Chapter 6

An Australian Cyber-warfare Centre

Desmond Ball

Introduction

The Australian Defence Force (ADF) is in the process of being transformed to enable it to gain information superiority in future contingencies.[1] Substantial elements of its future Information Warfare (IW) architecture are already in place, such as the *Collins*-class submarine, some of the satellite communications (SATCOM) systems, and some of the land-based intelligence facilities, but these will all have to be extensively modified and technically updated. However, most of the ADF's force and support elements remain inadequately networked. Other advanced capabilities, including the Royal Australian Navy (RAN)'s Air Warfare Destroyers (AWDs), new Royal Australian Air Force (RAAF) fighter aircraft, and various sorts of Unmanned Aerial Vehicles (UAVs) are in the process of acquisition. Complete functional integration of the 'system of systems' remains embryonic. Some essential elements of the ADF's future IW architecture are barely conceived. The most important is a cyber-warfare centre and its operational capabilities.

There has been considerable development of doctrine by the ADF since the early 2000s. In June 2002, the ADF released its doctrinal statement on Australia's approach to warfare. This occurred at about the same time that the notions of being able to gain an information advantage, dispersing forces, and networking them began to appear. The ADF argued that its aim for the future was to obtain common and enhanced battlespace awareness and, with the application of that awareness, deliver maximum combat effect. It would seek to achieve this through networked operations, which would necessitate a comprehensive 'information network' that would link sensors (for detection), command and control (C2) (for flexible, optimised decision-making), and engagement systems (for precision application of force).[2]

In 2002, the ADF also released *Force 2020*—the ADF's vision statement—whereby networked operations were seen as allowing the war-fighter, through superior command decision-making supported by information technologies coupled with organisational and doctrinal agility, to utilise relatively small forces to maximum effect. *Force 2020* states that 'in the force of 2020, we will have transitioned from platform-centric operations to Network-Enabled

Operations'. The aim is 'to obtain common and enhanced battlespace awareness, and with the application of that awareness, deliver maximum combat effect'. Shared information 'allows a greater level of situational awareness, coordination, and offensive potential than is currently the case'.[3] Further doctrinal development proceeded through 2003, including production of an NCW Concept Paper and an *NCW Roadmap*, which were completed by December 2003, and promulgated in February 2004.[4]

However, the work in 2002–2003 was fundamentally incomplete. It was mostly concerned with enhancing and sharing battlefield awareness and with shortening decision cycles; it essentially ignored the offensive opportunities and challenges of Network Centric Warfare (NCW), and the offensive role of IW more generally.

The *NCW Roadmap*, released in February 2007, reflected enormous recent progress. It articulated a plan for managing the transition of the ADF 'from a network-aware force to a seamless, network-enabled, information-age force', and provided a series of 'milestones' that 'the ADF views as critical to the realisation of its vision for NCW'. It described the mechanisms through which NCW considerations, such as cost, connectivity and vulnerability issues, are now addressed in the capability development process. And it stresses that the purpose of NCW is to enhance the ADF's 'warfighting effectiveness', specifically mentioning 'the offensive support system'.[5]

Since September 2001, a major focus of network-centric activity, across the whole–of-government, has concerned counter-terrorism. The 'war on terror' has stimulated some aspects of Information Operations (IO) while distracting planners from the longer-term construction of an all-embracing NCW architecture. The Defence Signals Directorate (DSD) has enhanced its capabilities for monitoring and tracking mobile phones, and for surveilling websites, Internet usages and international email traffic. It played a key role in the capture of the organisers of the Bali bombings in October 2002. Imam Samudra was arrested in November 2002 after sending an email. Mukhlas was traced by his mobile phone, even though he changed his Subscriber Identity Module (SIM) card every two days and spoke for only a few seconds at a time. Azahari bin Husin, who also helped plan the second Bali bombings in October 2005, was killed in a shoot-out with police in November 2005 after DSD monitored and tracked the mobile phone of one of his accomplices.[6] However, these achievements have been essentially defensive, involving investigative and forensic activities, rather than exploiting cyber-space for offensive IO.

Fundamental issues concerning the development of NCW capabilities remain unresolved, while the role and place of offensive IO and an institutionalised cyber-warfare centre are yet to even be considered. There is a palpable risk that Australia will be caught deficient in some critical capability necessary for securing

our most vital national interests in the security environment of the late 2010s and the 2020s.

There is a myriad of complex and extremely difficult issues that require resolution before radically new C2 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 C2 structures; the availability of different sorts of 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 (ROE); 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.[7] 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.

Numerous organisations currently have important responsibilities concerning some aspect of network vulnerabilities, security and regulation, in addition to the Department of Defence, the ADF and the intelligence and security agencies. Defence has a responsibility to defend vital national infrastructure, and is critically dependent on parts of that infrastructure for command, operational and logistical activities, but it is not the lead agency with respect to network security. Within Defence and the ADF, NCW-related activities remain compartmented; between Defence and the other national authorities, the coordination is fitful, sectoral and poorly organised for IO. No agency appears to be responsible for planning and conducting offensive cyber-warfare.

This chapter proposes the establishment of an Australian Cyber-warfare Centre. It argues that a Centre of some form is necessary to provide coordination of all matters concerning cyber-warfare in Australia. It would provide an institutionalised agency for the development of doctrine, operational concepts and ROE for the ADF concerning cyber-warfare. It would provide a mechanism for ensuring not only that all proposed new Defence capabilities are optimised with respect to comprehensive networking, but also that the requirements for future cyber-activities are satisfactorily identified and articulated. It would develop cyber-warfare contingency plans and specify preparatory actions. It would plan and conduct offensive as well as defensive operations. This chapter also considers several associated issues, including issues involved in determining the best location for such a Centre; the implications of cyber-warfare for command arrangements, intelligence processes and covert activities; and the need to develop appropriate ROE, doctrine and operational concepts. It also includes a brief summary of some regional developments with respect to the institutionalisation of cyber-warfare activities and the practice of cyber-warfare techniques. Finally, it argues that the establishment of an Australian

Cyber-warfare Centre has now become a matter of considerable urgency, and that without it Australia will lack a core system in its 'system of systems' required for warfare in the thoroughly networked Information Age.

The relevant organisations and their coordination

The overall responsibility for e-security in Australia rests with the Attorney-General's Department, through its charter to protect the National Information Infrastructure (NII), which 'comprises information systems that support the telecommunications, transport, distribution, energy, utilities, banking and finance industries as well as critical government services including defence and emergency services'.[8] Its mission is essentially defensive, primarily identifying and coordinating responses to incidents that seriously affect the NII.

The government's 'core policy development and coordination body on e-security matters' is the E-Security Coordination Group (ESCG), established in 2001. It is the 'lead agency addressing e-security matters'.[9] The ESCG is supported by the Critical Infrastructure Protection Group (CIPG), which is responsible for 'identifying and providing advice on the protection of Australia's information infrastructure where the consequences of a security incident are defined as critical'. It 'evaluates the threats and vulnerabilities to the NII', and coordinates crisis management arrangements with other Commonwealth agencies, including with respect to 'defence, national security and counter-terrorism programs'. It is chaired by the Attorney-General's Department, and includes representatives from the Australian Federal Police (AFP), which provides 'an enhanced law enforcement response capability'; the Australian Security Intelligence Organisation (ASIO), which provides intelligence analysis and threat assessment advice; the DSD, which provides 'enhanced incident analysis and response for Commonwealth agencies'; and the Australian Securities and Investments Commission, which undertakes 'detection, investigation and prosecution of electronic fraud in the financial sector'.[10]

There are many agencies within the Department of Defence and the ADF concerned with some aspect of NCW, including monitoring of the electro-magnetic spectrum and cyber-space; ensuring information security (Infosec) and e-security with respect to both national and Defence information and communications systems; conducting research, development and testing of NCW concepts and equipment; and addressing NCW criteria in the capability development process.

The Director General Capability Plans (DGCP) 'provides integration and coordination of NCW with other capability development matters'. The Director General Integrated Capability Development (DGICD) 'provides cross-project NCW integration'. The Director of NCW Implementation 'provides research and policy support' in NCW matters for the capability planning process. The Network

Centric Warfare Project Office (NCWPO) is 'the battlespace architect'; it is responsible for 'ensuring cross-project integration … through testing NCW compliance with battlespace architectures'. The Chief Information Officer Group (CIOG) 'manages the Network Dimension of Defence NCW capability'. The Intelligence and Security Group (I&SG) is responsible for development of the intelligence component of Defence NCW capability, and for 'managing the implementation and ongoing development of the *Intelligence, Surveillance and Reconnaissance Roadmap*'.[11]

The DSD, Australia's largest intelligence agency, responsible for both the collection of foreign signals and the security of the national information and communications systems, has extensive capabilities relating to cyber-warfare. It has broadened, with respect to its collection activities, from focusing almost entirely on the interception of information 'in motion', as electro-magnetic waves travel through the ether, to now also undertaking the collection and manipulation of information 'at rest', stored on computer databases, disks and hard drives.[12]

