Edith Cowan University

Research Online

Australian Information Warfare and Security Conference

Conferences, Symposia and Campus Events

12-3-2012

The Reception, Incorporation and Employment of Informatin Operations by the Australia Defence Force: 1990-2012

Jeff Malone
Centre for Excellence in Policing and Security (CEPS)

Follow this and additional works at: https://ro.ecu.edu.au/isw

 Part of the Computer Sciences Commons

DOI: 10.4225/75/57a843b1befb1
13th Australian Information Warfare and Security Conference, Novotel Langley Hotel, Perth, Western Australia, 3rd-5th December, 2012
This Conference Proceeding is posted at Research Online.
https://ro.ecu.edu.au/isw/48

THE RECEPTION, INCORPORATION AND EMPLOYMENT OF INFORMATION OPERATIONS BY THE AUSTRALIAN DEFENCE FORCE: 1990 - 2012

Jeff Malone
Centre for Excellence in Policing and Security (CEPS)
jeffrey.malone@anu.edu.au

Abstract

The paper investigates the Australian Defence Force's (ADF) approach – understood here as the reception, incorporation and operational employment – to military information operations (IO), from 1990 to 2012. The paper identifies key characteristics of the ADF's approach to IO, and proposes explanatory factors to account for the specific form the ADF's approach to IO has been manifested. The paper concludes with predictions regarding the future form of IO within the ADF, in the context of the increasing significance of social media, the upcoming 2013 Defence White Paper (WP13) and the US 'pivot' to the Asia-Pacific region. The paper is based in-progress doctoral research, and knowledge with respect to IO during his service in the Australian Army.

Keywords
Australian Defence Force, information operations

INTRODUCTION

Stratagems, based on the exploitation and manipulation of information, are as old as the history of human conflict. But it has only been in the last two decades or so that such stratagems have been formalised as a specific mode of conflict. Across the globe, various states have developed their own terminologies to describe information-based warfare. Specifically within the Anglophone military community the systematic employment of information-based capabilities in military operations has come to be known as 'information operations' (IO). Activities typically associated with IO include – but are not limited to - electronic warfare (EW), computer network operations (CNO), psychological operations (PSYOPS), military deception (MILDEC), public affairs (PA) and civil affairs (CA). This paper examines the reception, incorporation and operational employment of IO by the Australian Defence Force (ADF) from 1990 to 2012, and proposes explanations for the particular approach to IO adopted by the ADF. The paper concludes by offering some predictions regarding the ADF's approach to IO from 2013 onward.

RESEARCH METHOD AND PROCESS

This study employs a qualitative, chronological case study method, being temporally bounded by the Cold War's end (1990) and the present (2012). The study employs a Grounded Theory methodology (Bryant and Charmaz 2007: 1-29) to formalise data collection, coding and analysing data, and producing research findings. To structure the research process, the study classifies data into one of four broad and inter-related categories, being Environmental, Declarative Policy, Institutional Policy, and Operational Policy:

- *Environmental*. This category entails data relating to the external environment, such as other nations' policies (declarative, institutional and operational) or other outside issues which might influence the ADF's approach to IO.
- *Declarative Policy*. This category entails data relating to IO contained in formal Australian Government statements of policy. This includes White Papers, strategic reviews, ministerial statements and budget/resourcing statements.
- *Institutional Policy*. This category entails data relating to policies and initiatives relating to IO carried out within Defence and/or the ADF. This includes doctrine and future operating concept documents, organisational initiatives, and training and exercise activities.
- *Operational Policy*. This category entails data relating to the ADF's employment of IO on actual operations.

The study is further structured by dividing the period under investigation chronologically into four eras:

- 1990-1995 – the era in which ADF was exposed to information-based war-fighting concepts for the first time;

- 1996-2001 - the era in which the ADF began to incorporate information-based war-fighting concepts into its structure and practices;
- 2002-04 – the era in which the ADF formalised IO as a core element of how it undertakes operations; and
- 2005-12 – the era in which the ADF has employed IO in the context of protracted counter-insurgency operations, particularly in Iraq and Afghanistan.

1990 – 1995: INITIAL RECEPTION OF INFORMATION-BASED WARFIGHTING BY THE ADF

Environment 1990-1995

The spectacular success of the US-led coalition in the first Gulf War (1990-91) arguably suggested an emergent approach to war-fighting centred on information-based activities (Campden et al 1992; Arquilla and Ronfeldt 1993). Commentators across the globe sought to identify prospective lessons for future operations. But the US retreat from Somalia (1993) – arising from the so-called 'CNN Effect' (Stech 1994) sparked by the (sic) 'Blackhawk Down' incident (Bowden 1999) – demonstrated that even an unsophisticated adversary could exploit the global electronic media environment to achieve strategic success (Brennan and Ellis 1996). Subsequent US-led peace operations in Haiti (1994) (Avruch et al 2000: 109-52) and Bosnia (1995-1996) (Wentz 1998) – in the wake of the Somalia operations - reinforced the merits of the integrated conduct of psychological operations (PSYOPS), civil affairs (CA) and public affairs (PA) activities in operations short of conventional war. This led the US to formalise the concepts of information warfare (IW) and command and control warfare (C2W) in capstone policy (Defense 1992; CJCS 1993) and future operating concept documents (US Air Force 1995; US Army 1995). These documents were profoundly influential, and arguably established a core lexicon for describing information-based war-fighting across the globe.

