OFFENSIVE INFORMATION OPERATIONS

A KEY ENABLER FOR THE LAND FORCE

LIEUTENANT COLONEL JAMES ROCHE

ABSTRACT

The ADF experience of Information Operations is heavily weighted towards 'influence' and civil-military interaction. This bias is reflected in our concepts and philosophical doctrine. Army needs to recognise the utility of offensive capabilities, such as electronic and computer network attack, in both conventional and intra-state war. Recognising this, Army should develop appropriate organic capabilities, while enhancing its capacity to harness current and future effects. This development will be fundamental to the success of the Land Force in the complex informational terrain of the near future.

> *Logic and experience suggest it will be more important to pursue three ever present…mission needs… win the psychological contest with current and potential adversaries; keep the trust and confidence of home and allied populations while gaining the confidence and support of the local one; and win the operational and strategic, cognitive*

and technical 'information age applications' contest with current or potential adversaries.

Brigadier General Waas de Czege (Ret) US Army

The Australian experience of Information Operations (IO)[1] has developed against a background of peacekeeping and stability operations within our near region. These operations have seen a heavy emphasis on pamphleteering, civil military liaison and limited electronic exploitation. This is best exemplified in the words of an International Force East Timor (INTERFET) IO officer:

> The INTERFET information campaign falls into the broad classification of support information operations. Its dual aim was to shape the psychological perceptions of large elements of the population and to mould opinion where possible. In Operation STABILISE the campaign was not aimed at attacking the computer networks of an enemy or waging electronic warfare against an opponent. Rather, the campaign aimed to defend the reputation of the peacekeeper and to protect the local population…[2]

Even the nature of Australian operations in Iraq and Afghanistan, while significantly more lethal than those mentioned above, lend themselves to the 'strategic communications' battle focused on public perception management.[3] As a consequence the Australian Army's concepts and doctrine regarding IO are substantially biased towards the defensive element and towards what is referred to above as 'support information operations'.

… Army runs the risk of falling behind key allies in the development and use of offensive IO capabilities …

Due to this emphasis, Army runs the risk of falling behind key allies in the development and use of offensive IO capabilities[4] and losing one element of the capability edge within the ADF's primary operational environment.[5] Further, the Defence White Paper 2009 aspires to a future defence force that has a 'winning edge' enabled by information superiority. It is implied that this capability advantage is crucial to success across conventional war, intra-state conflict, and the broad range of supporting and enabling roles identified in the White Paper. To meet this wide range of requirements, the government undertook to enhance the ADF's electronic warfare and cyber warfare capabilities. Given the active pursuit of offensive capabilities by our allies and the clear strategic guidance, Army needs to consider its requirements for offensive IO effects.

The purpose of this article is to stimulate discussion within Army regarding the integration of offensive IO effects into future concepts and capability development. The article will focus on the application of computer network attack and electronic attack given the broader understanding of other offensive elements such as destruction. The article will examine the current doctrinal and conceptual environment, and argue that the Army's intellectual approach to IO has been skewed toward the non-offensive disciplines. The article recognises that this is partially due to the classified nature of the offensive capabilities and their use, and provides several open source examples to illustrate both the utility and limitations of these capabilities. The article will then identify the implications for Army: the principal element of the Land Force.[6]

THE INTELLECTUAL BASIS

As a concept-led, capability-based Army, the intellectual basis for Army's approach to IO is particularly important. So too, is the recognition that any Army IO activities occur within a broader Joint and national framework. In this sense, it is notable that Joint concepts and doctrine provide little philosophical guidance for the conduct of offensive IO. *Joint Operations in the 21st Century, the Future Joint Operating Concept*, Defence's capstone concept, provides limited guidance on any specific capabilities due to its effects-based approach. At the same time, the higher level doctrinal publications[7] are heavily weighted, both in the level of detail and the examples used, towards psychological operations, civil-military liaison, and the 'related discipline' of public affairs. Offensive IO capabilities are only broadly and briefly described.