DSD has two stations concerned with intercepting SATCOM in the region, monitoring long-distance telephone calls, emails, facsimiles, and computer-to-computer data exchanges. DSD's largest station, at Shoal Bay, near Darwin, is primarily concerned with intercepting Indonesian communications, including both radio transmissions and SATCOM. Project *Larkswood*, which began in 1979, involves the interception of Indonesian SATCOM, and especially those involving Indonesia's *Palapa* communications satellite system. It also includes the communications of other Association of South East Asian Nations (ASEAN) countries that use the *Palapa* system.[13] Many more dish antennas were installed in the late 1990s, making eleven as at September 1999. Most of the new antennas were designed to intercept various sorts of SATCOM involving Indonesia, including mobile satellite telephone (Satphone) conversations using Inmarsat and Global System for Mobile Communications (GSMC) services.[14] DSD's other SATCOM signals intelligence (SIGINT) station is at Kojarena, near Geraldton, WA; it became operational in the mid-1990s, and currently has five large radomes. It is able to monitor selectively the communications from more than a hundred geostationary satellites stationed along the equator from about 40°E to about 170°W longitude.[15] The station reportedly functions as part of the much-publicised 'Echelon' system.[16]

DSD is also Australia's 'national authority' for Infosec. DSD's Information Security Group is responsible for 'the protection of Australian official communications and information systems', with respect to 'information that is processed, stored or communicated by electronic or similar means'. The Group also works with private industry in relation to the development of new cryptographic products, and evaluates Infosec products for industry.[17]

The ADF maintains a variety of electronic warfare (EW) capabilities which are relevant to cyber-warfare. The RAAF's Electronic Warfare Operational Support Unit (EWOSU) was established in Salisbury, SA, in 1991. One of its first responsibilities was to compile 'the first integrated electronic warfare intelligence data base in Australia'.[18] In 1976, the Australian Army raised 72 Electronic Warfare Squadron at Cabarlah, Qld, the home base of the Army's 7 Signal Regiment, to provide EW support to Army forces. It is equipped with a variety of communications intelligence (COMINT) and EW systems, employed for high-frequency (HF) and very high-frequency (VHF) interception, DF, and jamming operations.[19] During the International Force East Timor (INTERFET) operation in late 1999–2000, a component of the Squadron provided the headquarters in Dili with 'timely indicators and warning', and, 'as a secondary task', provided other reconnaissance, surveillance and intelligence collection services.[20]

EW and cyber-warfare are becoming conflated as the electro-magnetic environment merges with cyber-space. Cyber-techniques will be increasingly used to penetrate the electronic components in weapons systems, collecting electronic intelligence to inform the development of electronic support measures (ESM), electronic countermeasures (ECM) and electronic counter-countermeasures (ECCM). ECM and ECCM operations will involve a conjunction of radio-EW and cyber-attacks.

The Defence Science and Technology Organisation (DSTO) has a major role in the implementation of NCW in the ADF, providing 'essential scientific and technological support' with respect to intelligence, surveillance and reconnaissance (ISR), communications, human-computer interfaces, and decision-support tools. Its work on NCW is coordinated by a NCW Steering Group that was formed in early 2003, and includes the development of technologies for battlespace communications and protection of the infrastructure, as well as integration of future weapons systems into the C2 and engagement grids.[21]

The DSTO has recently initiated a series of 'Net Warrior exercises' to 'build, demonstrate and enhance' ADF battlespace interoperability. The participants include the Airborne Early Warning and Control Aircraft (AEW&C) Testbed, the Air Defence Ground Environment Simulator (ADGESIM), and a 'Future Ship' maritime platform. An important focus has been the tactical data-links for exchanging 'battle-space situational awareness information', including the use of 'Internet-based transmission approaches'.[22]

The ADF Warfare Centre at Williamtown is involved in the development of doctrine and the delivery of specialist courses on joint EW and joint IW.

The AFP has considerable expertise in several important aspects of cyber-warfare. It is capable of processing large quantities of digital imagery, such as recorded by closed-circuit television systems. Its Telecommunications Interception Division, which is particularly skilled in monitoring mobile phones, has expanded substantially since the late 1990s, initially under the National Illicit Drug Strategy (NIDS),[23] and since 2001 in accordance with the Australian Government's counter-terrorism agenda. In the case of the so-called 'Bali nine', the Australian heroin smugglers arrested in Bali in April 2005, AFP personnel reportedly cracked the Personal Identification Number (PIN) codes on some of the 10 mobile phones seized, enabling them to identify the network providers and obtain records of 'every phone call made or received during the life of the cards in each mobile'.[24] It is also able to intercept emails, Short Message Service (SMS) and voicemail messages 'that are temporarily delayed and stored during passage over a telecommunications system'.[25] The Australian High Tech Crime Centre (AHTCC), which is hosted in Canberra by the AFP, provides a 'national coordinated approach to combating serious, complex and multi-jurisdictional' computer-generated crime.[26]

ASIO has a Technical Operations Branch which supports its counter-intelligence and counter-terrorism responsibilities. It has expertise not only in monitoring telephones, but also in covert installation of 'bugs' and other technical devices in embassies, private residences and meeting places, and in penetrating computer-related systems.

The Australian Secret Intelligence Service (ASIS) has a Technical Section which generally conducts technical operations in foreign capitals, although it sometimes cooperates with ASIO in operations against foreign missions in Canberra. For example, it was alleged in May 1995 that ASIS had worked with ASIO to install fibre-optic devices in the Chinese Embassy in Canberra while it was being built in the 1980s.[27] Since the 1960s, ASIS has assisted DSD by obtaining foreign code-books; since the late 1990s, it has also provided DSD with internal telephone and email directories. There has been increasing cooperation between ASIS and DSD since the 1990s with respect to technical collection and surveillance operations in foreign capitals. Offensive cyber-warfare operations, and, indeed IO more generally, will place increasing demands on ASIS for covert support overseas.

The corporate sector, and especially the telecommunications, IT and aerospace companies, is an enormous reservoir of cyber-warfare capabilities. Most of the NII is in private hands. Telecommunications are virtually monopolised by Telstra and Optus. There is a plethora of Internet Service Providers (ISPs), some of them committed to the provision of maximum security for their services, regardless of the implications for access by the authorities. The corporate sector contains

technical expertise, entrepreneurial ability and research and development (R&D) capabilities.

Telstra and Optus maintain central parts of Australia's NII. Optus has a new headquarters, with 6 500 staff, at Macquarie Park in northwest Sydney. A Network Operations Centre (NOC) at the headquarters was opened by former Prime Minister John Howard in October 2007. The Optus C-1 communications satellite is particularly critical to the ADF's NCW architecture. Positioned in geostationary orbit over the equator at 156°E longitude (i.e. just north of Bougainville), it provides relatively high data rate links between headquarters and tactical platforms to support current and future C2, surveillance, intelligence, logistics and administrative networks. It carries four Defence payloads (Global Broadcast, ultra high-frequency (UHF), X-band and Ka-band), was successfully launched on 11 June 2003; it allows AEW&C *Wedgetail* aircraft, *Jindalee* Operational Radar Network (JORN) and the ground radar net to share data at required data rates.[28] Optus maintains a Satellite Earth Station at Belrose, which has four 13-metre antennas, one of which is dedicated to controlling the C-1 satellite.[29]

Telstra is the largest provider of local and long-distance telephone services, mobile phone services, and wireless, ADSL and cable Internet access in Australia. It was able to assist DSD during the hunt for the October 2002 Bali bombers. Two Telstra technicians visited Jakarta in late October and spent 'several days at the main link to Indonesia's government-owned telecommunications carrier, Telkomsei', where they extracted 'a database of millions of phone numbers', which was then handed to DSD for processing.[30]

Nearly all the servers and routers used in the Australian NII are made by Cisco Systems, headquartered in California. For example, Cisco provided the Internet Protocol (IP) phones, the wireless local area network (WLAN) and the network security at the new Optus head office in Macquarie Park.[31] Cisco has a Product Security Incident Response Team (PSIRT).[32]

AusCERT, the Australian Computer Emergency Response Team, based in Sydney, is a national agency providing expertise on computer network security, particularly with respect to incident response. It is affiliated with the CERT Coordination Centre in the United States, which studies Internet security vulnerabilities, researches long-term changes in networked systems, and provides information to improve the security of networked systems. AusCERT provides a central point in Australia for reporting on security incidents and dissemination of information relating to threats, vulnerabilities and defensive mechanisms.[33]

The aerospace companies possess a range of R&D, design and manufacturing capabilities directly relevant to the cyber-warfare exercise. These include tactical data-links, C2 systems, antenna and radio frequency (RF) propagation systems,

and UAVs, as well as specialist electronic components and testing equipment. There is already extensive cooperation between Defence and many companies with respect to NCW systems. For example, DSTO and ADI Ltd signed an agreement at DSTO's Defence Science Communications Laboratory at Edinburgh, north of Adelaide, in September 2004 to form a 'Strategic R&D Alliance' for the collaborative development of NCW technologies.[34] Raytheon Australia has a test-bed Combat Control System (CCS) at its headquarters in North Ryde in Sydney which can simulate, and test new concepts and connectivities with, the Combat Information Systems (CIS) of both the *Collins*-class submarine and the prospective AWDs.

Research, planning and preparation

The dimensions of the terms of reference for an Australian Cyber-warfare Centre require considerable debate and contemplation, and, indeed, they will eventually only evolve once a Centre has begun operating. However, there are several basic planning functions that would be central in any construct. Its activities would be both defensive and offensive. Indeed, the relationship between these is symbiotic, each nourishing the other. Research into ways of penetrating foreign cyber-systems inevitably uncovers vulnerabilities in Australian systems, while research into possible vulnerabilities often suggests ways of exploiting these for offensive purposes.