Declarative Policy 1990-1995

Coming into the 1990s, Australian defence policy - articulated in the 1987 White Paper (Defence 1987) and based on capability assessments from a 1986 review (Dibb 1986) - noted the significance of command, control, communications and intelligence (C3I) and intelligence, surveillance and reconnaissance (ISR) capabilities for Australia's defence within the Defence of Australia (DOA) strategy (Defence 1987: 34-40). But there was no sense that information-based capabilities would play anything other than supporting/defensive roles. Subsequent review and policy documents through to 1992 (Defence 1990; Defence 1991; Defence 1992) continued this trend. Pointedly, the tabling speech for the May 1991 *Force Structure Review* (Defence 1991) was dismissive of any lessons to be drawn from the Gulf War (Ray 1991). Later Defence policy documents (Defence 1993; Defence 1994a) elevated the significance of C3I and ISR capabilities for Australia's defence, but information-based war-fighting concepts remained absent from declarative policy documents.

Institutional Policy 1990-1995

In contrast to declarative policy, lower-level documents within Defence in this period had begun to investigate the implications of information-based war-fighting concepts for the ADF. Indicatively the Royal Australian Airforce (RAAF) 1990 Airpower Manual (RAAF 1990) – which predated the Gulf War – highlighted the significance of offensive EW capabilities for modern warfare, and noted the lack of such within the ADF. Other publications by the RAAF's Air Power Studies Centre proposed lessons for the ADF from the Gulf War (Waters 1992), and investigated employment doctrine for offensive EW and EMP munitions (Kopp 1992; Kopp 1993). Whilst insightful, these publications (and others) articulated aspirational visions rather than endorsed plans for the ADF. But by the end of 1995 – via official conferences (Defence 1994b) or formal study papers (Defence 1995), the terms IW and C2W had entered the ADF's lexicon.

Operational Policy 1990-1995

ADF employment of information-based capabilities remained limited in this period, but steadily grew to include influence activities. Direct UN control of the information campaigns supporting peace operations in Namibia (1989-90) and Cambodia (1991-93) excluded national contingents – including the ADF – from undertaking influence activities (Lehmann 1999: 28-83). The ADF's maritime contribution to the Gulf War (1990-91) meant that formed ADF units were not involved in air and land environment information-based war-fighting activities (Horner 1992). But ADF exchange personnel within US and UK units did provide the ADF with a measure of exposure to such operations (Australian Army 1991). Lacking an ADF PSYOPS capability, the

Australian Army used loaned US PSYOPS teams to support humanitarian operations in Somalia in 1993 (Wilson 1994), being the first occasion that the ADF had employed PSYOPS since the Vietnam War. Building on the Somalia experience, the ADF formed its own ad-hoc PSYOPS detachments to support peace/humanitarian operations in Bougainville (1994) (Bowd 2007) and Rwanda (1994-95) (Londey 2004: 195-206).

1996 – 2001: INITIAL INCORPORATION OF INFORMATION-BASED WARFIGHTING BY THE ADF

Environment

The influence of US-originated concepts and terms continued through this period. By the late 1990s, the term 'IO' – as a central point of reference for information-based war-fighting – had tended to take over from 'IW' and 'C2W'. 'IO' had displaced 'IW' as it was recognised that information-based activities had utility – indeed arguably greater utility – outside of conventional wars, and during all phases of a conflict. Similarly, 'IO' had displaced 'C2W', as it was recognised a target set beyond an adversary's C3I systems were vulnerable to influence or attack by informational means. These evolved concepts and terminology were reflected in US doctrine (CJCS 1998; US Army 1996; US Air Force 1998) and vision statements (CJCS 1996), which in turn influenced developments internationally, including in Australia (see institutional policy below). Observations on the role of IO during US-led operations in Kosovo in 1999 were also influential. IO undertaken by the US and other NATO members employed the doctrine and operational concepts noted above, suggesting lessons to be learnt (Wentz 2002). But also - mainly from the Serbian side - the conflict arguably involved the first extensive use of the Internet as a tool to disseminate propaganda: a precursor to the employment of social media in conflicts during the 21st century (Larsen 2000).