… Joint concepts and doctrine provide little philosophical guidance for the conduct of offensive IO.

Army's capstone concept, *Adaptive Campaigning – Future Land Operating Concept* identifies 'Information Actions' as one of the five mutually reinforcing and interdependent lines of operation of Adaptive Campaigning.[8] Information Actions are defined as:

> Actions that inform and shape the perceptions, attitudes, behaviour and understanding of target population groups: assure the quality of our own information, while attempting to disrupt or dislocate enemy command capabilities.

Adaptive Campaigning states further that this line of operation 'will remain central to campaign success and will tie all other lines of operation together'.[9]

The Information Actions line of operation is further defined by the tactical sub-concepts of: influence, counter command, and command and information protection. Despite the inclusion of the latter two sub-concepts, the majority of

the Information Actions discussion focuses upon media and public affairs, 'tactical ambassadors' and 'cultural competence'. The underlying philosophical approach is further emphasised in the statement:

> …the contest to tell one's story before an enemy is becoming more influential in the final outcome of conflict…all actors aim to rally support for their cause, create an impression of effectiveness and inevitably victory, discredit their oppositions…and destroy public morale. Consequently the primary purpose of Information Actions is to inform and shape the perceptions, attitudes, behaviour and understanding of targeted population groups…[10]

Army's philosophical level of doctrine, including Land Warfare Doctrine 1: *The Fundamentals of Land Warfare* (2008) and Land Warfare Doctrine 3.0: *Operations* (Developing Doctrine 2008), pays scant attention to the function of IO or Information Actions. Both documents recognise the perception battle in terms of domestic and international audiences, establishing the dominant narrative, and exploitation and denial of media. So too, both describe the goal of 'information dominance' in terms of information acquisition, analysis and assurance. Despite this, neither document considers how such activities would be conducted, or how they would be integrated into the overall operational design. It is also worth noting that Army's procedural doctrine publication Land Warfare Doctrine 3.2.0: *Information Operations*, while providing a balanced and coherent description of Information Actions, remains 'developing doctrine'.

This brief review of the conceptual and doctrinal basis for Australian IO demonstrates that the philosophical approach is strongly biased …

This brief review of the conceptual and doctrinal basis for Australian IO demonstrates that the philosophical approach is strongly biased in favour of psychological operations, civil-military liaison and public affairs. Unfortunately, this limited view does not allow for adequate consideration of the role and effects of offensive IO in both conventional and intra-state wars, and in both the perception and the information battle. Given the lack of philosophical and doctrinal information, a brief review of offensive IO in recent conflicts may provide a useful starting point to consider Army's needs.

OFFENSIVE IO IN AN OPERATIONAL CONTEXT

While cyber warfare has gained increasing public prominence over the last twelve months, the use of computer network operations, in particular computer network attack, has been relatively commonplace in the conflicts of this decade. Principally,

this discipline has been used to support the perception battle, both within state-based 'conventional' conflict and counterinsurgency operations. At this stage there is little evidence of the use of computer network attack to target digital battlefield command and control systems. This may reflect both the technical difficulties of attacking 'closed networks' and the fact that in each case studied in this paper, one or more of the combatants did not field such a system. It is to be expected that techniques will develop to allow for their exploitation and disruption as these systems continue to proliferate.

Some of the more useful examples of computer network attack can be found in Russia's conflicts at each end of the last decade: the second Chechen War commencing in August 1999 and the conflict in Georgia in 2008. Russia was one of the earliest exponents of 'information warfare' so it is not surprising that both conflicts demonstrated the use of computer network attack in support of an extensive 'perception battle'. In each case Russia sought to establish and control the narrative, both in the traditional media and in cyberspace. The second Chechen War saw extensive hacking of websites supporting the Chechen cause. A number of sites were disabled, others were linked to the Russian Internal Security Service site, while others were defaced with pro-Russian slogans.[11] Of note this activity reflected complete disregard of national borders or sovereignty. Many pro Chechen sites were hosted in third world countries; however, this did not protect them from manipulation or disruption.