A core research function of any Australian Cyber-warfare Centre would be the study of telecommunications architectures—the terrestrial microwave relay networks, SATCOM, and fibre-optic cables—both across the region and in particular countries. SATCOM and microwave relays are reasonably accessible, allowing IPs and *pro formas* for computer-to-computer data exchanges to be identified, and providing opportunities for hacking into command chains, combat information systems, air defence systems and databases. This research activity would also involve the identification of the mobile phone numbers and email addresses of foreign political and military leaders.

Another core research function would be the study of the electronic sub-systems in major weapons systems, such as the avionics of particular combat and support aircraft. This would include, for example, finding ways of penetrating the 'firewalls' protecting avionics systems and of using wireless application protocols (WAPs) to insert 'Trojan horses'. This would conceivably allow Australian cyber-specialists to effectively hijack adversary aircraft (and to choose between hard or soft landings for them). In other cases, it would allow electronic components to be disabled or deceived—essentially conducting ECM and ECCM operations through cyber-space.

A Centre would be centrally concerned with studying the vulnerabilities in both Australian and foreign networks and developments in viruses, worms,

'Trojan horses' and other threats to computer-based systems. Publicly acknowledged vulnerabilities in servers indicate promising routes for exploitation. In June 2001, for example, CERT reported a critical flaw in the Hypertext Transfer Protocol (HTTP) component of Cisco Internetwork Operating System (IOS) software using local authentication databases, which 'allows an intruder to execute privileged commands on Cisco routers' and to effectively take 'complete control' of affected systems.[35] In June 2006, multiple vulnerabilities were reported in certain versions of the Cisco Secure Access Control Server (ACS) for Windows, a key part of Cisco's 'trust and identity management framework' and a cornerstone of its Network Admission Control (NAC) system. Some of the vulnerabilities caused the ACS services to crash, while others allowed 'arbitrary code execution if successfully exploited'.[36]

The study of viruses and worms would be not merely for remedial or longer-term protective purposes, but even more importantly would inform the R&D of superior viruses and 'Trojan horses'—making them more malicious, or more selective, or more difficult to trace and diagnose, or less able to be fixed. Some recent examples are the VBS/Loveletter worm (appearing in 2000 and causing between US$5 and US$10 billion dollars in damage), which used a back-door 'Trojan horse'; the Code Red and Code Red II worms in 2001, which attacked the Index Server in Microsoft Internet Information Servers; the SQL Slammer worm, which attacked vulnerabilities in the Microsoft SQL Server; the Blaster worm, which exploited a vulnerability in Microsoft Windows systems; Sobig and MyDoom worms, which spread rapidly via emails; Witty, which exploited vulnerabilities in several Internet Security Systems (ISS); and Santy, a 'Web-worm' that exploited vulnerabilities in Google.[37] Systematic exploration of all known viruses would suggest the most lucrative avenues to explore.

Destructiveness is not necessarily the objective. Although there is a place in IO for relatively crude cyber-operations, such as defacement of websites and Denial of Service (DS) attacks, the most effective and successful cyber-warfare activities are those in which control of computer-related systems is taken without detection by the hosts. Covert corruption of databases, deception of sensor systems, and manipulation of situational awareness is much more likely to produce favourable strategic and tactical outcomes.

A Cyber-warfare Centre would be responsible for the preparation of contingency plans. These would include the development of various forms of 'Trojan horses' designed to surreptitiously corrupt data and files, and matched to particular national stock exchanges, power utilities, air traffic control systems and other information infrastructure; of plans for disabling and deceiving critical elements of military chains of command; and plans for targeting the computer, communications and electronic systems used by particular individuals and

agencies. Scenarios would be continually researched and techniques practised to ensure the currency of the plans in contingent circumstances.

A Cyber-warfare Centre would be responsible for identifying the preparations necessary for expeditious implementation of the plans, including the preparations for offensive operations. Some of this preparatory activity will involve the placement of taps on communications systems, of intercept equipment in microwave alleys, and of various electronic devices on antenna systems and communication junctures in foreign countries—to monitor communications, identify IPs and *pro formas*, collect local electronic emanations for the application of countermeasures, and to manipulate and deceive air defence and logistical systems. Devices could be implanted in radars and other sensor systems, or at junctures in their data-links. It is obviously easier to do this before crises or wars eventuate. A Cyber-warfare Centre would have to work very closely with designated ASIS or Special Forces elements with respect to these sorts of activities.

The proportion of both international and local telecommunications traffic being conveyed by fibre-optic cables has increased rapidly since the late 1980s, notwithstanding the increasing volume of mobile telephony connected by both satellite and terrestrial transponders. A rising proportion of voice telephony is being carried by the Internet, via cable, satellite and wireless, as Voice Over Internet Protocol (VOIP) communications. Current trans-oceanic fibre-optic cables typically have four or eight pair of fibre strands, each pair providing four channels, with a capacity of 10 Gigabits per second per channel. Systems have been demonstrated which can carry 14 Terabits per second (111 Gigabits per 140 channels) over a single optical fibre.[38] However, tapping fibre-optic cables is much more difficult than intercepting satellite or terrestrial microwave communications. It requires considerable expertise and specialised equipment, and direct access to the cables.

There are two approaches to tapping fibre-optic cables. One is to access the amplifier or repeater points which regenerate the signals, and which are typically every 160 km or so. This is relatively easy in older systems, which use opto-electronic repeater amplifiers. These convert the optical signals into electrical signals, clean and amplify them and then convert them back to optical for re-transmission; the signals can be intercepted by external induction collars during their electronic stage.[39]

More modern optical cable systems use Erbium [Er]-Doped Fibre Amplifiers (EDFA), in which the signal is boosted without having to be converted into electricity. At each EDFA repeater point there is a small internal tap that takes signals from the eastwards fibre and sends them back along the westwards fibre to let the cable operators diagnose cable fault points very accurately. These signals can be monitored by inserting tap couplers into the EDFAs, although care must be taken to avoid a voltage drop.

The second approach involves the 'scrape and bend method', in which a small piece of cladding is removed from one side of the cable, allowing a detectable amount of light to escape but not enough to alert the cable operators. The exposed fibre is placed in a special reader unit that slightly bends it so that some of the light is refracted (due to it hitting the glass close enough to the perpendicular), and a photon sensor or light detecting device then reads the escaping light. Dummy light packets may have to be inserted so that photon loss is not noticed.[40]

Transmission of the intercepted data is a formidable problem. A cable can be carrying hundreds of gigabits of data, or the equivalent of a hundred million telephone calls at a time. It requires prioritising, based on careful consideration of future intelligence requirements, as well as placement of equipment at the tap sites. The techniques involved include distinguishing the Synchronous Optical Network (SONET) frames that carry the multiplexed digital traffic; concentrating on selected IPs and other easily sorted packages; and using filters that filter terabits per second down to reasonable data level.

In 2005, the USS *Jimmy Carter*, one of the new *Seawolf* class of submarines, was extensively modified for a range of covert missions, including tapping undersea optical cables.[41] However, these missions are obviously extremely complex as well as very expensive.

Fortunately, signals are rarely conveyed by optical cable, let alone undersea cable, for the whole of their journey from sender to recipient. Undersea cables have landing points where they connect with satellite ground stations, terrestrial microwave relay stations, or other cable systems, which in turn often connect with mobile telephony or broad-band wireless transponders. The terminals, junctions and switching centres, as well as the Network Access Points (NAPs), now usually called Internet Exchange Points (IXPs), which serve as Internet exchange facilities, are more accessible and likely to be more lucrative than most undersea cables.

Offensive activities

Many of the posited functions of a Cyber-warfare Centre are already being performed, to a greater or less extent and with unsatisfactory coordination, by one or more of the organisations operating in the Defence intelligence or cyber-security areas. However, none of them has any mandate for the planning and preparation of offensive cyber-warfare activities. Offensive capabilities, represented by the strike capacity of the F-111s and important parts of the Army and RAN, are an essential feature of Australian strategic policy. They must be complemented by offensive NCW and cyber-warfare capabilities at the operational level.

The ADF has moved slowly to acknowledge the offensive dimension of NCW. *Force 2020*, the vision statement issued in 2002, stated that 'in the force of 2020, we will have transitioned from platform-centric operations to Network-Enabled Operations', and that the objective is 'to obtain common and enhanced battlespace awareness, and with the application of that awareness, deliver maximum combat effect'. It said that shared information 'allows a greater level of situational awareness, coordination, and offensive potential than is currently the case'.[42] This remained the only mention of the word 'offensive' in the public guidance for another five years, although in 2002–2003 the Knowledge Staff under the Chief Knowledge Officer argued that, among its transformational capabilities, NCW would provide 'an offensive information operations capability'.[43]

The 2007 *NCW Roadmap* also argued that a networked force would 'facilitate enhanced situational awareness, collaboration and offensive potential'. It described 'the offensive support system', which is 'predominantly based in the engagement grid [of the NCW architecture]', but which also 'combines aspects of the sensor and command and control (C2) grids while exploiting the information network to exchange information between all the grids'.[44]

However, this conception of offensive activities is essentially limited to Network-enabled operations which exploit networking to provide enhanced situational awareness, more informed targeting, and greater precision in weapons delivery. Indeed, the Knowledge Staff classed offensive NCW not only as 'effectors', but as 'weapons systems'.[45] It does not extend to the conduct of offensive cyber-warfare activities—hacking, disabling information infrastructures, disrupting chains of command and decision-making processes, corrupting databases and conducting sophisticated IW—which could well have at least as much impact on some conflict outcomes as more efficient and more effective application on conventional force.