Declarative Policy 1996-2001

Information-based war-fighting concepts began to be visible in declarative policy documents, but centred on defensive and enabling capabilities. The report of the Defence Efficiency Review (Defence 1997a; Defence 1997b) was the first declarative policy document to include the term 'IW', but only used as a synonym for IT security (Defence 1997b: 119). The December 1997 statement *Australia's Strategic Policy* (Defence 1997c) articulated the 'Knowledge Edge' concept: achieving decision superiority over an adversary by the ADF possessing advanced C3I and ISR capabilities (ibid: 56). But absent was the notion that the ADF might employ offensive capabilities to target adversary information systems. The *2000 White Paper* (Defence 2000) elevated 'Information Capabilities' to a discrete capability grouping (ibid: 94). But in common with the Defence Efficiency Review report, the White Paper used 'IW' merely as a synonym for IT security (ibid: 95). Nor did WP2000 mention the ADF PSYOPS capability that had proved so important for ADF operations in Bougainville and East Timor (see next section), nor offensive capabilities and activities.

Institutional Policy 1996-2001

Arising from the recommendations of the 1995 C2W study paper (Defence 1995), a range of policy initiatives in this period reflected the growing acceptance of IO by the ADF/Defence. In 1996 the Defence Science and Technology Organisation (DSTO) commenced Project Takari to enhance the effectiveness of the ADF by exploiting IT, specifically including support for IO (Evans 2001: 8-9); being the first use of term 'IO' proper within Defence. In 1997 a range of structural reforms at the strategic (departmental) and operational levels (in the newly formed Headquarters Australian Theatre [HQAST]) created organisations with specific IO-related responsibilities. Operational concept (Defence 1998) and service doctrine publications (Australian Army 1998; RAAF 1998) specifically addressed employment of IO by the ADF. By 1999 interim ADF joint IO doctrine (Defence 1999) – based on US joint doctrine (CJSC 1998) - had been developed, was being taught via a specialised course at the Australian Defence Force Warfare Centre, and tested in major exercises. Collectively, these measures critically underpinned the actual successful operational employment of IO by the ADF in Bougainville, East Timor and the Solomon Islands during this period.

Operational Policy 1996-2001

This period marked the first actual operational employment of IO proper by the ADF. The ADF did not deploy PSYOPS elements during humanitarian operations in Papua New Guinea (1997-98) and Indonesia (1998). But these operations contributed to Australian diplomatic objectives, suggesting connections between ADF IO and the national-level employment of information as an instrument of influence. It was during unarmed peace operations in Bougainville (1997-2003) that the ADF first employed IO as the integrating strategy for PSYOPS,

CA, PA and other information-based activities, with great success (Clark 1998). Similarly IO critically contributed to the success of the more challenging Australian-led coalition operations in East Timor (1999-2000) (Beasley 2002; Blaxland), though this was not necessarily supported by broader public diplomacy efforts (ANAO 2002: 110-11). UN sensitivities precluded the employment of IO in subsequent UN-led military operations in East Timor (2000-2004), a point lamented by the Australian Deputy Force Commander (Smith 2002: 135-6). The ADF employed IO – based on the Bougainville experience - with some initial success in unarmed peace operations in the Solomon Islands (2000-02) (Hegarty 2001). But these activities – and the overall operation – were ultimately unsuccessful, both for the want of a peace to keep and the perceptions of Australian partisanship.

2002 – 2004: FORMALISATION OF IO WITHIN THE ADF

Environment 2002-2004

The US-led intervention in Afghanistan (2001-02) – prompted by the 11 September 2001 terrorist attacks – involved the extensive employment of IO, both to cripple the C3I capabilities of the Taliban and Al-Qaida forces, and to isolate these combatants from the general Afghani populace (ref). Similarly, the extensive employment of IO during the US-led intervention in Iraq (2003) – including the full range of destructive and lethal IO capabilities – arguably demonstrated the value of cowing an adversary into submission via (sic) 'Shock and Awe' (Koch 2003). But in both these cases, initial operational successes were not transformed into strategic success, ultimately becoming counterinsurgency (COIN) campaigns (see Environment 2005-12 section below). But the promise shown by IO in these conflicts led the US to elevate the significance of IO as a war-fighting discipline, formalised via the 2003 IO Roadmap (Defense 2003). And whilst the Roadmap was (initially) highly classified, initiatives associated with it arguably influenced other states to emulate the US example of elevating the significance accorded to IO (Watson 2007).

