Cyber Defence and Warfare

Desmond Ball and Gary Waters

The 2013 Defence White Paper includes security against major cyber attacks on Australia as an element of our 'defence of Australia' national strategic interest. It devotes a separate section to cyber in its strategic outlook. While the White Paper makes heartening comment about the need to integrate cyber power into national strategy, it provides no insights into how this might be achieved, nor does it set any real strategic direction for an improved whole-of-nation effort. It does not attempt to identify any cyber objectives that should underpin Australia's national security strategy. Australia needs to develop a current baseline cyber posture, derive a consolidated view of all requirements and gaps, and develop future remediation and implementation plans in an integrated fashion. Without this, cyber capability gaps across the Australian Government will continue to hinder the agencies' ability to plan for and conduct effective operations. Accordingly, this article calls for a comprehensive capabilities-based assessment, a national cyber capability plan, and an implementation plan (with specific actions and implementation responsibilities, timeframes, and performance measures) and a funding strategy for addressing any gaps resulting from the assessment. It also calls for a clearer articulation of operational planning considerations, including dealing with the conflation of electronic warfare and cyber warfare, and the use of uninhabited aerial vehicles for improved intelligence collection and network penetration.

Past Policy and Guidance

The Australian Government acknowledged in its 2009 White Paper that new disruptive technologies that could threaten network capabilities were likely to increase, and that the threat and complexity of cyber warfare was also likely to increase. Cyber warfare not only poses a serious threat to Australia's military capabilities but also to critical infrastructure, as acknowledged in the Minister's Preface to the 2009 White Paper. The 2009 White Paper also noted the growing importance of operations in cyberspace and observed that Australia's national security could be compromised by cyber attacks on the nation's defence, wider governmental, commercial or infrastructure-related information networks. It argued that the emerging threat would require significant and sustained investment in new technology and analytical capability to guard the integrity of information and ensure the successful conduct of operations. That new money however has not been forthcoming.

There has been increasing effort within the Department of Defence to address cyber as a domain, but that will require dedicated additional resources. There is recognition that cyber operations will need to be conducted within the Australian Defence Force (ADF) at force level, while the government acknowledges the need for a whole-of-nation effort. The cyber threat is real and is persistent. Increasingly, one should anticipate pressure mounting to structure Defence to better manage its cyber activities. Similarly, one should anticipate that Defence will realise the conflation of cyber and electronic warfare and recognise an expanded role for Uninhabited Aerial Vehicles (UAVs) and refrain from addressing them as separate issues.

Main Decisions of the 2013 White Paper

The 2013 White Paper devotes ten paragraphs in Chapter 2, and another five paragraphs in Chapter 8 (which is largely a repeat of the points made in Chapter 2) to cyber aspects. Importantly, Chapter 3 explicitly includes security against major cyber attacks on Australia beyond the capacity of civilian agencies to counter as part of the defence of Australia against direct armed attack—Australia's most basic strategic interest.[1] The White Paper addresses electronic warfare and UAVs but does not attempt to bring them together with cyber considerations into any sort of operational planning construct.

The 2013 White Paper builds on the acknowledgement in the 2009 White Paper that national security could be compromised by cyber attacks on defence, government or commercial information networks. Cyber security concerns gave rise to Australia and the United States confirming, in 2011, the applicability of the ANZUS Treaty to cyber attacks. The 2013 White Paper argues that this move emphasised the need for capabilities that allow Australia to gain an advantage in cyberspace, guard the integrity of our information, and ensure the successful conduct of operations. It also argues the need for Australia to exploit cyber power, including working with partners and integrating cyber power into national strategy and a whole-of-nation effort.

