar sites, his maritime patrol aircraft and his other airborne collectors - and his command, control and communications infrastructure (sometimes called a nodal strategy). We know that computer attack is a burgeoning field and may eventually allow electronic attack of his decision making processes, but the likelihood is that this too will need to be complemented by physical attack, certainly in the medium term (say, twenty years). In any case, having attained a sufficient degree of decision superiority, we will need at some stage to physically attack and destroy the target sets associated with his centre of gravity.[10] The technology of the information revolution has provided us the means to accomplish this with great accuracy using precision guided munitions.

The battlespace awareness needed for decision superiority also provides the first element in accomplishing precision engagement. We already know what the target is and where it is located. The next element is recognition of the target and guidance of the weapon to impact. This will almost always require different sensor characteristics with a much narrower field of view and a much higher resolution than wide area surveillance sensors. Some components of the sensor system will need to be mounted on the weapon itself, while others, for example a target illuminator, may be mounted on the aircraft releasing the weapon. A more recent innovation is the use of off-board sensing to better utilise very expensive sensor systems and minimise the cost of the attack aircraft, and this trend can be expected to continue in the future. An early example of this technique was 'buddy lasing' where one aircraft laser was used to designate the target while the laser guided bomb was released by another. Similarly, ground based laser designation has long been used by forward ground controllers (FAC) in close air support missions. More recently, weapon delivery cues have been passed from a ground based FAC directly to the head-up-display of F-16 aircraft during the Bosnian conflict and this system is also capable of linking video in both directions.[11] Some emerging weapons systems such as the Joint Strike Fighter are planned to utilise a high degree of off-board sensing and they will routinely take target information from airborne systems such as JSTARS aircraft and more than likely from space-based systems.[12]

Off-board sensing is multi-static illumination by another name but oriented toward target recognition and illumination rather than wide area surveillance. However, this

[10] Stephens, Alan, 'Weapon of first choice: Strike Aircraft in the Asia-Pacific Region', *Asia-Pacific Defence Reporter*, Volume XXIII, Number 1, January 1997, pp 26-27.
[11] Project Sure Strike - an improved data modem in Block 40 F-16C allows a ground based FAC with a laser range finder to transmit target co-ordinates via UHF/VHF radio to an aircraft for presentation on the HUD. Also allows video transmission both directions. See Warwick, Graham, 'USAF Plans Upgrade for F-16s', *Flight International*, Number 4615, Volume 153, 4-10 March 1998, p 25.
[12] La Franchi, Peter, 'Master of the Battlefield', *Australian Defence Business Review*, 19 December 1997, p 17.

trend may not suit Australia's circumstances because of lack of autonomy through not controlling the off-board systems, especially those which are space-based, and alternative arrangements may be necessary. On the other hand, off-board sensing provides a strong measure of force protection by allowing the high value sensor system to stand off from the target and the release aircraft to remain passive to minimise detection and engagement by target defences. This is a powerful incentive for a small air force where aircraft attrition cannot be tolerated. Somehow we must achieve a balance between multi-static and onboard, autonomous sensors.

We have already seen with the surveillance sensors required for situational awareness that complementary systems have a strong multiplying effect and this is also true of the sensors associated with precision engagement. But rather than occurring in the slower time of wide area surveillance, multi-mode sensors must function in the compressed time frame of the final engagement. When this has been accomplished, a significant increase in effectiveness has been evident. For example, US Army and other force experience of operational degradation of electro-optical sensors by weather, dust or battlefield smoke and haze has led to the incorporation of millimetre wave fire control radar into the Longbow AH-64D version of the Apache attack helicopter. The combination of the electro-optical suite and the radar enables the generation of multi-spectral imagery allowing operation in almost any type of condition.[13] In the future, precision guided munitions will routinely incorporate multi-mode sensors. There have already been demonstrations of communications with other airborne platforms such as the E-8 JSTARS and the RC-135 Rivet Joint electronic intelligence system, combining targeting and terminal guidance information. This synchronisation of surveillance information with targeting and terminal guidance information has great potential to enhance the knowledge base by providing rapid, high quality feedback.

There has already been some experimentation with an even wider operational concept to tie together surveillance and targeting capabilities using airborne early warning and control aircraft (AEW&C), joint strike targeting system aircraft (JSTARS), and signals and electronic intelligence gathering aircraft (Rivet Joint), which has been called the electronic triad.[14] Linking the information available on each of these platforms using human operators to interpret and task strike aircraft, provides an unprecedented precision engagement capability while affording maximum concealment of the strike package and unparalleled force protection. The effect of precision engagement based on superior battlespace situational awareness and multi-static targeting is that a small strike force like that of the RAAF becomes extremely viable.