Declarative Policy 2002-2004

Despite IO being formalised in ADF joint doctrine (see next section), discussion of IO remained essentially absent from declarative policy documents. The *2003 Defence Update* (Defence 2003a) – which addressed changes in the security environment and Defence's response, particularly as regards capabilities – noted only enhanced defensive EW equipment for ADF aircraft (ibid.: 24). In 2004, Defence released *Winning in War, Winning in Peace* (Defence 2004), which provided an overview of ADF operations over the previous decade. But despite the prominence of IO in operations in Bougainville, East Timor and the Solomon Islands, neither IO nor IO-related capabilities warranted a mention. The absence of IO from Australian declarative defence policy documents – particularly after the 2003 Iraq war – contrasted markedly with the prominence of IO in US and UK counterparts.

Institutional Policy 2002-2004

In contrast to declarative policy, in this period IO was formalised within institutional policy. In 2002, the ADF promulgated formal joint IO doctrine (Defence 2002a). The new publication reflected the ADF's recent operational expertise and organisational arrangements for IO, but also closely resembled US joint IO doctrine (CJSC 1998). Similarly, Army (Australian Army 2002) and RAAF (RAAF 2002) doctrine publications incorporated IO. Equally joint (Defence 2002b; Defence 2003b) and Army (Australian Army 2004) future operating concept documents incorporated IO. But also during this period, the DSTO Takari program was quietly terminated in mid-2002 and strategic level organisational structures in Defence (in 2000 named Knowledge Staff Division) were disbanded with staff moved to the newly-created Office of the Chief Information Officer (OCIO) (Defence 2002c). Within OCIO IO-related work was dropped, in favour of efforts to address Defence's long-standing enterprise IT woes. Thus at the very time that the ADF formalised IO in doctrine, key enabling functions within Defence supporting IO were disbanded.

Operational Policy 2002-2004

Despite IO being incorporated in joint doctrine, the ADF's actual operational employment of IO during this period was mixed. The nature of the main ADF contribution to Afghanistan (2001-02) - special forces (SF) undertaking direct action tasks - meant that there was little scope for the conduct of IO by ADF elements beyond defensive activities. Similarly, the nature of core ADF contribution to the intervention in Iraq (2003) – a direct action SF element and fighter aircraft– meant that ADF IO activities were limited to defensive measures and physical attacks on Iraqi C3I targets (Defence 2003c: 23-4). In contrast, IO undertaken by the Australian-led mission in the Solomon Islands (2003-present) resembled those conducted during the East Timor intervention, with the scale of the initial ADF deployment intended to create a (sic) 'Shock and Awe' effect, analogous to that

created by the US during the invasion of Iraq (Defence 2012: 38). But gaps remained between ADF IO and Australia's broader national public diplomacy activities (Glenn 2007: 112). And whilst political sensitivities precluded employing influence activities during post-tsunami humanitarian operations in Indonesia (2004-05), the operation contributed to national-level public diplomacy outcomes focused on audiences both in Indonesia and the wider global Islamic community (Senate 2007: 36).

2005 – 2012: ADF IO IN THE 'NEW COUNTER-INSURGENCY ERA'

Environment 2005-12

Across the globe, a range of issues focused attention on the value of IO as a conflict strategy. As the US-led interventions in Afghanistan and Iraq dragged into protracted counterinsurgency campaigns, the nature of the IO undertaken in these conflicts changed. In particular, insurgents increasingly turned to improvised explosive devices (IEDs) as a weapon of choice, both for their lethal effects and to generate imagery for sophisticated propaganda campaigns disseminated via the Internet. Recognising the strategic nature of IED employment, the US ultimately established the Joint IED Defeat Organization (JIEEDO) to respond to this threat (JIEDDO 2006: 1), an initiative which was copied across the globe. The use of social media as a platform for influence activities during the Lebanon War (2006), and subsequent conflicts in Gaza (2008-09; 2012) and other conflicts associated with the Arab Spring suggested social media as a new battleground for influence activities (SecDev Group 2009). And denial of service (DOS) attacks on critical infrastructure, either as a stand-alone act in Estonia (2007), or in conjunction with conventional military operations in Georgia (2008) reinvigorated interest in CNO as a core IO capability.

Declarative Policy 2005-12

IO remained essentially absent from declarative policy documents during this period. In its discussion of the capabilities that the ADF would require to meet future military challenges, the Defence Update 2005 (Defence 2005) made no mention either of IO or IO-related capabilities. The 2007 Defence Update (Defence 2007a) alluded to (sic) 'soft power' roles for the ADF – suggestive of PSYOPS and CIMIC capabilities – but lacked any detail (ibid.: 16). The Update also noted the requirement to protect national-level information networks from (sic) 'cyber-warfare', but lacked detail on what role Defence of the ADF might play (ibid.: 53). The 2009 White Paper (Defence 2009a) explicitly noted the requirement for the ADF to possess offensive EW capabilities, and enhanced PSYOPS capabilities and also announced the establishment of the Cyber Security Operations Centre (CSOC) (ibid; Defence 2009b) as a national centre to counter cyber threats. In turn, the CSOC linked to a broader national cyber-security strategy. But still absent from declarative policy was the notion that ADF information capabilities could be employed in an integrated fashion, or that this might in turn link to the national-level employment of information-based capabilities/activities as an instrument of power.