The 2nd Chechen War saw extensive hacking of websites supporting the Chechen cause.

Russia's short war with Georgia in 2008 displayed a similar focus and techniques. The offensive into Georgia was preceded by a wave of cyber attacks against Georgian government websites, including defacement of public targets, such as government websites, and distributed denial of service[12] attacks. These attacks had an impact on the availability of government websites and denied access to public services such as electronic banking through the National Bank of Georgia. While not officially attributed to the Russian government, these attacks appeared coordinated with indications of government guidance and support to private individuals and groups. Denial techniques, malware[13] and target lists were made available and distributed on Russian or pro Russian forums and sites.[14] The coordinated approach, including target lists of sites and the selection of the 'best fit' malware for the sites, also suggests a level of organisation and capability beyond that of amateur partisan supporters.[15]

The Georgian conflict also demonstrated the dual effect of cyber attacks: the physical and the cognitive. Firstly, the actions denied access to the communications network supporting the Georgian leadership, undermining the Georgian ability to coordinate a response, maintain contact with the public, or develop their

narrative for domestic and international audiences. Secondly, the denial of access to national institutions and the defacement of sites (particularly linking pictures of the Georgian President with Hitler) reduced the confidence and trust of the Georgian population.[16]

Similar actions were on display during the Israeli Operation CAST LEAD in Gaza in 2008. Both Hamas and Israel launched cyber campaigns, focusing on the promulgation of their narrative, enlisting online support, and attacking each other's cyber activities. 'The online war over Gaza was relentless. Hackers on both sides worked to deface websites…'[17] Once again this conflict saw actions such as distributed denial of service attacks and defacement of both Hamas and Israeli websites conducted by 'non-state actors', such as the 'Jewish Internet Defence Force'. There are also strong indications that both sides made 'coordinated efforts to create supportive online communities that might act as force multipliers in cyberspace'.[18] At the very least it is clear that the Israeli government provided information to sympathetic members of the virtual community through the Foreign Ministry 'hasbara' (public explanation) department.[19]

… it is clear that the Israeli government provided information to sympathetic members of the virtual community …

These cases demonstrate both the utility and limitations of computer network attack. Firstly, it can be seen to have contributed to the maintenance of the narrative by denying and disrupting the ability of the adversary to pass their story across the Internet. In each case, the obscuration of responsibility and the ability to mobilise a virtual community allowed for deniability by the respective nation-states. It also allowed for the mobilisation of the public and the creation of a groundswell of support through 'active' participation in the conflict. The Georgian conflict also demonstrated the contribution that cyber attacks can make to 'isolation of the battle space'. This concept is defined in *Adaptive Campaigning* as: '[preventing] the enemy from informing, supporting, controlling or reinforcing their forces and…unduly [influencing] the civilian population in a selected portion of the battlespace'. [20]

In none of these cases, however, did the offensive actions completely isolate their opponents. Both the Chechens and Hamas were able to maintain an Internet presence through re-routing sites and use of the global virtual community. It is also important to note that during the conflicts in Georgia and Gaza, Russia and Israel placed significant restrictions upon the traditional media, unlike their adversaries. Consequently traditional media still played a vital role in supporting the Georgian and Hamas narrative. Thus, while an important and effective tool in the perception battle, it is clear that computer network attacks must be undertaken within the context of a broader information campaign.

Offensive Information Actions also have a clear role to play in both the counter command battle: 'attacking and eroding the enemy's will to fight, diminishing their understanding…and their ability to make timely and effective decisions'.[21] The growing military dependence on battlefield networks and public information infrastructure provides an increasingly broad target list for electronic attack. This includes both communications systems and non-communications emitters such as navigation systems.

