ANU Press

Chapter Title: Introduction: Australia and Cyber-warfare
Chapter Author(s): Gary Waters and Desmond Ball

Book Title: Australia and Cyber-warfare
Book Author(s): Gary Waters, Desmond Ball and Ian Dudgeon
Published by: ANU Press. (2008)
Stable URL: https://www.jstor.org/stable/j.ctt24h2tt.7

Chapter 1

Introduction: Australia and Cyber-warfare

Gary Waters and Desmond Ball

In 2005 Air Commodore (Ret'd) Gary Waters and Professor Desmond Ball examined the key issues involved in ensuring that the Australian Defence Force (ADF) could obtain information superiority in future contingencies.[1] The authors discussed force posture, associated command and control systems, information support systems, operational concepts and doctrine. They discussed the ADF's approach to Network Centric Warfare (NCW); examined the command and control aspects of dispersed military operations utilising networked systems; outlined some of the principal strategic, organisational, operational, doctrinal and human resource challenges; and discussed the information architecture requirements for achieving information superiority.

Through its NCW developments, the ADF is aiming to obtain common battlefield awareness and superior command decision-making, using a comprehensive 'information network' linking sensors (for direction), command and control (for flexible, optimised decision-making), and engagement systems (for precision application of force).

The authors examined the twin notions of leveraging off indirect connections and generating effects in unheralded ways to determine what advantages might accrue to the dispersed and networked force and what paradigm shifts would be needed to realise those advantages. They also argued that whatever collaborative form of command and control might be used in future, it had to preserve simplicity, unity of command and balance. This collaborative element would be all about networking, interacting; sharing information, awareness and understanding; and making collaborative decisions.

A number of hypothetical Information Operations (IO) scenarios were presented, in which the ADF was able to defeat an adversary's air assault by cyber-attack; immobilise their naval fleet by electronic warfare (EW) attack; jam and deceive their air defences; destroy or incapacitate their command, control and communications systems; and corrupt their networks. An Information Warfare (IW) architecture for Australia was sketched out and key related issues canvassed.

The authors acknowledged that interrelationships and interdependencies between weapons, sensors, commanders and the supporting network could form the Achilles' heel of the future ADF. Furthermore, as Australia moves down a whole-of-nation approach to security, the way we cooperate and coordinate our activities across government and with allies will extend that supporting network and broaden the potential vulnerabilities.

Reliance on the network will mean enhancing the capability and survivability of Defence's and related networked infrastructures to ensure sustained and protected flows of information. This becomes increasingly problematic as reliance on commercial technologies increases.

Planned US programs offer an unprecedented level of access and availability of information to forces in the field and Australia needs to develop equivalent initiatives so it can 'plug and play' with the United States.

While the authors discussed the Defence Information Infrastructure (DII), which they defined as an 'interconnected, end-to-end set of information systems and technologies that support the electronic creation, collation, processing, protection and dissemination of Defence information', they did not discuss the national and global equivalents, nor how these might be protected. Furthermore, Defence has published several documents since 2005, which underscore its reliance on NCW and the underpinning networks. Hence, it is now timely to examine the potential challenges to those networks and the information that flows across them and how it might all be protected.

Chapter 2 of this volume, by Gary Waters, describes the recent developments with respect to Defence planning for NCW. It examines what the ADF is hoping to achieve through NCW, and outlines the key elements of the *NCW Roadmap* released in 2005 and updated in 2007.

Notwithstanding Defence's published view, the implementation of NCW is being challenged by the demands on planners resulting from the extraordinary tempo of current operations, and the focus on Coalition and regional operations. Much needs to be done in ensuring that Australia will have the necessary capabilities for achieving information superiority around 2020. The work carried out prior to 2005 was fundamentally incomplete as it was mostly concerned with enhancing and sharing battlefield awareness and with shortening decision cycles; it essentially ignored the offensive opportunities and challenges of NCW, and the offensive role of IW more generally. Furthermore, the NCW work since then has continued to pay insufficient attention to the human and organisational dimensions.