Institutional Policy 2005-12

The difference in prominence of IO in institutional policy contra declarative policy continued through this period. The ADF updated its joint IO doctrine in 2007, which remained essentially similar to the 2002 version but with CA (now termed Civil Military Cooperation – CIMIC) given a greater prominence (Defence 2007b). Likewise across this period, updated Service doctrine (Australian Army 2006; Australian Army 2008; RAAF 2007) and future operating concept documents (Defence 2007c; Defence 2011) featured IO prominently. In early 2006 the ADF established the Counter-IED Task Force (CIEDTF) – based on JIEDDO – whose remit specifically included the development and support of counter-IED EW systems. In late 2008, Defence established the Asia Pacific Civil-Military Centre of Excellence (APCMCOE) – later named the Australian Civil Military Centre (ACMC) – as the ADF's centre of excellence for CIMIC. Collectively these measures suggested that the principal influences on institutional policy regarding IO originated in either the broader environment or the ADF's operational experience, rather than from declarative policy.

Operational Policy 2005-12

The ADF's varied employment of IO during this period reflected the diverse nature of its operational deployments. In Iraq (2005-08), the Al Muthana Task Group (AMTG) – later Overwatch Battle Group (OBG) – ADF IO integrated influence (CIMIC and PA) and defensive (counter-IED EW) activities within the framework of a US-led IO campaign. But the relatively low threat level within the AMTG/OBG's area of operations meant there was no requirement for the ADF to undertake more aggressive activities (Harris 2006). In Afghanistan (2005-12, ongoing as at November 2012) the ADF's reconstruction/mentoring and SF elements employed IO in a higher threat COIN environment, again within the framework of a US-led IO campaign. Again, this entailed integrated influence (CIMIC, PA and PSYOPS) and defensive (counter-IED EW) activities, with more

offensively-oriented IO activities being undertaken by US military units (ref). Following the outbreak of violence in East Timor in 2006, ADF elements (2006-12) operating under national rather than UN command conducted IO activities similar to those previously undertaken by INTERFET (Defence 2012: 25-26). ADF elements in the Solomon Islands continued IO activities in support of peace operations (ongoing from 2003 to 2012). And whilst political sensitivities precluded employing influence activities during humanitarian operations in Pakistan (2005-06 and in 2010), these operations again supported national-level public diplomacy outcomes focused on audiences both in Pakistan and the wider global Islamic community.

CHARACTERISING AND EXPLAINING THE ADF'S APPROACH TO IO

Characterising the ADF's Approach to IO

Arguably five key features characterise the ADF's approach to IO in the period 1990 - 2012: the absence of IO from Australian declarative policy; the influence of US concepts and operational experience; the tensions between declarative contra institutional and operational policy on IO; a general emphasis on defensive and perception management IO disciplines in the ADF; and the absence of a firm organisational locus for IO within the ADF.

- *Absence of IO from Declarative Policy*. Discussion of IO has remained absent from Australian declarative policy across the period of this study. This contrasts markedly with the declarative policy of other states (US and UK), and also stands in contrast to both the prominence of IO in institutional policy and actual operational employment of IO by the ADF during this timeframe.

- *US Influence*. The influence of the US approach to IO on Australian institutional policy is clear across the period of the study. During this timeframe, the ADF readily adopted US terminology, concepts and doctrine, though not without modification. Further, the individual Australian Service approaches to IO have tended to have more in common with their US equivalents, than with the Australian joint approach to IO.

- *Tension between Declarative versus Institutional and Operational Policy*. There is a clear tension between the absence of IO from declarative policy, and the considerable (though varying across the period of the study) instantiation of IO within institutional policy arrangements and the operational employment of IO.

- *Emphasis on Defensive and Perception Management Capabilities*. Across the period of the study, the capabilities held and employed by the ADF have largely focused on defensive and perception management activities within IO, albeit this begins to change toward the end of the period of the study (for example,the decision to acquire an airborne offensive EW capability announced in 2012).

- *Absence of an Organisational Locus*. Whilst a range of ADF units have been established to maintain specific IO-related capabilities, organisational arrangements to support IO as a composite discipline have been either short-lived or absent. This stands in contrast to arrangements in the US, UK and elsewhere, which have established specific organisational arrangements to foster IO proper.

Explaining the ADF's Approach to IO

The ADF's specific approach to IO is explicable in terms of four key factors rooted in broader themes in Australian defence and national security policy: the centrality of the (sic) 'Defence of Australia' strategy; a 'tactical' tradition in the ADF impacting on the development of joint capabilities; the actual operational record of the ADF; and a fundamental dissonance in Australian defence policy between the ideational and the actual operational record.