As the 2013 version says, understanding of the cyber threat has increased markedly since the 2009 White Paper. The Cyber Security Operations Centre (CSOC) now provides

> a comprehensive understanding of the cyber threat environment and coordinated responses to malicious cyber events that target government networks.[2]

Furthermore, it has allowed Australia to increase "its intrusion detection, analytic and threat assessment capabilities, and improved its capacity to respond to cyber security incidents".[3]

Notwithstanding the improvements, further work is required to ensure the security and resilience of defence systems. While the 2013 White Paper mentions some aspects of this work, such as strengthening network and system management, and personnel and physical security, there is no real

[1] Commonwealth of Australia, *Defence White Paper 2013* (Canberra: Department of Defence, 2013), para 3.9.
[2] Ibid., para 2.87.
[3] Ibid.

discussion on the breadth and depth of issues that need to be addressed. That said, the White Paper does mention that Australia is participating in international efforts to achieve a common understanding of how international law such as the UN Charter and international humanitarian law applies to cyberspace.

The White Paper amplified the Prime Minister's January announcement of creating a new "Australian Cyber Security Centre to improve partnerships between government Agencies and with industry".[4] The intention is to bring together within a single facility cyber security capabilities from across the national security community. The White Paper lists the various elements as Defence Signals Directorate's (DSD) CSOC, other parts of DSD's Cyber Security Branch, the Attorney-General's Computer Emergency Response Team Australia, the Australian Security Intelligence Organisation's Cyber Espionage Branch, elements of the Australian Federal Police's High-Tech Crime Operations capability and all-source-assessment analysts from the Australian Crime Commission.[5] Key industry and other private sector partners will be part of the Centre and Defence will play the principal role in the Centre's operation.[6]

The intent behind this new Cyber Centre is to achieve

> faster and more effective responses to serious cyber incidents, and provide a comprehensive understanding of the threat to Australian Government networks and systems of national interest.[7]

A Board, led by the Secretary of the Attorney-General's Department will oversee the Centre and will report regularly to the National Security Committee of Cabinet.

Implications for Future National Policy

The cyber threat is clearly escalating. The unprecedented sophistication and reach of recent cyber attacks demonstrate that malicious actors have the ability to compromise and control millions of computers that belong to governments, private enterprises and ordinary citizens worldwide. If Australia is going to prevent motivated adversaries from attacking its systems and stealing data, the broader community of security professionals —including academia, the private sector and government—must work together to understand emerging threats and to develop proactive security solutions to safeguard the Internet and physical infrastructure that relies on it.

[4] Ibid., para 2.90.

[5] Ibid..

[6] Ibid, para 2.91.

[7] Ibid.

This is far broader than Defence and in meeting this escalating threat, Australia needs a National Cyber Security Strategy that should seek to maintain and enhance the benefits the nation derives from its activities and capabilities in cyberspace while shaping the strategic environment and strengthening the foundations of its national capabilities. Its key objectives should be to:

- strengthen security and safety in cyberspace;
- maintain and enhance the strategic advantages afforded to Australia by cyberspace; and
- energise the cyber industrial base that supports the nation.

From a national security perspective, government has implicitly argued for access to cyberspace in peace, crisis, or conflict. That means Australia must be able to meet the needs of national security leaders and personnel, irrespective of degradation of the cyber environment or attacks on specific systems. Ensuring this, means Australia must improve the foundation of its national security cyber enterprise—including systems, acquisition processes, industrial base, technology, innovation, and most importantly, the ability to grow Australia's own cyber professionals and continually improve their expertise and skills.

An Australian National Cyber Security Strategy should draw upon all elements of national power—economic, diplomatic, military, informational, technological, and societal—and should adopt a set of interrelated strategic approaches such as:

- promote responsible, secure, and safe use of cyber;
- develop improved Australian cyber capabilities;
- partner with responsible nations, international organisations, and commercial firms;
- prevent and deter aggression against cyber infrastructure that supports the nation; and
- prepare to defeat attacks and to operate in a degraded environment.

Armed with a National Cyber Security Strategy that sets out strategic objectives and approaches, Australia could integrate the various agendas that call for individual security, corporate security, national security, and international security. Calls for action within these agendas are likely to become more strident as cyber crime, cyber espionage, cyber attacks and security breaches increase in frequency, complexity and sophistication.

Indeed, most indicators point to future cyber crime and cyber attacks becoming more severe, more complex, and more difficult to prevent, detect, and address.