Information Warfare and the intelligence process

IW, and cyber-warfare in particular, poses several new challenges for the intelligence community. The centrality of intelligence collection and analysis is enhanced. Timeliness becomes even more critical; indeed, analysis and assessment become conflated with operations. New intelligence skills are required.

The intelligence collection and processing stations, the EW centres and the cyber-warfare facilities will effectively be integrated. The intelligence centres disseminate the processed intelligence, collated from all sources (especially SIGINT and imagery intelligence (IMINT)) in real-time to the high command, subordinate headquarters and staffs, and to field units. The EW centres maintain catalogues of electronic order of battle (EOB) data about radar systems and other electronic emitters in prospective areas of operations. This includes data on the location of the emitters, their signal strengths and frequencies, the pulse width

and pulse length of the signals, and the physical descriptions of the emitting antenna system. The cyber-warfare centre is responsible for both offensive and defensive cyber-activities. It penetrates foreign computer networks, implants viruses, worms and 'Trojan horses', conducts DS attacks, defaces websites, sends misleading information, and disrupts or manipulates connected sensor and information systems.

These centres not only provide intelligence and EW and cyber-warfare capabilities to support the conventional functional and designated commanders; they are also *integrally* involved in the planning and conduct of operations. In future wars (including prospective phases in the 'war on terror'), the winners in the long-term will not necessarily be those who enjoy military success on the battlefields but those who win the information war. In many (but not all) contingencies, the IO units could well play more determinate roles than the conventional force elements. They are the essence of 'effects-based' operations.

NCW and IO have fundamental implications for the role and place of the intelligence process, although this was ignored in the Flood inquiry into Australia's intelligence agencies in 2004.[46] In IO activities, the intelligence process is categorically conflated with the conduct of operations. The role of intelligence changes from a staff agency to an instrumental service. The intelligence cycle becomes the definitive sequence in the operations themselves. In exemplary cases, remotely-controlled sensor systems serve as both intelligence sources and shooters.

This conflation is greatly facilitated by UAVs. Its essence was demonstrated in the use of a *Predator*, armed with *Hellfire* missiles, to hit a car in Yemen on 3 November 2002, killing its six occupants, including the al-Qaeda leader responsible for planning the attack on the USS *Cole* in October 2000.[47] The *Predator* was remotely-piloted from Djibouti, with the surveillance imagery relayed in real-time to a field user equipped with a remote video terminal and to the Central Intelligence Agency (CIA)'s headquarters in Virginia.[48]

The Defence intelligence agencies will have to be drastically reformed, and in parts substantially augmented, in order to perform their central role in NCW and IO/IW. They presently lack important technical capacities, and are surely incapable of providing the timely, accurate and insightful intelligence necessary, when operationalised through IW and cyber-warfare activities, to manipulate the policy-making and decisional processes of notional adversaries.

Command issues

Construction of an IW architecture, including a cyber-warfare component, raises numerous important organisational and command issues for the ADF. Networking will provide more direct sensor-to-shooter connections and enable a more flattened C2 structure. IO generally do not require, and indeed are likely to be

impeded by, the erstwhile hierarchical C2 structures of traditional armed forces. With all force elements digitised and connected with sufficient bandwidth, the high command and the 'front-line' IO units can work with a shared battlefield awareness; orders can be issued by the high command to the IO units directly and in real-time, without passing through intermediate echelons; and the IO units, with full appreciation of both the tactical and strategic dimensions, can operate with considerable autonomy from intermediary oversight.

Most IW involve several Services and Defence agencies, with (currently) complex, complicated and distributed command arrangements—as in the plausible IO mission scenario in which a *Collins*-class submarine embarks Special Forces and 'special intelligence' personnel to implant electronic devices in adversary communications, control, command and intelligence (C3I) systems to enable cyber-warriors, using UAVs for connectivity, to penetrate and take control of adversary networks, providing other ADF elements with unrestricted access to adversary telecommunications systems and airspace. Civilians would be integrally involved in the conduct of important operations, especially those involving cyber-warfare. DSTO will accrue new responsibilities, with large elements also directly involved in operations, as the 'wizard war' becomes real-time. New concepts and mechanisms are required for the utilisation of reserves and mobilisation of other civil resources (especially IT and super-computer resources).

Plausible operations could involve a cyber-warfare centre in Canberra working in direct support of air strikes by corrupting an adversary's air defence data, or supporting amphibious lodgements by confusing an adversary's sensor systems and response processes, or supporting counter-terrorist operations by temporarily disrupting electrical power in a particular locality, while depending on UAVs, submarines and Special Forces to provide access to the adversary's networks. Civilians would be involved in the actual conduct of operations, first, where particular hacking skills are required, and, second, to provide subject expertise. Experts on a foreign national financial system, or the key personalities and political processes in a foreign government, would literally sit next to the hackers, providing direction and advice as penetration is achieved, data surreptitiously distorted, effects modulated, and decisions effectively manipulated.

The issue of creating a Commander of Information Operations, at the equivalent level of the present functional or environmental commanders (i.e. 2-star), has been raised elsewhere.[49] The case will undoubtedly become increasingly compelling, as the role of IO not only as an enabler of more effective air, maritime and land operations but also as a determinant of conflict outcomes becomes more apparent, and other benefits with respect to IO planning, doctrine development and capability development become better appreciated. Operational command and control of a cyber-warfare centre would be simplified, as would

some of the tasking arrangements involving special operations units and platforms such as the submarines and UAVs.

A premium on *ante-bellum* activities

IO place a premium on the conduct of preparatory activities, inherently involving covert operations in peacetime. It is a process quite different to the planning and logistics preparations that are involved in conventional operations; it is more akin to the craft of the cryptanalyst.

Information Supremacy requires intimate familiarity with the intricacies of an adversary's C2 structure, public media, defence communications systems, sensor systems, and cyber-networks. It requires the maintenance of comprehensive, accurate and completely up-to-date EOB data for the design of ESM and ECM EW systems and application tactics. It requires detailed knowledge of the antenna systems and electronic equipment aboard adversary combatants (such as the avionics in aircraft) and installed in hardened command centres, in order to design EW, 'front-door', 'in-band' high-power microwave (HPM), and cyber-penetration techniques. Cyber-warriors must explore offensive cyber-warfare, in which software is developed for penetrating the firewalls in designated sectors (such as air traffic control and air defence networks); worms, viruses and 'Trojan horses' are developed, and plans are prepared and tested, for the corruption or disablement of websites and databases; and 'back-door' programs are installed in designated computer networks enabling data to be copied from files without detection, or the cyber-warfare centre to take control of the infected computers.

Much of this would be done in the Australian Cyber-warfare Centre itself, using airborne connectivity with the adversary's networks. However, the process would be greatly advantaged by the prior emplacement of various sorts of devices on adversary C3I systems—such as telephone exchanges, microwave relay towers, radar equipment, and even SATCOM ground control stations.

There are questions about Australia's willingness and capacity for engaging in *ante-bellum* activities, especially those involving identifiable penetrations of cyber-networks or physical implants of technical devices.

Rules of engagement, doctrine and operational concepts

The ROE for IW, including cyber-warfare, will have to be very different from those of traditional military operations. New doctrine will have to be promulgated. New 'laws of war' will have to be developed and accorded some international standing.

New ROE are required to accommodate the transient nature of some of the real-time intelligence available to the shooter and to remove intermediary command levels. For example, early in Operation *Enduring Freedom*, a *Predator*

UAV armed with *Hellfire* missiles, on a mission for the CIA, spotted 'a top Taliban leader' entering a building. The aircraft could have taken a shot at the building, but the CIA officials had to seek permission from US Central Command in Tampa, Florida, and by the time the military officials ordered a strike the Taliban leader had fled.[50]

New ROE are also required for those ADF elements that might be engaged in pre-emptive operations, covert operations, and offensive cyber-warfare activities. US military officials have said that clarifying the ROE for initiating computer network attacks has been 'a particularly thorny issue' in the Pentagon, 'due to larger political considerations, particularly to ensure that the attacks do not have any important unintended political ramifications or effects beyond the target'.[51] During the planning of Operation *Iraqi Freedom*, IO officers encountered opposition from 'the Pentagon's legal community', which was worried about the unintended effects of IO.[52] US officials have said that the activities of the *Compass Call* IW aircraft were determined, both preceding and during the war, partly by legal arguments (which determined that 'jamming a sovereign country is an act of war'), and that 'it was very difficult for us to get our hands around what we were authorized to do before the start of hostilities'.[53]

New operational concepts and doctrine will have to be developed for new areas of activity, especially those involving offensive cyber-warfare. For example, doctrine is required to define and exploit the 'intersection of information warfare and air defence suppression'. Special mission aircraft, such as the RC-135 *Rivet Joint*, can tap into enemy radar systems to 'see' what they are detecting—and hence instruct fighters to either press home or abort an attack.[54]

Some of this doctrine and associated ROE will have to be developed in the absence of any relevant international law. The killing of the al-Qaeda operatives by the *Predator* UAV in Yemen on 3 November 2002 raised troubling ethical questions. Swedish Foreign Minister Anna Lindh called it 'a summary execution that violates human rights'.[55]

The inherent transnational and non-State attributes of cyber-activities, confounding distinctions between external and internal security operations, pose not only new technical challenges but also contain new risks, in terms of both national vulnerabilities and threats to civil liberties. These have to be addressed in both national legislation and ROE.