- *Centrality of the 'Defence of Australia' strategy*. For the US, the IW and C2W concepts – later IO – emerged out of operational experience in fighting a specific adversary (Iraq), focusing on a specific target set (C3I systems), which in turn had roots in Cold War operational concepts that sought to exploit vulnerabilities in the Soviet C3I system. By contrast, the absence of an identified adversary within the DOA strategy – and the marginalisation of non-DOA contingencies within the DOA strategy – has meant that there has been little imperative – in a historical context - to incorporate IO into Australian declarative policy.

- *The 'Tactical Tradition'*. Historically, ADF units have tended to fight as tactical-level elements within larger allied forces, which has arguably retarded the development, reception and incorporation of high-level operational war-fighting concepts, including IO (Evans 2008: 112-4). Nor is there a requirement to create an organisational framework to support such concepts. Further, as technically-oriented

offensive IO capabilities tend to be disposed of centrally within a large force structure – rather than being held at the tactical level – this has meant that the ADF has traditionally not acquired or employed offensive IO capabilities.

- *ADF Operational Experience*. To the extent that the ADF has acquired genuine operational experience in employing IO as coalition leader, it has been in low-technology/low threat operational environments such as Bougainville, East Timor and the Solomon Islands. Offensive, technically oriented IO activities were not undertaken – to the extent that the ADF might actually have the capability to do so – because such activities were not required. And with respect to influence activities, the low technology media environment in these contingencies has meant that the ADF has not – thus far – been required to undertake these activities in a sophisticated (social) media environment.

- *Dissonance in Australian Defence Policy*. A key theme in Australian defence policy is the dissonance between what the ADF is *supposed* to do (per the ideational DOA strategy) versus what it *actually* does. (Evans 2005). Thus, the ADF's capability and preparedness requirements – as articulated in declarative policy – have continued to be dominated by imperatives at variance from those arising from the ADF's actual operational experience. Given that IO – historically centred on influence activities – has been a key feature of actual ADF operations, it follows that IO is effectively beyond the pale of declaratory policy.

CONCLUSION: WHITHER ADF IO?

Beyond 2012, a range of new strategic challenges will confront Australia and the ADF. By 2014, ADF elements are scheduled to have departed Afghanistan and returned home. In the Asia-Pacific region, Australia (and other states) must cope with a confident and economically strong China that is now beginning to possess the military capability to back long-standing territorial claims. Equally the US has recognised the increasing significance of the Asia-Pacific region, via the so-called 'pivot' to the region. Prompted by these challenges – at least in part – Defence is scheduled to release a new White Paper during 2013. Noting these factors, it is therefore timely to consider the future prospects for IO in the ADF.

The key opportunity for ADF IO in the new White Paper is to finally formalise IO in declarative policy. Doing so would send a strong signal regarding the significance of IO (and related capabilities) for the ADF. In turn, this would provide a strong policy basis for enhancing particular ADF IO capabilities, specifically including the capability to undertake influence activities in a sophisticated social media environment. To illustrate a point, the uptake of mobile telephony and internet in the South Pacific (Cave 2012) mean that future prospective ADF operations will take place in a radically different communications and media environment than was the case in first decade of the 21st century. Incorporating IO within declarative policy also provides a stronger policy basis for integrating ADF IO with the broader national employment of information (public diplomacy) as an instrument of influence.

So to conclude, it is almost certainly the case that the significance of IO within military operations will continue to increase in the immediate future. It therefore follows that – in order to be able to operate effectively in this future environment – that the ADF must consider at length how it approaches IO.

*The views expressed in this paper are solely those of the author, and should not be construed as representing the views of the Australian Government, CEPS, or any other entity.

REFERENCES

Arquilla, J and Ronfeldt, D.F. (2003) – 'Cyberwar is Coming!', *Comparative Strategy*, Vol. 12, No. 2, Spring 1993, pp. 141-165.

Australian Army (1991) – *Observations on the Gulf War by Members of the Australian Intelligence Corps*, Canberra.

Australian Army (2002) – *Land Warfare Doctrine 1: Fundamentals of Land Warfare*, Canberra.

Australian Army (2004) – *Future Land Operating Concept*, Army Headquarters, Canberra.

Australian Army (2006) – *Land Warfare Doctrine 1: Fundamentals of Land Warfare*, Canberra.

Australian Army (2008) – *Land Warfare Doctrine 1: Fundamentals of Land Warfare*, Canberra.

Avruch, M. et al (2000) – *Information Campaigns for Peace Operations*, C4ISR Cooperative Research Program, Washington D.C.

Beasley, K. (2002) – *Information Operations During Operation STABILISE in East Timor*, Working Paper No. 120, Land Warfare Studies Centre, Canberra.