In considering its preparedness and response options to military threats, Defence assesses adversary capability. As the cyber threat evolves further, clearer delineation will be needed between activities that could manifest as cyber crime, cyber espionage, or cyber warfare. This means that there will be cyber activities and challenges that Defence will be interested in, while there will be others that fall under the purview of other government agencies and indeed within industry capacity and expertise. There is much work to be done here.

The Government Did Not Address Operational Planning

There is no mention whatsoever of any aspect of operational planning for cyber warfare in the 2013 White Paper. There is little doubt that the CSOC is already engaged in such activity, the technical details of which require the utmost security. DSD (now the Australian Signals Directorate) is a privileged party to cyber warfare developments in the United States and the United Kingdom, including, one would expect, techniques and plans for both defensive and offensive operations. While the US Department of Defense releases an enormous amount of information about cyber threats and its own organisational and operational activities designed to both counter those threats, and to allow the United States to undertake offensive cyber operations against adversaries more generally, Australia strives to ensure that nothing is disclosed about these activities from its side, nor is anything given away about Australia’s activities. But there are aspects of operational planning which ultimately cannot be disguised, including the development and assimilation of doctrine within the ADF and the procurement of particular capabilities.

Sound doctrine is essential for the conduct of successful military operations. While only an authoritative guide, it does provide a focus for strategy and operational planning and forms a common baseline that enhances education and understanding. It brings together those fundamental principles that have worked in the past and those innovative ideas that look to the future.

Electronic warfare (EW) and cyber warfare are becoming conflated as the electro-magnetic environment merges with cyberspace. 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 counter-measures (ECM) and electronic counter-counter-measures (ECCM). ECM and ECCM operations will involve a conjunction of radio-electronic warfare and cyber attacks.

In some cases, cyber specialists would directly engage the electronic sub-systems in major weapons systems, such as the avionics of particular combat and support aircraft. This would include, for example, penetrating the 'firewalls' protecting avionics systems and using wireless application protocols 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 cyberspace.

Cyber warfare operations thus require the use of specialised equipment of various sorts. Much of it consists of assorted miniature devices for implantation at various physical places in adversary networks, which hopefully would never be found.

But there is also a requirement for major support platforms. UAVs offer extraordinary promise for both enhanced and precisely-targetable communications intelligence (COMINT) collection and penetration of networks exposed during microwave transmissions. The acquisition of a squadron of Global Hawks for Signals Intelligence (SIGINT) collection is a serious possibility within the next decade. There are programs to produce a version of the Global Hawk with a 3,000 lb SIGINT payload, including COMINT capabilities. An Airborne Signals Intelligence Payload (ASIP) is available which can locate and monitor microwave signals out to ranges beyond 500 km. It could well be the case that three Global Hawks (with one on continuous 24-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.

Broadening this discussion, commentators are now talking about active defence and while some have defined it precisely, the term continues to cover a broad spectrum. For example, it is used to cover software that scans for viruses without breaching systems on the one hand, while on the other, it is used to cover tools that defend against a cyber attack by disrupting the attacker's network. Lying between these two ends of the active defence spectrum is the action of hacking into a server to protect data that an intruder is trying to steal. The Australian Government has missed an opportunity for addressing active cyber defence in this latest White Paper.

Conclusion: The Need for a National Cyber Framework

While the 2013 White Paper addresses specific Defence aspects, the government has not addressed a fulsome National Cyber Security Strategy and attendant cyber capability plan that reaches across different parts of government and industry. There are vulnerabilities inherent in cyberspace that make it imperative for Australia to develop the requisite strategy, capabilities, policy, tactics, techniques, and procedures for employing the full suite of cyber operations to ensure freedom of action in cyberspace and, to the maximum extent practicable, the safety and security of Australian citizens using cyberspace.