While electronic attack appears to have disappeared from the Australian Army capability 'golf bag', the lessons from recent conflicts have led to a resurgence of this capability within other Western forces. Following the Hezbollah conflict in 2006, the Israeli Defence Force has invested significant effort in revitalising their electronic attack capabilities. This includes establishing an electronic warfare centre and developing a range of new capabilities. During Operation CAST LEAD in 2008, the Israeli Defence Force conducted substantially more jamming than during the 2006 conflict. This included jamming radio, television and cellular phones.[22] The effect was to disrupt information flows, steer Hamas onto systems that were easier for the Israeli Defence Force to monitor, and to create the perception that 'everything was jammed'. The trust in, and access to, decision-making information was degraded.

Electronic attack has also risen in prominence in the US Army over the past decade. Open source information on US operational use of electronic attack is limited, often covered by comments such as the one below relating to Operation AL–FAJR conducted in Iraq in 2004:

Electronic attack has also risen in prominence in the US Army over the past decade.

> MNC-A and MNF-A also controlled the enemy's communications … restricting his access … and not only denying the enemy a means to communicate but also directing him to a means we could monitor.[23]

Despite the reluctance to provide details, the utility of electronic attack, both in the 'conventional' phase of Operation IRAQI FREEDOM and the subsequent insurgencies in Iraq and Afghanistan has convinced the US Army to revitalise their offensive electronic warfare capabilities. Due to a focus on the signals intelligence function, the US Army had ceded leadership in electronic warfare to the other services. As a result the other services, particularly the US Navy, had to deploy large numbers of electronic warfare officers in support of the counter improvised explosive device (IED) fight. In response, the US Army established an electronic warfare division within the Army Asymmetric Warfare Office in 2006. This organisation aimed to drive organisational change as well as training and equipment

development. The division's focus has broadened over time from counter IED to include multi-spectral jamming that targets communications, weapons guidance systems and navigation aids.[24]

The focus on attacking non-communications systems has also gathered moment in the last decade. In particular, targeting of navigational aids has become increasingly evident. During Operation IRAQI FREEDOM the Iraqi forces deployed at least four Global Positioning System (GPS) jammers in an effort to disrupt part of the overwhelming US technological advantage.[25] This had limited effect, with all jamming systems destroyed very early in the war. That said, it highlights the obvious and growing reliance of most Western armies on satellite-based geo-location, and the consequent efforts by adversaries to counter this advantage. A more subtle and effective example was demonstrated during the Russian offensive in Georgia. GPS mapping of Georgia was not available for 48 hours of the short ground phase of the conflict.[26] It has been alleged that this denial of service was engineered by the United States in support of their Georgian ally; however, this has never been confirmed.[27] Given the incomplete state of the Russian satellite geo-location system,[28] this 'denial of service' was significant. The Russians were unable to use precision munitions, and had to resort to 1960's artillery targeting equipment and traditional methods of navigation. This introduced further friction in the command and control of the operation, increased global pressure upon Russia due to the lack of precision targeting, and bought time for the Georgian response.

The Russians were unable to use precision munitions, and had to resort to 1960's artillery targeting equipment and traditional methods of navigation.

IMPLICATIONS FOR THE AUSTRALIAN ARMY

These examples demonstrate the clear utility of these functions within modern operations. If this utility is accepted, the Australian Army needs to address a shortfall in both our conceptual and practical approach. Army needs to recognise the utility of these functions and determine our concepts of employment across the five lines of operation, in a range of operational settings. This needs to be considered at greater depth than the current broad functional descriptions in procedural pamphlets or the generic counter command warfare concept contained in *Adaptive Campaigning*. Army must also participate in the Joint and whole-of-government debate over the legal and ethical use of offensive effects against networks and systems that may exist in the 'global commons', or those that provide public utility.