Blaxland, J. (2002) – *Information-Era Manoeuvre: The Australian-Led Mission to East Timor*, Working Paper No. 118, Land Warfare Studies Centre, Canberra.

Bowd, R.R.E. (2007) – *Doves Over the Pacific: In Pursuit of Peace and Stability in Bougainville*, Australian Military History Publications, Loftus.

Bowden, M. (1999) – *Black Hawk Down*, Bantam, London.

Bryant, A. and Charmaz, K. (eds.) (2007) – *The SAGE Handbook of Grounded Theory*, SAGE Publications Ltd, London.

Brennan, R. and Ellis, R.E. (1996) – *Information Warfare in Multi-Lateral Peace Operations: A Case Study of Somalia*, Science Applications International Corporation, Washington D.C.

Campden, A. (et al) (1992) – *The First Information War: The Story of Communications, Computers and Intelligence Systems in the Persian Gulf War*, AFCEA International Press, Fairfax, Virginia.

Cave, D. (2012) – *Digital Islands: How the Pacific's ICT Revolution is Transforming the Region*, Lowy Institute, Sydney.

CJCS (1993) – *Memorandum of Policy No. 30 – Command and Control Warfare*, Washington D.C.

CJSC (1996) – *Joint Vision 2010*, Washington D.C.

CJSC (1998) – *Joint Publication 3-13, Information Operations*, Washington D.C.

Clark (1998) – 'The Road to Peace: Aspects of Information Operations Applied to Peace Monitoring Operations on Operation BEL ISI, Bougainville 1997-98', *Combat Arms*, Issue 2/98, pp. 51-60.

Davies, M.J. (1996) – 'Command and Control Warfare: Analysing the Node', *Combat Arms*, Issue 1/96, pp. 1-14.

Dibb, P. (1986) – *Review of Australia's Defence Capabilities – Report to the Minister of Defence*, Australian Government Publishing Service, Canberra

Defence (1987) – *The Defence of Australia 1987*, Australian Government Publishing Service, Canberra.

Defence (1990) – *The Defence Force and the Community: Report for the Minister of Defence*, Australian Government Publishing Service, Canberra.

Defence (1991) – *Force Structure Review – Report to the Minister of Defence*, Australian Government Publishing Service, Canberra.

Defence (1992) - *Australia's Strategic Planning in the 1990s*, Australian Government Publishing Service, Canberra.

Defence (1993) – *Strategic Review 1993*, Australian Government Publishing Service, Canberra.

Defence (1994a) – *Defending Australia: Defence White Paper 1994*, Australian Government Publishing Service, Canberra.

Defence (1994b) – *Command and Control Towards 2005 Conference*, Canberra. Whilst these proceedings remain classified, they are extensively cited in Harris 1995.

Defence (1995) – *Australian Defence Force Command and Control Warfare Study Final Report*, Canberra. Whilst this report remains classified, it is cited in Davies 1996.

Defence (1997a) – *Future Directions for the Management of Australia's Defence*, Department of Defence, Canberra.

Defence (1997b) – *Addendum to the Report of the Defence Efficiency Review – Secretariat Papers*, Department of Defence, Canberra.

Defence (1997c) – *Australia's Strategic Policy*, Department of Defence, Canberra.

Defence (2000) – *Defence 2000: Our Future Defence Force*, Department of Defence, Canberra.

Defence (2002a) - *Australian Defence Doctrine Publication 3.13 - Information Operations*, Department of Defence, Canberra.

Defence (2002b) – *Force 2020*, Department of Defence, Canberra.

Defence (2002c) – *Media Release 456/02: Merger Marks New Era in Defence Information Management*, Department of Defence, 4 September.

Defence (2003a) – *Defence Update 2003*, Department of Defence, Canberra.

Defence (2003b) – *Future Warfighting Concept*, Department of Defence, Canberra.

Defence (2003c) – *The War in Iraq: ADF Operations in the Middle East in 2003*, Department of Defence, Canberra.

Defence (2005) – *Defence Update 2005*, Department of Defence, Canberra.

Defence (2007a) – *Defence Update 2007*, Department of Defence, Canberra.

Defence (2007b) – *Australian Defence Doctrine Publication 3.13 – Information Operations*, 2nd Edition, Department of Defence, Canberra.

Defence (2007c) – *Future Joint Operating Concept*, Department of Defence, Canberra.

Defence (2009a) – *Defending Australia in the Asia-Pacific Century: Force 2030*, Department of Defence, Canberra.

Defence (2009b) – *Cyber Security Operations Centre Brochure*, Department of Defence, Canberra.

Defence (2011) – *Future Joint Operating Concept 2030*, Department of Defence, Canberra.

Defence (2012) – *Partnering for Peace*, Australian Civil-Military Centre, Department of Defence, Canberra.