The 'war on terror' has stimulated some aspects of IO while further distracting planners from the longer-term construction of an all-embracing NCW architecture that also addresses the offensive and defensive aspects of IW. Recent

achievements have been essentially defensive, involving investigative and forensic activities, rather than exploiting cyber-space for offensive IO.

Chapter 3, by Gary Waters, starts by highlighting the value of information to Australia and the ADF today, before discussing the potential forms of IW that could be used against us. There are certain actions an adversary might take against us and certain things we can do to protect ourselves. And there are cyber-crime activities that need to be addressed, as well as critical information infrastructure aspects. This discussion on cyber-attacks and broad network defence sets the scene for the next two chapters on attacking and defending information infrastructures.

Chapter 4, by Ian Dudgeon, discusses how information infrastructures underpin and enable today's information society, and national defence capabilities, and how they shape and influence the way we, and others, live and what we see, think, decide and how we act. It identifies the importance of these infrastructures as targets in war, to achieve physical and psychological outcomes, in order to weaken the military capability and national morale of an adversary, and how psychological outcomes can also strengthen the morale of friends and allies and influence the attitudes of neutral parties. It also discusses how, in certain non-war circumstances, foreign infrastructures may also be targeted to project national power and shape events to national advantage.

Chapter 5, by Gary Waters, discusses the twin challenges of balancing information superiority and operational vulnerability, and security and privacy in information sharing, before examining cyber-security and how we might best secure the Defence and National Information Infrastructures (NIIs). Indeed, this aspect is mentioned in the 2007 *Defence Update*, which stated that: 'There is an emerging need to focus on "cyber–warfare", particularly capabilities to protect national networks to deny information'.[2]

There is a myriad of complex and extremely difficult issues that require resolution before radically new command and control arrangements can be organised, new technical capabilities acquired and dramatically different operational concepts tested and codified. These include the extent to which complete digitisation and networking of the ADF will permit flatter command and control structures; the availability of different sorts of Unmanned Aerial Vehicles (UAVs) and the timeframes for their potential acquisition; the role of offensive operations and the development of doctrine and operational concepts for these; the promulgation of new rules of engagement; and a plethora of human resource issues, including the scope for the creative design and utilisation of reserve forces and other elements of the civil community.[3] These matters will take many years to resolve and even longer, in some cases at least a decade, for the ensuing decisions to be fully implemented.

In chapter 6, Des Ball argues a critical deficiency is the lack of a net-war or cyber-warfare centre. Australia has a plethora of organisations, within and outside Defence, concerned with some aspects of cyber-warfare (including network security), but they are poorly coordinated and are not committed to the full exploitation of cyber-space for either military operations or IW more generally.

A dedicated cyber-warfare centre is fundamental to the planning and conduct of both defensive and offensive IO. It would be responsible for exploring the full possibilities of future cyber-warfare, and developing the doctrine and operational concepts for IO. It would study all viruses, Denial of Service (DS) programs, 'Trojan horses' and 'trap-door' systems, not only for defensive purposes but also to discern offensive applications. It would study the firewalls around computer systems in military high commands and headquarters in the region, in avionics and other weapons systems, and in telecommunications centres, banks and stock exchanges, ready to penetrate a command centre, a flight deck or ship's bridge, a telephone or data exchange node, or a central bank at a moment's notice, and able to insert confounding orders and to manipulate data without the adversary's knowledge. It would identify new capability requirements. It should probably be located in a building close to the Defence Signals Directorate (DSD) in the Russell Hill complex and be run out of the Department of Prime Minister and Cabinet (DPM&C).

ENDNOTES

[1] Gary Waters and Desmond Ball, *Transforming the Australian Defence Force (ADF) for Information Superiority*, Canberra Papers on Strategy and Defence, no. 159, Strategic and Defence Studies Centre, The Australian National University, Canberra, 2005.

[2] See Department of Defence, *Australia's National Security: A Defence Update 2007*, Department of Defence, July 2007, p. 53, available at <http://www.defence.gov.au/ans/2007/pdf/Defence_update.pdf>, accessed 25 February 2008.

[3] Waters and Ball, *Transforming the Australian Defence Force (ADF) for Information Superiority*, pp. 61–68.