IO as a capability. Army should engage in the ongoing debate regarding the utility of IO as a capability descriptor. Australian doctrine allocates *eleven* discrete functions to IO[29] while the US Army allocates a number of core capabilities; psychological operations; electronic warfare; computer network operations, military deception and operational security; as well as a range of supporting and related capabilities.[30] The utility of this 'kit bag' approach has been the subject of some debate in the United States for the last few years, based on lessons learnt from recent operational experiences. It has been argued that IO as a capability should focus upon psychological operations, civil military liaison and public affairs, with the other elements distributed across existing staff functions. Under this model electronic attack, computer network attack and destruction would be placed under the operations staff.[31] At a practical level, the US Army plans to integrate its revitalised electronic attack capability into the fire support coordination process as 'electronic fires'.[32] The Australian Army should follow this ongoing debate closely to inform both concepts and capability development.

Army must also determine which offensive IO capabilities it needs to 'own' and which can be provided from joint and national capabilities.

Joint Effects. Army must also determine which offensive IO capabilities it needs to 'own' and which can be provided from Joint and national capabilities.[33] While this is nothing new, the distinction is important to ensure expectations are managed, capability development is not skewed, and that effective links to Joint and strategic organisations are developed. This latter point is crucial in order to leverage scarce assets which, in the case of a future computer network attack capability, would be coordinated at the highest level.

Education. It is also important that the offensive IO capabilities are, within sensible security constraints, demystified. In particular the intellectual capacity to integrate these effects into operational or tactical planning should not reside solely with corps-based subject matter experts or specialist staff. While the details of techniques, equipment and sources may need to be closely held, the effects available and the broad constraints and freedoms of action involved in their use should be part of the broader education and training continuum.

Organic electronic attack. Army should seek to reinvigorate our organic electronic attack capabilities. The ability to achieve electromagnetic spectrum control[34] for a given time and in a specific location is a key tool for commanders in both conventional and irregular warfare. The Australian Army's experience of electronic attack, in the main, has been based upon old shelter-based jamming equipment that allowed for few training opportunities and a limited ability to develop robust

capabilities. Technology is reducing the footprint for land-based electronic attack and developing the capability well beyond the traditional target of 'push to talk radios'. Additionally the Army may look at electronic attack capabilities that can be configured as part of tactical unmanned aerial vehicle payloads[35] providing both counter IED and communications targeting. Army should also consider the application of electronic attack on non-communications emitters, such as GPS ground stations or GPS dependent equipment. This could have particular utility during land based support to strategic strike.

Army should also ensure that it maintains and enhances land-based tactical electronic warfare capabilities …

Army should also ensure that it maintains and enhances land-based tactical electronic warfare capabilities as opposed to defaulting to the signal intelligence paradigm. While there are many benefits to be gained from developing a Joint electronic warfare centre as highlighted in the Defence White Paper 2009, Army needs to ensure that the unique requirements of providing tactical ground based electronic warfare support are not lost. Such capabilities will remain a limited resource and Army needs to decide between the unique capabilities required of the Land Force and those capabilities that can be drawn from joint and strategic assets. In particular the development of electronic attack capabilities, while closely meshed to the other elements of electronic warfare and signals intelligence, would break the paradigm that sees Land Force electronic warfare as just another collector in the broader signals intelligence network.

Electromagnetic Spectrum degraded training environment. An additional benefit from the development of a broad range electronic attack capability would be the ability to train in a degraded electromagnetic environment. Given the Army's intent to become network enabled, the least we should expect from an adversary is to attempt to degrade the network. The Land Force must develop the ability to work through systematic electronic attack, computer network operations, and the physical loss of key communications hubs. This should be part of our foundation warfighting skills, but is a challenge that Army has not embraced for some time.

CONCLUSION

There are a number of decisions for Army to make if it wishes to enable effective offensive IO. Our conceptual basis is biased towards support and defensive IO elements. This limits the potential range of effects available to the Land Force in both conventional and intra-state conflict. The examples provided in this article

demonstrate the utility of both computer network attack and electronic attack in the perception battle, in supporting efforts towards isolation of the battle space, and in supporting counter command efforts. Not the least, offensive IO disciplines provide one element of the technological capability advantage within the ADF's primary operational environment.