Capability planning

The 2007 *NCW Roadmap* described the mechanisms through which the NCW Concept has now thoroughly infused the capability development process. All major capability proposals are now rigorously vetted from an NCW perspective, primarily focused on their 'level of connectivity and integration requirements', their IT vulnerabilities, and the potential contribution of their Combat

Information Systems to provide enhanced ISR capabilities and to enable more combat effect.[56]

A Cyber-warfare Centre would add a new and critically important dimension to this process. Major capability proposals have to have initiators and mentors. There has to be some place concerned with identification of long-term cyber-warfare requirements apart from critiquing the NCW aspects of other proposals. A Cyber-warfare Centre would provide an institutionalised advocate for funding and specialised equipment beyond the scope of the current process.

Some of the specialised requirements equipment will only become apparent after such a Centre has been functioning for a while. Much of it will consist of assorted miniature devices for implantation at various physical places in adversary networks, but there might also be major support platforms. UAVs offer extraordinary promise for both enhanced and precisely-targetable COMINT collection and penetration of networks exposed during microwave transmissions. The acquisition of a squadron of *Global Hawks* for SIGINT collection is a serious possibility within the next decade. There are programs to produce a version of the *Global Hawk* with a 3000 lb SIGINT payload, including COMINT capabilities. It might well be the case that three *Global Hawks* (with one on a continuous 36-hour station), equipped with various sorts of antenna systems, could provide comparable COMINT coverage to that of the first *Rhyolite* geostationary SIGINT satellites in the 1970s. Other configurations, focused on 'microwave alleys', could provide direct support for interactive cyber-warriors.

The costs of NCW and IO will not be trivial. The bandwidth requirements of NCW and IO are staggering. Advanced communications satellite systems will be necessary, using laser transmission and Internet routing to provide high-bandwidth connectivity.[57] The networks and servers used by Defence for Network-enabled operations have to be completely secured—not only against terrorists and other non-State actors, but also against the cyber-warfare activities of notional regional adversaries. Special operations units will have to be formed for covert activities, such as placement of devices in microwave relay facilities, optical cable networks, switching centres and air defence systems in particular countries. The construction of a Cyber-warfare Centre could well cost more than a billion dollars. However, this would be spread over many years, and could begin quite modestly, with more robust networking of various current activities and capabilities, and direction and coordination provided by a small core.

Location of a Cyber-warfare Centre

Location is a factor of organisational, technical and operational considerations. A Cyber-warfare Centre would be a national asset, serving grand strategy as much as tactical encounters. It would have to respond to direction from, report to, and interact with agencies at several levels. Its central role in operations has

to be reflected in ADF command arrangements. Robust connectivity with the rest of the NCW infrastructure and the NII is fundamental. The physical proximity of all its components is not necessary, so long as functional coordination and cooperation can be organised. Networking enables elements to be distributed, across agencies and geographically. There will inevitably be offices in more than one place, as well as out-rider units in high-tech centres such as the Salisbury/Edinburgh area in north Adelaide.

A Cyber-warfare Centre would have at least two new elements that would require accommodation. One comprises the executive, coordination, planning and management functions, which extend across the whole of government. This is the purview of the National Security Division of the Department of the Prime Minister and Cabinet (DPM&C), which has a mandate 'to foster greater coordination of, and a stronger whole-of-government policy focus on, national security' and which has greatly strengthened the whole-of-government approach to counter-terrorism. There are many aspects of cyber-warfare that require coordination at a national level. This includes all cyber-activities aimed at influencing adversary political and strategic agencies and processes. Covert operations in peacetime must be endorsed at this level because of the risks and consequences of possible exposure. In time of war, the whole-of-government approach would be a crucial feature of the simultaneous application and progressive interaction of kinetic and cognitive effects.

The second element is the operational facility, the place where the cyber-warriors would work. Technical intelligence collection stations, EW centres and cyber-warfare capabilities will remain dispersed, but a place devoted to cyber-operations would promote interaction of the specialist personnel in these areas, where close cooperation is not only essential to operational success, but is likely to encourage future technical advances at the interstices.

It is important to have a place where defensive and much-enhanced offensive activities are co-located. Those working on defensive matters need to keep the offensive planners apprised of the avenues they are finding most difficult to protect. Those working on offensive plans should obviously keep the defensive side informed as they discover potential vulnerabilities in national systems while exploring avenues to exploit. The symbiosis should enhance the security, reliability, capacity and endurance of national networks while maximising the potency and perniciousness of Australia's cyber-warfare capabilities against hostile systems.

The question of location is complicated by the decision to locate the Headquarters Joint Operations Command (HQJOC) near Bungendore, 29 km east of Canberra (and about 28 minutes to drive), rather than at HMAS *Harman* or somewhere else close to the Defence complex at Russell Hill. An obvious place would be in or near the DSD building—the main centre for the collection,

processing and analysis of intercepted telecommunications, the main repository of certain specialised cyber-skills, the manager of some of the most secure networks in the world, and the national agency responsible for the defensive cyber-warfare mission, protecting the Australian Government's communications and information systems. However, a component element will now have to be located at Bungendore to serve the Chief of Joint Operations (CJOPS), requiring some bifurcation of the Cyber-warfare Centre and very difficult decisions about which capabilities and activities to maintain at Russell Hill and which to repose at Bungendore.

A component element might also be located at HMAS *Harman*, 11.4 km southeast of Russell Hill (and 19 minutes to drive). It hosts the Defence Network Operations Centre (DNOC), the hub of the third largest communications network in Australia after Telstra and Optus, which provides network support for military operations. The operational elements of the DNOC include the Naval Communications Station Canberra (NAVCOMMSTA), which provides UHF satellite services in support of the RAN and other ADF users; the Naval Communications Area Master Station Australia (NAVCAMSAUS) which supports RAN fleet communications; and the Defence Information Systems Communications Element (DISCE), which provides a secure and survivable communications network to support strategic and tactical operations of the ADF and selected Government departments. Under Project JP 2008 (Phase 3F), a new ground station is to be constructed at HMAS *Harman*, together with two new terminals at the Defence communications station at Geraldton, to upgrade 'the entire Australian Defence Satellite Communications Capability (ADSCC) Ground Segment'.[58]

The HQJOC will have a dedicated fibre-optic cable extending 27 km to the DNOC at HMAS *Harman*. Redundancy will be provided by 'four links into the local carrier network'. The facility will also have 'a back-up satellite link'.[59]

Regional developments

Over the past decade or so, responding to either the Revolution in Military Affairs (RMA) or to the challenges and opportunities of the Internet, many countries have established cyber-warfare organisations of some sort or another. Some of them are attached to national intelligence agencies or Defence Ministries, while others function as part of military command structures. The United States has a variety, spawned by the National Security Agency (NSA), the CIA, the Federal Bureau of Investigation (FBI) and the Department of Homeland Security (DHS) in Washington. In 2000, the US Space Command was given responsibility for both Computer Network Defence (CND) and Computer Network Attack (CNA) missions. After the Space Command was merged into the US Strategic Command (USSTRATCOM) in June 2002, several new organisations were established for planning and conducting cyber-warfare, including the Joint Functional

Component Command for Network Warfare (JFCC-NW), responsible for 'deliberate planning of network warfare, which includes coordinated planning of offensive network attack'; the Joint Functional Component Command for Space and Global Strike (JFCC-SGS), which also houses the Joint Information Operations Warfare Center (JIOWC), responsible 'for assisting combatant commands with an integrated approach to information operations'; and the Joint Task Force for Global Network Operations (JTF-GNO), which has responsibility for Department of Defense cyber-security.[60] The US Navy established a Naval Network Warfare Command (NNWC) at Norfolk in Virginia in July 2002. The US Air Force established a new Cyberspace Command at Barksdale Air Force Base in Louisiana in June 2007, 'already home to about 25 000 military personnel involved in everything from electronic warfare to network defence'.[61] IW teams deploy with combatant commands. Interoperability with the US cyber-warfare architecture requires appropriate institutional arrangements on the part of US allies.