With further acceleration of information technology and miniaturisation the likely medium to long term outcome is the combination of all these surveillance and targeting systems into a single platform. The immediate question then is: can these manned aircraft eventually be replaced by uninhabited aerial vehicles?

[13] La Franchi, 'Master of the Battlefield', p 19.
[14] Wall, Robert, 'The Electronic Triad', *Air Force Magazine*, Vol. 81, No. 1, January 1998, pp 54-59.

Is There Anybody Up There?

Unmanned aerial vehicles (UAVs) are ostensibly a very attractive alternative option to manned aircraft, especially for high-risk missions. Without the need to provide life support systems for a crew, airframe and engine complexity can be greatly reduced, in turn reducing weight and cost which can be translated into a variety of desirable attributes; for example, exchanged for increased range and endurance. In particular, unmanned aircraft can be designed to routinely operate at very high altitudes (above 50 000 feet) where human life support systems become very complex, and can take advantage of this to provide very long endurance (several days). A vehicle configured for high altitude, very long endurance flight begins to assume some of the characteristics of a low orbit, (almost) geostationary satellite with wide area coverage and great persistence. But most important of all, the loss of an unmanned aerial vehicle does not represent the waste of the very considerable investment in highly trained aircrew.

However, despite rapid advances in information related technologies, the unmanned aerial vehicle has not yet come of age as part of a system. Bosnian experience with UAVs indicates the life cycle costs of the total system to be not less than manned aircraft despite the cost of aircrew. For the future, Northrop Grumman is exploring ways to save as much as one third of the life cycle costs and it is looking at ways for one person to control up to eight unmanned aircraft.[15] Also, the system is totally reliant on extensive and wide band communications links that may be difficult to provide reliably and securely, and are vulnerable to interception. Finally, the flexibility inherent in a manned system is diminished in comparison with an unmanned system because, among other reasons, the element of human interpretation is at the end of a long, vulnerable, bandwidth-limited communication link. Of course, even a very high altitude UAV is subject to sovereignty laws and cannot penetrate foreign airspace until war has been declared or rules of engagement permit this intrusion.

Nevertheless, there are considerable advantages for the use of unmanned aerial vehicles in the Australian situation, particularly to complement other remote and manned systems. Continuing research and experimentation with Pathfinder aircraft indicates that solar powered UAVs may have long duration persistence at high altitudes. The coverage of such craft and size of footprint may contribute to air power in the areas of communications at a cost lower than satellites.[16] In addition, a high altitude, long endurance vehicle can carry several types of sensors and provide wide area surveillance coverage. It can act as a communications link between other platforms and a ground air operations centre, giving us independence from non-sovereign satellite systems and a smaller footprint for interception of traffic. Finally, an unmanned aerial vehicle can provide targeting information to a manned strike package. In suppression of enemy air defence (SEAD) tests a Hunter UAV was able to transmit targeting data to F-16 aircraft fitted with improved data modems (IDM).[17] The introduction of Uninhabited Combat Air Vehicles (UCAVs) is distant, probably past 2010. UCAVs would probably rely on off-board sensing '...to keep cost and

[15] 'Pentagon to Test Lethal Air Strikes by Robot Planes', *Defense News*, Volume 13, Number 10, p 36.
[16] 'Pathfinder Quest', *Flight International*, 25 February-3 March 1998, p 43.
[17] 'UAVs Go To SEAD', *Flight International*, 25 February-3 March 1998, p 22.

operational complications to a minimum.'[18] One of the main advantages for a UCAV is that it possesses greater manoeuvrability because of the higher normal accelerations (g forces) it can sustain unfettered by the physical limits of a human being.[19] Lockheed Martin also predict that taking the pilot out of the aircraft could reduce acquisition costs by 20 percent.[20] However because of a lack of an onboard pilot to provide situational awareness, the UCAV would require an automated self-protection system. Another implication resulting from the lack of an onboard pilot is that typical rules-of-engagement require human intervention in the sensor-to-shooter link. The critical issues facing UCAV systems are command and control and particularly the ability to fly multiple vehicles, including operating manned and unmanned aircraft together.[21]