Army's challenge is to understand the utility of these effects, validate the requirement for organic systems, and develop the ability to draw from and contribute to joint effects. Perceptions must also be managed. These offensive effects are not a 'silver bullet', rather they provide additional capabilities that support broader operational and tactical goals. However, these capabilities provide additional effects that will enable the Land Force to carry out operations successfully in a complex information environment. Army needs to define its requirement for these effects and progress appropriate conceptual and capability development.

ENDNOTES

1 As defined in Australian Defence Doctrine Publication (ADDP) 3.13: *Information Operations* (Edition 2), 'The coordination of information effects to influence the decision-making and actions of a target audience and to protect and enhance our decision-making and actions in support of national interests.'

2 K Beasley, *Information Operations During Operation Stabilise in East Timor*, Working Paper No. 120, Land Warfare Studies Centre, Canberra, 2002, p. 2.

3 J Molan, 'Do you need to decisively win the Information War? Managing Information on Operations in Iraq', *Security Challenges*, Vol. 5, No. 1, The Kokoda Foundation, Canberra, 2009, pp. 39–42.

4 Generally accepted as Electronic Attack, Computer Network Attack and Destruction.

5 As defined in the Defence White Paper 2009: 'from the eastern Indian Ocean to the island states of Polynesia and from the equator to the Southern Ocean.'

6 The Land Force is defined as 'task organised elements drawn from all Australian Defence Force Services and the other government agencies…optimised for joint operations, operating in the joint environment…', *Adaptive Campaigning – Army's Future Land Operating Concepts*, Department of Defence, Canberra, 2009, p. xii.

7 ADDP 3.13 *Information Operations* (Edition 2); ADFP 3.13.1 *Information Operations Procedures* and ADDP 3.0 *Operations* (Developing Doctrine).

8 These lines of operation provide a philosophical conceptual framework for the conduct of adaptive campaigning and are present in all conflicts. *Adaptive Campaigning*, p. 29.

9 Ibid.

10 Ibid., pp. 50–51.

11 T Thomas, 'Manipulating the Mass Consciousness: Russian and Chechen "Information War" Tactics in the 2nd Chechen-Russian Conflict', Foreign Military Studies Office Publications, <http://fmso.leavenworth.army.mil/fmsopubs/issues/chechiw.htm> accessed 21 March 2003.

12 Distributed denial of service is an attempt to make a computer resource unavailable to its intended users. One common method of attack involves saturating the target (victim) machine with external communications requests, such that it cannot respond to legitimate traffic, or responds so slowly as to be rendered effectively unavailable. A distributed denial of service attack occurs when multiple systems flood the bandwidth or resources of a targeted system, usually one or more web servers. <http://en.wikipedia.org/wiki/Denial-of-service_attack> accessed 28 June 2010.

13 Malware, short for 'malicious software', is software designed to infiltrate a computer system without the owner's informed consent, <http://en.wikipedia.org/wiki/Malware>, accessed 28 June 2010.

14 'Cyber Attacks against Georgia: Legal Lessons Identified', Cooperative Cyber Defence Centre of Excellence, Estonia, <http://www.carlisle.army.mil/DIME/documents/Georgia%201%200.pdf> pp. 7–14.

15 Ibid., pp. 13, 14.

16 R Crowell, 'War in the Information Age: A Primer for Cyberspace Operations in 21st Century Warfare', <http://www.carlisle.army.mil/DIME/CyberSpace.cfmp> p. 14.

17 Y Schliefer, 'Blogs, You Tube: the new battleground of Gaza conflict', cited in W Cadwell, M Murphy and A Menning, 'Learning to Leverage New Media', *Military Review*, May–June 2009, p. 7.

18 Ibid.

19 J Cook, 'Israel deploys cyber team to spread positive spin', *The National*, Abu Dhabi, <http://www.thenational.ae/apps/pbcs.dll/article?AID=/20090721/FOREIGN/707209856/1135> accessed 2 May 2010.