Asia has emerged as the 'early proving ground' for cyber-warfare'.[62] This is especially the case in Northeast Asia, where cyber-warfare activities have become commonplace. China has the most extensive and most tested cyber-warfare capabilities, although the technical expertise is very uneven. China began to implement an IW plan in 1995, and since 1997 has conducted several exercises in which computer viruses have been used to interrupt military communications and public broadcasting systems. In April 1997, a 100-member elite corps was established by the Central Military Commission to devise 'ways of planting disabling computer viruses into American and other Western C2 defence systems'.[63] In 2000, China established a strategic IW unit (which US observers have called 'Net Force') designed to 'wage combat through computer networks to manipulate enemy information systems spanning spare parts deliveries to fire control and guidance systems'.[64]

Chinese cyber-warfare units have been very active, although it is often very difficult to attribute activities originating in China to official agencies or private 'netizens'. Since 1999, there have been periodic rounds of attacks against official websites in Taiwan, Japan and the United States. These have typically involved fairly basic penetrations, allowing websites to be defaced or servers to be crashed by DS programs. More sophisticated 'Trojan horse' programs were used in 2002 to penetrate and steal information from the Dalai Lama's computer network.[65] 'Trojan horse' programs camouflaged as Word and PowerPoint documents have been inserted in computers in government offices in several countries around the world.[66] Portable, large-capacity hard disks, often used by government agencies, have been found to carry 'Trojan horses' which automatically upload to Beijing websites everything that the computer user saves on the hard disk.[67] Since the late 1990s, the People's Liberation Army (PLA) has conducted more

than 100 military exercises involving some aspect of IW, although the practice has generally exposed substantial shortfalls.[68]

It has recently been reported that Chinese 'cyber-espionage' activities have been conducted against 'key Australian Government agencies'. According to media reports in February 2008, 'Chinese computer hackers have launched targeted attacks on classified Australian Government computer networks', and that China is 'believed to be seeking information on subjects such as military secrets and the prices Australian companies will seek for resources such as coal and iron ore'. The Chinese activities have reportedly prompted an official review of IT security'.[69]

In August 1999, following a spate of cross-Strait attacks against computer networks and official websites in Taiwan, the Minister for National Defense (MND) in Taipei announced that the MND had established a Military Information Warfare Strategy Policy Committee and noted that 'we are able to defend ourselves in an information war'.[70] In January 2000, the Director of the MND's Communication Electronics and Information Bureau announced that the Military Information Warfare Strategy Policy Committee had 'the ability to attack the PRC with 1,000 different computer viruses'.[71] In August 2000, Taiwan's *Hankuang* 16 defence exercise included training in cyber-warfare, in which more than 2000 computer viruses were tested. Two teams of cyber-warriors used the viruses in simulated attacks on Taiwan's computer networks.[72] In December 2000, the MND's Military Information Warfare Strategy Policy Committee was expanded and converted into a battalion-size centre under the direct command of the General Staff Headquarters, and with responsibilities for network surveillance, defence, and countermeasures.[73] In its *2002 National Defense Report*, released in July 2002, the MND for the first time included discussion of 'electronic and information warfare units'. It proclaimed Taiwan's commitment to the achievement of 'superiority [over the PRC] in information and electronic warfare', and it ranked EW and IW ahead of air and sea defence in terms of current MND focus. It specifically cited such threatening developments by the PRC as 'Internet viruses, killer satellites, [and] electromagnetic pulses that could fry computer networks vital to Taiwan's defence and economy'.[74]

Japan was surprisingly laggard about developing cyber-warfare capabilities. In April 1999, faced with a growing problem of cyber-crime (involving offences such as computer-based fraud, on-line sales of illegal drugs, and transmission of pornography), the National Police Agency set up a 'special unit of cyber-sleuths … who specialise in investigating computer-related crimes and cyber-terrorism'.[75] A 'specialised anti-hacker task force' was set up on 21 January 2000, but it was quickly shown to be impotent. Two days later there began an intense spate of attacks on Japanese government websites, probably

triggered by denials by right-wing Japanese that Japanese troops had massacred Chinese civilians when they seized Nanjing in 1937.[76]

In May 2000, Japan announced plans to establish a Research Institute and an operational unit for fighting cyber-terrorism. The announcement was prompted by further sporadic hacking attacks. Some of these involved a 'cyber war between netizens of South Korea and Japan' over Japanese claims to the disputed Tok-do islets.[77] It also followed revelations in March 2000 that the *Aum Shinri Kyo* (Supreme Truth) sect (responsible for the sarin gas attack in the Tokyo subway in March 1995) had written computer software used by police agencies, which had enabled cult members to obtain secret data on police patrol cars, as well as other software which allowed them access to data on the repairs and inspections of several nuclear power plants.[78]

In July 2000, the Japan Defense Agency (JDA)'s[79] *Defense of Japan 2000* acknowledged, for the first time, the threat posed by IW. It noted that 'there is a greater possibility that invasion and tampering with computer systems by hackers will affect our life immensely', that 'a new computer security base will be established', that facilities would be developed for operational evaluation of computer security systems and techniques, and that JDA personnel would be dispatched to the United States to develop computer security expertise. It also noted that JDA officials contribute to the 'Action Plan for Building Foundations of Information Systems Protection from Hackers and Other Cyberthreats' by 'studying measures against hackers and cyber-terrorism'.[80] It was reported in October 2000 that the JDA's 'cyber-squad' was developing software capable of launching anti-hacking and anti-virus attacks and of destroying the computers of hackers trying to penetrate Japan's defence networks.[81]

South Korea has evidently also moved to establish a cyber-warfare capability. The number of attacks on South Korean commercial and government websites increased markedly during 2000 (partly reflecting the 'cyber-war' with Japanese 'netizens'). The South Korean MND and the National Intelligence Service (NIS) both reported during 2000 that the South Korean armed forces should 'prepare for cyber-warfare in the future from enemy countries' and that they should consider establishing 'specialist units for cyber-warfare'.[82] A National Cyber Security Center attached to the NIS was functioning by 2004.[83]

Even North Korea, the most backward country in East Asia in IT terms, reportedly set up a cyber-warfare unit in the late 1980s. Media reports actually refer to two different places, but these may be different elements of the one agency. An electronic communications monitoring and computer hacking group from the State Security Agency is reportedly located at the Korea Computer Centre in Pyongyang.[84] The North Korean Army created a dedicated cyber-warfare unit, called Unit 121, in 1998. Its staff is estimated to include from 500 to more than 1000 'hackers'. Its capabilities include 'moderately advanced

Distributed Denial of Service (DDS) capability' and 'moderate virus and malicious code capabilities'. In October 2007, North Korea tested a 'logic bomb' containing malicious code designed to be executed should certain events occur or at some pre-determined time; the test led to a UN Security Council (UNSC) resolution banning sales of mainframe computers and lap-top personal computers (PCs) to North Korea.[85] North Korea also uses cyber-space extensively for its propaganda or psychological warfare campaigns.[86]

In Southeast Asia, Singapore has both the leading IT industries and the most advanced cyber-warfare capabilities. Singapore's defence hierarchy 'is committed to the development of an offensive cyber-warfare capability'.[87] The Ministry of Defence and the Singapore Armed Forces initiated a Cyberspace Security Project in the mid-1990s to develop 'countermeasures which respond automatically to attacks on their computer systems'.[88] A dedicated cyber-warfare unit is thought to have been established within the Ministry of Defence, and methods for inserting computer viruses into other countries' computer networks have been developed.[89]

This is not the place to evaluate these regional agencies. They include many different sorts or organisations with wide-ranging responsibilities, not all of them necessarily relevant to Australia's circumstances. They operate in secret. Little is publicly known about them, and this is suffused with misinformation and disinformation. However, they have each accumulated experiences of one sort or another, developed practical and forensic skills, acquired equipment, and undertaken operations with counterpart civilian or military authorities to a greater or lesser extent. This accrual derives from bureaucratic institutionalisation and provides a basis from which 'asymmetric' surprises can be launched. They can only be systematically monitored and countered in institutionalised fashion.

Conclusion

The lack of a Net-war or Cyber-warfare Centre is becoming a critical deficiency in Australia's evolving architecture for achieving and exploiting Information Superiority and Support (IS&S) beyond around 2020. Australia has a plethora of organisations, within and outside Defence, concerned with some aspect 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, 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 a 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, including new systems and support platforms for accessing adversary IPs and computer-to-computer *pro formas*. It would task special operations units both for covert preparatory missions in peacetime and during the conduct of offensive IO in conflict situations.

The 2007 *NCW Roadmap* reflected substantial progress with the institutionalisation of NCW perspectives within Defence; however, it also showed, at least implicitly, that vitally important activities are inadequately attended by current structures and processes, and that some sort of Cyber-warfare Centre is best able to address these potentially debilitating deficiencies. Networked databases are useless if the data can be corrupted, providing confusing or misleading information, or if decision-makers lose confidence in them. Expansive networking, incorporating more databases, involving more carriers, and connecting with many more customers, can increase network vulnerabilities; there are more access points for hostile intruders, and more data-links that can be disrupted. Shared and enhanced situational awareness is a superlative 'force multiplier', but it can be disastrous if it is subject to surreptitious manipulation.

The current capability development process ensures that key NCW criteria are examined with respect to all prospective acquisitions, including the levels of connectivity and security, and their contribution to ISR missions, thus increasing the potency of new acquisitions. However, there is no endorsed vision of any notional ADF IW architecture for the period beyond 2020 which can ensure that the sorts of capabilities currently being acquired or being proposed for acquisition are the optimal components of that architecture; there is no agency committed to ensuring that all the requisites for effective cyber-warfare (including equipment) will be in place (which will only become apparent through the plans and activities of some Cyber-warfare Centre).

Furthermore, the 2007 *NCW Roadmap* portrays a severely delimited concept of offensive cyber-operations. It alluded to the central place of the 'offensive support system' in the ADF's NCW architecture. However, its scope is essentially confined to enablement of increases in the combat power of ADF units (through enhanced situational awareness, speedier decision-making, and more precise and more tailored application of force). There is no evident appreciation of the role of offensive cyber-warfare in influencing conflict outcomes quite apart from (but carefully coordinated with) enhanced combat power.