In the Public Eye

Perhaps the single most striking feature of the new revolution in military affairs made possible by the technology of the information revolution is the pervasive influence of the media in all aspects of war-fighting. This has several implications for successful prosecution of warfare in the knowledge domain. The first is dealing with the 'CNN effect' and another is management of the adversary's perception.[22] The first Gulf War in 1991 saw near real-time reporting for the first time with vivid television images of the air attacks on Baghdad. For Australia and her highly professional defence force, the CNN effect is generally beneficial because it is likely to enhance the moral authority of the government's decision to resort to armed conflict and we should not fear close examination of our strict compliance with the laws of armed conflict. However, it has the downside that it is an avenue that is open to exploitation by the adversary and has the potential to give him powerful leverage over public opinion and the political reaction to it. In any case, because of the transnational characteristics of modern media capability, it is effectively beyond control even of a closed society and we must come to terms with its existence.[23] The main danger is that while the media cycle time is faster than our decision cycle time, the information available from media sources are snapshots selected by a news editor with particular intent and is more akin to uncorrelated data or information 'noise' than knowledge.

An important corollary of the CNN effect is that governments will be reluctant to commit to armed conflict and there will be a strong tendency to seek 'bloodless battles' to minimise casualties and reduce the duration of war. In company with this imperative for rapid resolution of conflict is an emphasis on negotiated settlement

[18] 'Navy Eyes Stealthy Unmanned Aircraft', *Aviation Week & Space Technology*, 13 October 1997, p 27.
[19] The Robotic Air Force, *Air Force Magazine*, September 1997, p 74.
[20] 'Pentagon To Test Lethal Air Strikes By Robot Planes', *Defense News*, Volume 13, Number 10, p 36.
[21] Warwick, Graham, 'Persistent Ambitions', *Flight International*, 15-21 October 1997, pp 36-37.
[22] For discussion on media operations see Cobbold, Richard, 'Information Warfare: An Underview', *The New International Security Review*, Royal United Institute for Defence Studies, London, 1997, pp 66-76; and Badsey, Stephen, 'Information Warfare and Media Warfare', unpublished paper given to the Annual Air Power Symposium held at the Royal Norwegian Air Force Academy, Trondheim, 10-12 February 1998.
[23] Column 8, *Sydney Morning Herald*, Thursday 19 March 1998, reported that RAAF personnel stationed in Kuwait were communicating with their families and the newspaper via the Internet and receiving their news from home from various media web sites.

rather than unconditional surrender. Since the superpower confrontation after the Second World War exposed the impossibility of total war, the traditional paradigm of warfare for the democracies has been of three phases. The first phase is reacting to aggression and halting the enemy advance, the second then building up combat power, and finally the third a counter-offensive to reverse the losses sustained. But this legacy view of war-fighting as a three-phase affair has been outmoded by the power of the media and the consequent electoral and political reaction. Now, governments must be seen to react to counter aggression or other unacceptable international behaviour but time will never be available to build up the forces required to roll back the aggressor's gains let alone to actually implement a counter-offensive.[24]

The outcome of this is a preference for particular forms of warfare and air power is likely to be the weapon of first choice. This is because air power provides the means of reacting quickly to a crisis by assembling and deploying forces, using their operational reach to threaten adversary forces early in his offensive, and employing combat power precisely and with great discrimination to halt his attack. No other form of combat power can achieve this without being permanently deployed forward, clearly not an acceptable political or economic proposition for Australia or her allies. Ships take too long to reach the area under threat, and the deployment and development of land combat power (the build up) takes even longer. However, the combination of the operational reach and precision strike capability of modern air power can be employed rapidly and to great effect. The important thing is to stop the aggressor quickly before he has time to make major territorial and political inroads or to consolidate his gains.

Don't Send Me a Memo

These new operational concepts of decision superiority and precision strike made possible by the technology of the information revolution may never be fully exploited unless we are able to adapt our internal processes to cope with the change. The ability of our hierarchical structure to respond to a technology that relies on networking is perhaps a bigger challenge than absorbing the technology.[25]

We have already seen that there are several elements of knowledge warfare. First, we need to define our knowledge requirements so that specialised agencies can collect data and information to satisfy what we need to know. Then this information (it may only become knowledge in our mental hands) must be filtered, organised and manipulated so that only that portion which requires interpretation by the human mind is presented and as much as possible of the remainder is handled electronically. Since this information is vulnerable to corruption in both its physical and electronic form it must be protected from unauthorised interception and change. Similarly, we must

[24] The difficulty in building and holding together a coalition to respond to Iraq's development of weapons of mass destruction is evident at the time of this conference. By skilful manipulation of world public opinion, Saddam Hussein has maintained the strategic initiative and looks likely to face down the threat of air strikes against him. Any ground action seems so improbable as to be ludicrous.