20 Ibid., p. 46.

21 *Adaptive Campaigning*, p. 51.

22 J Sprayregen, 'The Inside Story of Operation Cast Lead', *American Thinker*, <http://www.americanthinker.com/2009/01/inside_story_of_israels_success.html> accessed 1 July 2010.

23 T Metz, M Garrett, J Hutton and T Bush, 'Massing Effects in the Information Domain: A case study in Aggressive Information Operations', *Military Review*, May–June 2006, p. 109.

24 L Buckhout, 'Revitalizing Army Electronic Warfare', *Journal of Electronic Defence*, October 2007 <http://www.crows.org/jed/jed.html> accessed 7 May 2010; and L Buckhout, 'Army Electronic Warfare – Establishing an enduring Core Competency for Today's Fight…and Tomorrow's, presentation to the Association of Old Crows Convention, April 2010.

25 A Cordesman, *The Iraq War, Strategy, Tactical and Military Lessons*, Centre for Strategic and International Studies, Washington, 2003, p. 201.
26 R McDermott, 'Russia's Conventional Armed Forces and the Georgian War', *Parameters*, Spring 2009, p. 70.
27 K Moskvitch, 'Glonass: Has Russia's sat-nav system come of age?' *BBC News*, <http://news.bbc.co.uk/2/hi/science/nature/8595704.stm> accessed 6 April 2010.
28 Global Satellite Navigation System, GLONASS, is Russia's native satellite-navigation constellation, currently consisting of eighteen satellites and providing coverage of two thirds of the Earth. Portable ground receivers are not widely distributed.
29 Operational Security; Psychological Operations; Deception; Electronic Warfare; Computer Network Operations; Destruction; Information Assurance; Counter Intelligence; Protective Security; Military Networking; Posture Presence and Profile; Civil Military Cooperation; and Public Affairs as a related element to IO. ADDP 3-13 *Information Operations* (Edition 2).
30 W Richter, 'The Future of Information Operations', *Military Review*, January–February 2009.
31 Ibid.
32 Buckhout, 'Revitalizing Army Electronic Warfare', p. 4.
33 For example the US Marine Corps has made extensive use of the twenty dedicated EA-6B Prowler electronic warfare aircraft in direct support of ground forces in Iraq and Afghanistan. The Australian Army should develop concepts to utilise any future RAAF E/A-18G Growler variants, unmanned aerial vehicles or allied assets in support of ground forces when ground forces are the main effort.
34 This idea recognises that there are temporal and physical limits to the ability to control or dominate the domain. It builds on the concept of sea control. 'The condition that exists when one has freedom of action within an area of the sea for one's own purposes for a period of time…' as defined in the ADF online glossary. <http://adg.eas.defence.mil.au/adgms/results.asp?tab=index&q=Sea+Control&s=Search&terms=on&abbreviations=on&symbols=on> accessed 13 May 2010.
35 Reflects USMC plans to provide airborne electronic attack and intelligence surveillance and reconnaissance on tactical unmanned aerial vehicles to provide effects to platoons and squads. G Goodman, 'Democratized Jamming', *Journal of Electronic Defence*, October 2007, <http://www.crows.org/jed/jed.html> accessed 7 May 2010.

THE AUTHOR

Lieutenant Colonel James Roche graduated from RMC Duntroon in 1990 into the Royal Australian Corps of Signals. He held a range of regimental appointments within 1 Sig Regt, 5 Avn Regt, 139 Sig Sqn and 1 CSR. He has seen operational service as a troop commander in Western Sahara in 1993, as the X6 in Bougainville in 1998, and as the J6 for the ASNCE in East Timor in 2000. Lieutenant Colonel Roche commanded 17 Signal Regiment from 2007 until December 2008, before assuming his current appointment as Deputy Director Strategy – Army within the Directorate of Future Land Warfare and Strategy.