The establishment of an Australian Cyber-warfare Centre has now become a matter of considerable urgency. It is essential for it to be established soon to ensure that Australia will have the necessary capabilities for conducting technically and strategically sophisticated cyber-warfare activities by about 2020.

Several basic issues require considerable further debate, including the best location for a Centre, its organisation and staffing arrangements, its core functions and initial terms of reference, and its ADF command relationships. Some matters will only be resolved once the Centre has been functioning for several years, including some of the command relationships and some of the specialised equipment requirements. Assuming a decision to establish an Australian Cyber-warfare Centre was to be made by 2010, an initial operational capability could be assembled within a couple of years; however, it would not be able to perform all of its ascribed functions, especially those that require the development or acquisition of new capabilities and/or the placement of assorted devices overseas, much before about 2018. This means that an informed and vigorous debate on these issues should be encouraged as soon as possible.

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] Department of Defence, *The Australian Approach to Warfare*, Department of Defence, Canberra, June 2002, available at <http://www.defence.gov.au/ publications/taatw.pdf>, accessed 4 March 2008. See also Waters and Ball, *Transforming the Australian Defence Force (ADF) for Information Superiority*.

[3] Department of Defence, *Force 2020*, Department of Defence, Canberra, 2002, p. 19, available at <http://www.defence.gov.au/publications/f2020.pdf>, accessed 4 March 2008.

[4] Australian Defence Headquarters, *Enabling Future Warfighting: Network Centric Warfare*, ADDP-D.3.1, Australian Defence Headquarters, Canberra, February 2004, available at <http://www.defence.gov.au/strategy/fwc/documents/ NCW_Concept.pdf>, accessed 4 March 2008.

[5] Director General Capability and Plans, *NCW Roadmap 2007*, Defence Publishing Service, Canberra, February 2007, available at <http://www.defence.gov.au/capability/ncwi/docs/2007NCW_Roadmap.pdf>, accessed 4 March 2008.

[6] Cameron Stewart, 'Telstra Operation Helped Track Down Bali Bombers', *Australian*, 7 October 2006, p. 8, on-line version entitled 'Telstra Secretly helped Hunt Bali Bombers' at <http://www.news.com.au/story/0,23599,20537904-2,00.html>, accessed 4 March 2008; and Martin Chulov, 'A Win Against Terror', *Australian*, 7 October 2007, p. 17, available at <http://www.theaustralian.news. com.au/story/0,20867,20536940-5001561,00.html>, accessed 4 March 2008.

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

[8] 'Budget 2001-2002 Fact Sheet. Protecting the National Information Infrastructure: Part of the Government's E-security Initiative', Attorney-General's Department.

[9] Attorney-General, Minister for Communications, Information Technology and the Arts, and Minister for Defence, 'Security in the Electronic Environment', Joint News Release, 27 September 2001; and 'Budget 2001-2002 Fact Sheet. Protecting the National Information Infrastructure: Part of the Government's E-security Initiative', Attorney-General's Department.

[10] Attorney-General, Minister for Communications, Information Technology and the Arts, and Minister for Defence, 'Security in the Electronic Environment'; and 'Budget 2001-2002 Fact Sheet. Protecting the National Information Infrastructure: Part of the Government's E-security Initiative'.

[11] Director General Capability and Plans, *NCW Roadmap 2007*, p. 19.

[12] James Bamford, *Body of Secrets: How America's NSA and Britain's GCHQ Eavesdrop on the World*, Century, London, 2001, p. 480.

[13] Desmond Ball, *Australia's Secret Space Programs*, Canberra Papers on Strategy and Defence no. 43, Strategic and Defence Studies Centre, The Australian National University, Canberra, 1988, chapter 3.

[14] Desmond Ball, 'Silent Witness: Australian Intelligence and East Timor', in Richard Tanter, Desmond Ball and Gerry van Klinken, *Masters of Terror: Indonesia's Military and Violence in East Timor*, Rowman & Littlefield, New York, 2006, pp. 177–201.

[15] Ball, *Australia's Secret Space Programs*, chapter 4.

[16] Jeffrey Richelson, 'Desperately Seeking Signals', *Bulletin of the Atomic Scientists*, vol. 56, no. 2, March/April 2000, pp. 47–51.

[17] 'Infosec', Defence Signals Directorate, available at <http://www.dsd.gov.au/infosec/>, accessed 4 March 2008.

[18] See Desmond Ball, *Signals Intelligence in the Post-Cold War Era: Developments in the Asia-Pacific Region*, Institute of Southeast Asian Studies, Singapore, 1993, p. 83.

[19] Ball, *Signals Intelligence in the Post-Cold War Era: Developments in the Asia-Pacific Region*, p. 83.

[20] Major John Blaxland, 'On Operations in East Timor', *Australian Army Journal*, 2000, pp. 7, 9.

[21] Defence Science and Technology Organisation, 'Network-Centric Warfare', available at <http://www.dsto.defence.gov.au/research/4051/page/4387/>, accessed 4 March 2008. See also Tim McKenna, Terry Moon, Richard Davis and Leoni Warne, 'Science and Technology for Australian Network-Centric Warfare: Function, Form and Fit', *ADF Journal*, no. 17, pp. 62–75.

[22] Arthur Filippidis, Tan Doan and Brad Tobin, 'Net Warrior—DSTO Battlelab Interoperability', Simulation Industry Association of Australia, June 2007, available at <http://www.siaa.asn.au/simtect/2007/Abstracts/70.html>, accessed 4 March 2008.

[23] 'Increased Telephone Interception Capacity', in Australian Federal Police, *National Illicit Drug Strategy Initiatives, November 1997—April 2001* (Second edition), p. 13, available at <http://www.afp.gov.au/__data/assets/pdf_file/6634/nids.pdf>, accessed 4 March 2008.

[24] Philip Cornford and Rob O'Neill, 'Bali Nine Phone Cards Cracked', *Age*, 4 May 2005.

[25] 'Telecommunications Interception Law Dispute Shows Law Needs Overhaul', *Electronic Frontiers Australia*, 31 March 2004, available at <http://www.efa.org.au/Publish/PR040331.html>, accessed 4 March 2008.

[26] See Australian High Tech Crime Centre website at <http://www.ahtcc.gov.au/about_us/index.htm>, accessed 4 March 2008.

[27] Robert Milliken, 'Canberra Acts to Keep an Eye on its Spies', *Independent* (London), 2 June 1995, available at <http://findarticles.com/p/articles/mi_qn4158/ is_19950602/ai_n13986087>, accessed 4 March 2008.

[28] Trevor W. Mahony, 'A Hybrid Civilian/Military Payload to Support Battlefield Communications', *Journal of Battlefield Technology*, vol. 1, no. 1, March 1998, pp. 29–32.

[29] 'Optus Positions for National Satellite Success', December 2001, available at <http://www.optus.net.au/portal/site/aboutoptus/menuitem.813c6f701cee5a14f0419f108c8ac7a0/?vgnextoid=a7ab8336054f4010VgnVCM1000009fa87c0aRCRD&vgnextchannel=b93cfaf924954010VgnVCM10000029a67c0aRCRD&vgnextfmt=default>, accessed 4 March 2008.

[30] Chulov, 'A Win Against Terror'.

[31] CISCO, 'Optus Charts Future with Cisco Service Oriented Network at Macquarie Park Campus', 19 October 2006, available at <http://newsroom.cisco.com/dlls/global/asiapac/news/2006/pr_10-19.html>, accessed 4 March 2008.

[32] 'CISCO Security Advisories', available at <http://www.cisco.com/en/US/products/products_security_advisories_listing.html>, accessed 4 March 2008.

[33] See the AusCERT website at <http://www.auscert.org.au/>, accessed 4 March 2008.

[34] 'DSTO and ADI Forge New Links in Network Centric Warfare', Defence Science and Technology Organisation, 2 September 2004, available at <http://www.dsto.defence.gov.au/news/3283/>, accessed 4 March 2008.

35 CERT, 'CERT Advisory CA-2001-14 Cisco IOS HTTP Server Authentication Vulnerability', 28 June 2001, available at <http://www.cert.org/advisories/CA-2001-14.html>, accessed 4 March 2008.

36 Kevin McLachlan, 'Flaw Found in Cisco Secure Access Control Server', 26 June 2006, available at <http://www.crn.com/it-channel/189601708>, accessed 4 March 2008; and 'Multiple Vulnerabilities in Cisco Secure Access Control Server', 7 January 2007, available at <http://www.securiteam.com/securitynews/5DP0420KAG.html>, accessed 4 March 2008.

37 'Timeline of Notable Computer Viruses and Worms', Wikipedia, available at <http://en.wikipedia.org/wiki/Timeline_of_notable_computer_viruses_and_ worms>, accessed 4 March 2008.

38 Frank W. Kerfoot and William C. Marra, 'Undersea Fiber Optic Networks: Past, Present, and Future', *IEEE Journal on Selected Areas in Communications*, vol. 16, no. 7, September 1998, pp. 1220–25, available at <http://ieeexplore.ieee.org/iel4/ 49/15642/00725191.pdf?arnumber=725191>, accessed 4 March 2008; and '14 Tbps Over a Single Optical Fiber: Successful Demonstration of World's Largest Capacity', *NTT Press Release*, 29 September 2006, available at <http://www.ntt.co.jp/news/news06e/0609/060929a.html>, accessed 4 March 2008.