[25] Carl Builder has postulated four distinct models of human organisation. The hierarchy is best suited for power transactions such as in command and control arrangements whereas a network is best suited for information (or knowledge) transactions. Clearly, knowledge warfare will be primarily concerned with knowledge transactions.

attack (‘hack’) the enemy’s systems to alter his databases and degrade his level of knowledge. Because much of our knowledge base and that of the adversary will be derived from information in the public domain, we must be skilful in the presentation and use of public information to give the ‘pitch’ we want and diminish the effect of his ‘spin doctors’. The manipulation of public information will be a vital part of any deception and psychological operations plan. Finally, many of the tools of knowledge warfare are legacies from the field of electronic warfare, resident in the closely guarded world of the old crows.

In the past these have been seen as disparate elements but in the new paradigm of knowledge warfare, there would seem to be little sense in dispersing these functions among several staff branches such as intelligence, operations and communications. Rather they would be better grouped together at the operational level to reflect the central position of knowledge warfare in attaining decision superiority. There is already evidence of this as a successful approach in the formation of the Directorate of Information Warfare within Headquarters Air Command. Considerable synergy is evident by physically collocating specialists from each of the fields of knowledge requirements (intelligence), information management, information security, communications, public information, knowledge attack and electronic warfare. Of greater importance is that knowledge warfare is regarded as a functional entity and integrated into all operational planning starting from the initial mission analysis, through the appreciation and identification of courses of action, the development of the concept of operations, to the formulation of the air plan to support the campaign plan.

At the tactical level within Air Command, the intention is to unite all force elements involved in developing situation awareness under a single command to be called Surveillance and Control Group. This will take the existing Air Defence Ground Environment Wing encompassing all control and reporting units and their associated command support system and add imminent force structure improvements such as airborne early warning and control aircraft and the Jindalee operational radar network. Eventually, this Group will include electronic warfare assets and their support, computer emergency response teams, and unmanned aerial vehicles. Future remote or unmanned target designation systems would also come under this Group.

CONCLUSIONS

We are in the midst of a new revolution in military affairs driven by the private sector technology of the information revolution. This has opened up a whole new field of warfare in the knowledge domain which must be treated holistically if it is to be mastered. Successful warfare in the knowledge domain will require addressing all constituent elements - knowledge requirements, information management (including communications links), knowledge assurance, knowledge attack and public information. Our organisation must respond to the new environment and adapt to successfully exploit the emerging operational concepts.

The key to success is decision superiority that is attained by having better battlespace situation awareness than the enemy and by using this knowledge edge to make better decisions. To fight in the knowledge domain we must attack and defend both situation

awareness and the decision making process. The information revolution has given us new tools for offensive and defensive action in pursuit of situation awareness but this has always been an arena of battle. The revolutionary aspect is knowledge attack aimed at the decision making process. This potentially has much greater leverage than attacks against the lower levels of the hierarchy of understanding of data and information. Success in this arena will require a much better understanding of not just how humans make decisions but the decision making process of particular individuals, especially the opposing commander. This 'cognitive mapping' of the opposition may well provide the ultimate knowledge edge.

Where our future force structure and equipment are concerned, sophisticated sensor management and complementary sensor systems are prerequisite capabilities for both battlespace situation awareness and targeting. UAV and future airborne collection aircraft will provide the balance between autonomous sensors on board our fighter and strike aircraft, and off-board space-based systems.

Management of the public perception of events and limiting the adversary's ability to manipulate reporting of them are integral parts of successful knowledge warfare. More importantly, the other truly revolutionary part of the new revolution in military affairs is that taking and holding ground has been outmoded by the CNN effect.[26] Victory has been made obsolete.

A new arm of the Australian Defence Force will emerge in the next twenty years with the same tenacity that gave rise to the formation of the RAAF in 1921. There are many lessons to note from that historical event and to be applied wisely in this next important evolution. The Air Force can offer a great deal but what we would not want to see is a repeat of the debilitating divisions and arguments which marked the formation of the RAAF and undermined joint endeavour through three of the four major wars in which Australia participated this century. Decision superiority and precision engagement are key operational concepts in future warfare. Air power plays the main, perhaps dominant, role in both.

[26] The emerging operational concept of 'Halt Phase' warfare was elucidated by Lieutenant Colonel Peter Faber at the Royal Netherlands Air Force annual conference on Air Power Theory and Practice held in The Hague, 24-28 November 1997. I am indebted to Dr Alan Stephens for bringing these views to my attention before publication.