A national framework is needed to assess and prioritise nation-wide cyber-related capability gaps, assign responsibility and accountability for addressing them and to develop an implementation plan for achieving and tracking results. This would help identify the capabilities required to support the national cyber strategy of the day and help the agencies prepare long-term plans and funded programs to address critical cyber capabilities. One of the key elements of such a framework should be a capabilities-based assessment that defines the national cyber mission, identifies required capabilities, identifies gaps, assesses risk associated with those gaps, prioritises gaps, assesses solutions (both technical and otherwise), and recommends actions for government agencies and others to pursue.

The Australian Government has achieved much and is to be applauded thus far. However, nothing to date, or in train, addresses the cyber-related capability gaps that span technology, personnel skills and numbers, organisational requirements, education and training, facilities, support and services that would enable a current baseline cyber posture to be developed, a consolidated view of all requirements and gaps to be presented, and future remediation and implementation plans to be developed. As a result, cyber capability gaps across the Australian Government will continue to hinder the agencies’ ability to plan for and conduct effective cyber operations.

Best practices for strategic planning indicate that effective and efficient operations require detailed plans outlining major implementation tasks, defined metrics and timelines to measure progress, a comprehensive and realistic funding strategy, and communication of key information to decision makers, all within a transparent process that keeps the public informed.

The sense of threat and vulnerability is mounting and the public and private sectors will come under increasing pressure to ‘do something’ about cyber security. Australia needs a comprehensive capabilities-based assessment, a cyber capability plan, and an implementation plan (with specific actions and implementation responsibilities, timeframes, and performance measures) and a funding strategy for addressing any gaps resulting from the assessment.

Any cyber response by Australia should anticipate further cyber actions by others—these actions might be targeted specifically at Defence or the ADF, cross-Government interests, or whole-of-nation interests. Australia needs to ensure it has an integrated cyber capability that is resourced adequately and manages a number of competing demands, such as those for financial resources and cyber expertise, while ensuring disproportionate effort is not devoted to cyber—after all cyber does need to be ‘normalised’ as part of everyday activity and operations.

Desmond Ball is a Professor in the Strategic and Defence Studies Centre at the Australian National University, Canberra. He was Head of the Centre from 1984 to 1991. He is the author or editor of more than 50 books or monographs on technical intelligence subjects, nuclear strategy, Australian defence, and security in the Asia-Pacific region. His publications include Australia and Cyber-Warfare *(co-authored with Gary Waters and Ian Dudgeon);* Militia Redux: Or Sor and the Revival of Paramilitarism in Thailand *(co-authored with David Mathieson);* The Boys in Black: The Thahan Phran (Rangers), Thailand's Para-military Border Guards*;* Burma's Military Secrets: Signals Intelligence (SIGINT) from 1941 to Cyber Warfare*;* Breaking the Codes: Australia's KGB Network, 1944-50 *(co-authored with David Horner); and numerous articles on issues such as the strategic culture in the Asia-Pacific region and defence acquisition programs in the region. Professor Ball was elected a Fellow of the Academy of Social Sciences of Australia (FASSA) in 1986. He served on the Council of the International Institute for Strategic Studies (IISS) in 1994-2000, and was Co-chair of the Steering Committee of the Council for Security Cooperation in the Asia Pacific (CSCAP) in 2000-2002.* desmond.ball@anu.edu.au*.*

Gary Waters spent over thirty years in the Royal Australian Air Force (RAAF), retiring as an Air Commodore in 2002; worked as a senior public servant in Defence for four years; and then worked with Jacobs Australia as Head of Strategy for seven years. He left Jacobs in March 2013 and now acts as an independent consultant. He has written thirteen books on doctrine, strategy, cyber security, and military history. His latest two books are Australia and Cyber-Warfare *(with Professor Des Ball and Ian Dudgeon, 2008), and* Optimising Australia’s Response to the Cyber Challenge *(with Air Vice-Marshal John Blackburn, 2011). He is a Fellow of the Royal Melbourne Institute of Technology (graduating with majors in accounting and economics); a certified practising accountant; a graduate of the UK’s Royal Air Force Staff College; a graduate of the University of New South Wales, with an MA (Hons) in history; a graduate of the Australian Institute of Company Directors; and a graduate of the Australian National University with a PhD in political science and international relations.* waters_garyw@hotmail.com*.*