39 Stephen Cass, 'Listening In', *IEEE Spectrum Special Report on Intelligence and Technology*, vol. 40, no. 4, April 2003, pp. 32–37, available at <http://www.estig.ipbeja.pt/ ~lmgt/st/other/Listening%20In.pdf>, accessed 4 March 2008; and 'NSA Tapping Underwater Fiber Optics', available at <http://slashdot.org/articles/01/05/23/2142216.shtml>, accessed 4 March 2008.

40 John R. Freer, *Computer Communications and Networks*, UCL Press, University College London, London, 2nd edition, 1996, p. 305.

41 Cass, 'Listening In', pp. 33–37.

42 Department of Defence, *Force 2020*, p. 19.

43 Gary Waters, 'Australia's Approach to Network Centric Warfare', in Waters and Ball, *Transforming the Australian Defence Force (ADF) for Information Superiority*, p. 14.

44 Director General Capability and Plans, *NCW Roadmap 2007*, p. 5.

45 Gary Waters, 'Australia's Approach to Network Centric Warfare', p. 14.

46 See Philip Flood, *Report of the Inquiry into Australia's Intelligence Agencies*, Canberra, July 2004, available at <http://www.pmc.gov.au/publications/ intelligence_inquiry/index.htm>, accessed 4 March 2008.

47 Vince Crawley and Amy Svitak, 'Is Predator the Future of Warfare?', *Defense News*, 11–17 November 2002, p. 8.

48 Craig Hoyle and Andrew Koch, 'Yemen Drone Strike: Just the Start?', *Jane's Defence Weekly*, 13 November 2002, p. 3.

49 Desmond Ball, 'Information Operations and Information Superiority', in Waters and Ball, *Transforming the Australian Defence Force (ADF) for Information Superiority*, p. 61.

50 Gail Kaufman, 'New Eyes, New Rules', *Defense News*, 2–8 December 2002, pp. 1–2.

51 Andrew Koch, 'New Powers for Info Operations Chiefs', *Jane's Defence Weekly*, 17 September 2003, p. 6.

52 Robert Wall, 'Focus on Iraq Shapes Electronic, Info Warfare', *Aviation Week & Space Technology*, 4 November 2002, p. 34.

53 Andrew Koch, 'Information Warfare Tools Rolled Out in Iraq', *Jane's Defence Weekly*, 6 August 2003, p. 7.

54 David A. Fulghum, 'Infowar to Invade Air Defense Networks', *Aviation Week & Space Technology*, 4 November 2002, p. 30.

55 Crawley and Svitak, 'Is Predator the Future of Warfare?', p. 8.

56 Director General Capability and Plans, *NCW Roadmap 2007*, p. 21.

57 Henry S. Kenyon, 'Networking Moves Into the High Frontier', *SIGNAL*, April 2004, pp. 59–62.

58 'Projects: JP 2008 Phase 3F—ADF SATCOM Capability Terrestrial Upgrade', 9 March 2007.

59 Department of Defence, *Executive Summary. Draft Environmental Impact Statement (EIS): Defence Headquarters Australian Theatre*, Department of Defence, Canberra, September 2003, p. ES-8.

60 Clay Wilson, *Information Operations and Cyberwar: Capabilities and Related Policy Issues*, Congressional Research Service, Library of Congress, Washington, DC, 14 September 2006, p. 8, available at <http://www.fas.org/irp/crs/RL31787.pdf>, accessed 4 March 2008.

[61] Alex Spillius, 'America Prepares for Cyber War with China', *Telegraph* (London), 15 June 2007, available at <http://www.telegraph.co.uk/news/ main.jhtml?xml=/news/2007/06/15/wcyber115.xml>, accessed 4 March 2008.

[62] Charles Bickers, 'Cyberwar: Combat on the Web', *Far Eastern Economic Review*, 16 August 2001, p. 30.

[63] Ivo Dawnay, 'Beijing Launches Computer Virus War on the West', *Age* (Melbourne), 16 June 1997, p. 8.

[64] Jason Sherman, 'Report: China Developing Force to Tackle Information Warfare', *Defense News*, 27 November 2000, pp. 1 and 19.

[65] Christopher Bodeen, 'Mainland Asks Taiwan to Stop Interference', *Washington Times*, 26 September 2002; and Doug Nairne, 'State Hackers Spying On Us, Say Chinese Dissidents', *South China Morning Post*, 18 September 2002, available at <http://www.infosyssec.com/securitynews/0209/6536.html>, accessed 4 March 2008.

[66] See, for example, 'Outrage in Berlin Over Chinese Cyber Attacks', 31 August 2007, available at <http://www.weeklystandard.com/weblogs/TWSFP/ 2007/08/outrage_in_berlin_over_chinese.asp>, accessed 4 March 2008.

[67] Yang Kuo-wen, Lin Ching-chuan and Rich Chang, 'Bureau Warns on Tainted Discs', *Taipei Times*, 11 November 2007, p. 2, available at <http://www.taipeitimes.com/ News/taiwan/archives/2007/11/11/2003387202>, accessed 4 March 2008.

[68] I-Ling Tseng, *Chinese Information Warfare (IW): Theory Versus Practice in Military Exercises (1996–2005)*, MA Sub-thesis, Graduate Studies in Strategy and Defence, Strategic and Defence Studies Centre, The Australian National University, Canberra, March 2005.

[69] 'Chinese Cyber Espionage "Routine" in Australia', *Canberra Times*, 11 February 2008, p. 5.

[70] 'MND Sets Up Information Warfare Committee', *ADJ News Roundup*, August 1999, p. 14.

[71] Francis Markus, 'Taiwan's Computer Virus Arsenal', *BBC News*, 10 January 2000, available at <http://news.bbc.co.uk/1/hi/world/asia-pacific/597087.stm>, accessed 4 March 2008; and Wendell Minnick, 'Taiwan Upgrades Cyber Warfare', *Jane's Defence Weekly*, 20 December 2000, p. 12.

[72] 'Taiwan to Conduct Cyber Warfare Drills', *Jane's Defence Weekly*, 16 August 2000, p. 10; Minnick, 'Taiwan Upgrades Cyber Warfare', p. 12; and Damon Bristow, 'Asia: Grasping Information Warfare?', *Jane's Intelligence Review, December 2000*, p. 34.

[73] Minnick, 'Taiwan Upgrades Cyber Warfare', p. 12.; and Darren Lake, 'Taiwan Sets Up IW Command', *Jane's Defence Weekly*, 10 January 2001, p. 17.

[74] Ministry of National Defense, *Republic of China, 2002 National Defense Report*, Ministry of National Defense, Taipei, July 2002. See also 'Taiwan Prepares for Cyber Warfare', *CNN.Com*, 29 July 2002; and 'Taiwan Report Finds Cyberthreat From China', *International Herald Tribune*, 30 July 2002.

[75] Chester Dawson, 'Cyber Attack', *Far Eastern Economic Review*, 10 February 2000, p. 21.

[76] Dawson, 'Cyber Attack'; and 'Japan/Crime: Cyber-terror Task Force Established', *Bangkok Post*, 27 January 2000, p. 6.

[77] 'Tokyo's Claim to Tok-do Escalates Korea-Japan Cyber War', *Korea Times*, 14 May 2000.

[78] Elaine Lies, 'Doomsday Cult Casts Shadow Over Japan', *Canberra Times*, 20 March 2000, p. 7.

[79] On January 2007, the Japan Defense Agency was upgraded to a Cabinet-level ministry, and is now known as the Japanese Ministry of Defense.

[80] Japan Defense Agency, *Defense of Japan 2000*, Japan Defense Agency, Tokyo, 2000, chapter 3, section 3(ii), and chapter 4, section 5(3). See also Damon Bristow, 'Asia: Grasping Information Warfare?', pp. 34–35.

[81] Juliet Hindell, 'Japan Wages "Cyber War" Against Hackers', 24 October 2000, *Internet Security News*, available at <http://www.landfield.com/isn/mail-archive/2000/Oct/0116.html>, accessed 4 March 2008.

[82] Bristow, 'Asia: Grasping Information Warfare?', p. 35.

[83] 'North Korea Ready to Launch Cyber War: Report', Computer Crime Research Center, 4 October 2004, available at <http://www.crime-research.org/news/04.10.2004/ North_Korea_ready_to_launch_cyber_war/>, accessed 4 March 2008.

[84] John Larkin, 'Preparing for Cyberwar', *Far Eastern Economic Review*, 25 October 2001, p. 64.

[85] Kevin Coleman, 'Inside DPRK's Unit 121', DefenseTech.org. 24 December 2007, available at <http://www.defensetech.org/archives/003920.html>, accessed 4 March 2008. See also 'North Korea

Operating Computer-hacking Unit', *Korea Herald*, 28 May 2004, available at <http://www.asiamedia.ucla.edu/article-eastasia.asp?parentid+11559>, accessed 4 March 2008.

[86] 'North Korea's Information Technology Advances and Asymmetric Warfare', *WMD Insights*, April 2006, available at <http://www.wmdinsights.org/ I4/EA1_NorthKoreaInfoTech.htm>, accessed 4 March 2008.

[87] Bristow, 'Asia: Grasping Information Warfare?', p. 36.

[88] Tim Huxley, *Defending the Lion City: The Armed Forces of Singapore*, Allen & Unwin, Sydney, 2000, p. 91.

[89] Bristow, 'Asia: Grasping Information Warfare?', p. 36.