Defence (2004) – *Winning in War, Winning in Peace*, Department of Defence, Canberra.

Defense (1992) – *Department of Defense Directive TS3600.1, Information Warfare*, 21 December.

Defense (2003) – *Information Operations Roadmap*, Department of Defense, Washington D.C.

Evans, M. (2005) – *The Tyranny of Dissonance: Australia's Strategic Culture and Way of War, 1901-2004*, Land Warfare Studies Centre, Study Paper No. 306, Canberra.

Evans, M (2008) – 'The Closing of the Australian Military Mind: The ADF and Operational Art', *Security Challenges*, Vol. 4, No. 2, Winter, pp. 105-131.

Glenn, R.W. (2007) – *Counterinsurgency in a Test Tube: Analysing the Success of the Regional Assistance Mission to Solomon Islands (RAMSI)*, RAND, Santa Monica, California.

Harris, J.W. (1995) – 'Command and Control Warfare', *Combat Arms*, Issue 2/95, pp. 19-42.

Harris, M. (2006) – 'Military Public Affairs in Complex Environments', *Australian Army Journal*, Vol. 3, No. 2, pp. 137-144.

Hegarty, D. (2001) – *Monitoring Peace in the Solomon Islands*, State, Society and Governance in Melanesia Project, Working Paper No. 01/4, Canberra.

Horner, D.M. (1992) – *The Gulf Commitment: The Australian Defence Force's First War*, Melbourne University Press, Carlton.

JIEDDO (2006) – *Joint Improvised Explosive Device Defeat Organization, Annual Report 2006*, Washington D.C.

Koch, A. (2003) – 'Information War Played a Major Role In Iraq', Janes Defence Weekly, 18 July.

Kopp, C. (1992) - *Command of the electromagnetic spectrum : an electronic combat doctrine for the RAAF*, Working Paper No. 8, RAAF Air Power Studies Centre, Canberra.

Kopp, C. (1993) - *A doctrine for the use of electromagnetic pulse bombs*, Working Paper No. 15, RAAF Air Power Studies Centre, Canberra.

Larsen, W.A. (2000) – *Serbian Information Operations During Operation Allied Force*, dissertation submitted to the Air Command and Staff College, Maxwell Air Force Base, Alabama.

Lehmann, I.A (1999) – *Peacekeeping and Public Information: Caught in the Crossfire*, Frank Cass, London.

Londey, P. (2004) – *Other People's Wars: A History of Australian Peacekeeping*, Allen and Unwin, Crows Nest.

RAAF (1990) – *The Air Power Manual, 1st Edition*, RAAF Air Power Studies Centre, Canberra.

RAAF (1998) – *The Air Power Manual, 3rd Edition*, RAAF Air Power Studies Centre, Canberra.

RAAF (2002) – *The Air Power Manual, 4th Edition*, RAAF Air Power Development Centre, Canberra.

RAAF (2007) – *The Air Power Manual, 5th Edition*, RAAF Air Power Development Centre, Canberra.

SecDev Group (2009) – *Bullets and Blogs: New Media and the Warfighter*, Center for Strategic Leadership, US Army War College.

Senate (2007) – *Australia's Public Diplomacy: Building Our Image*, Report of the Senate Standing Committee on Foreign Affairs, Defence and Trade, Canberra.

Smith, M.G. (2002) – *Peacekeeping in East Timor: The Path to Independence*, Lynne Reinner, London.

Stech, F.J. (1994) – 'Winning CNN Wars', *Parameters*, Vol. XXIV, Autumn, pp. 37-56.

US Air Force (1995) – *Cornerstones of Information Warfare*, Washington D.C.

US Air Force (1998) – *Air Force Doctrine Document 2-5, Information Operations*, Washington D.C.

US Army (1995) – *Training and Doctrine Command Pamphlet 525-69, Concept for Information Operations*, Fort Monroe, Virginia.

US Army (1996) – *Training and Doctrine Command, Field Manual 100-6, Information Operations*, Fort Monroe, Virginia.

Waters, G. (1992) – *Gulf Lesson One – The Value of Air Power: Doctrinal Lessons for Australia*, RAAF Air Power Studies Centre, Canberra.

Watson, C. (2007) – 'Joint Information Operations: The Road Ahead', *Australian Army Journal*, Vol. 4, No. 1, Autumn, pp. 77-98.

Wentz, L. (ed.) (1998) – *Lessons from Bosnia: The IFOR Experience*, C4ISR Cooperative Research Program, Washington D.C.

Wentz, L. (ed.) (2002) – *Lessons from Kosovo: The KFOR Experience*, C4ISR Cooperative Research Program, Washington D.C.

Wilson, D.J. (1994) – 'Psychological Operations in Somalia', *Australian Defence Force Journal*, No. 107, July/August, pp. 35-42.