Australian Defence Policy in the Information Age

Submission for the 2015 Australian Defence White Paper

Greg Austin[1]
Professorial Fellow
EastWest Institute
New York/Brussels/Moscow

22 September 2014

Executive Summary: At the national level, Australia is falling behind in digital competitiveness. This is reflected in Defence planning in our inability to adjust to the demands of cyber war. We have adjusted well in respect of cyber security, but that is a fragment of the policy spectrum covered by modern concepts of war in the information age. Our key ally the United States, and other actors of high strategic interest to us, such as Japan, China and Islamic State, are making advances in this field. Australia's national level strategy papers need to respond both to what these actors are doing in military uses of the cyber domain, as well as articulate how we will use our cyber power offensively to achieve military and strategic aims through cyberspace. Our single services (Army, Navy and Air Force) are approaching the cutting edge in tactical terms, but there is no articulated national defence vision that rises to the challenges set by the emerging strategic environment or offered by the potential of transformative technologies of cyberspace. Remedial steps are needed, including a variety of baseline studies and organizational changes. We need to unleash our capabilities in this area through organizational and doctrinal innovation that matches the demands of the innovation era. As just one example of the changes we need, we could consider establishing a citizens' cyber militia to allow for rapid mobilization (call out) in the event of a crisis. But our unmet needs also need to be addressed in all areas of national force structure planning, especially in developing a concept of strategic strike enabled by cyber means.

Introduction

This brief submission[2] calls for a step change in Australian national strategy on promotion of cyber warfare[3] not just as an adjunct in national military planning but as its essential core. The

[1] See biographical note at the end of this paper.
[2] References are available on request.
[3] The United States avoids the term cyber war. It has adopted two terms that are related but have different meanings: "information operations" and "cyber effect operations" in an overarching military strategy of information dominance. This paper uses the term "cyber war" for ease of reference, understanding that it embraces the same purview as the United States understands in these three terms. None of the three is adequate by itself to capture the vast array of policy and capability in play. The term "cyber war" can also be misleading by implying that a conflict might take place exclusively in the cyber domain. This is highly unlikely. So the term "cyber war" means war, as the Chinese say, under conditions of informatization.

United States recognizes three integrated dimensions of the cyber operations environment: physical, informational and cognitive.[4] Australian policy is strongest in the first, on middle ground in the second, and weakest in the last. Advanced exploitation of information systems and of highly re-aggregated information subject to high-speed processing by artificial intelligence methods provides efficiencies and effectiveness to military operations regardless of the technology level of the other side or of the conflict. Most importantly, as the United States recognizes in its 2011 National Military Strategy (an approximate equivalent to our Defence White Paper), cyberspace is one of three "essential and interdependent mediums" for force projection and for an "ability to deter and defeat aggression". This short paper gives an overview of some of the issues before offering several recommendations for consideration.[5]

Australian Strategy Documents

Recent defence policy statements describing our national level posture barely touch on the subject of cyber warfare (dependent on advanced information aggregation, analysis, and rapid exploitation for strategic strike). Our White Papers give cyber warfare a primarily defensive function akin to physical protection of military command and control (C2) networks and other systems from cyber attack.[6] In very rough terms, this represents about one per cent of military reality in the information age. It is akin to "C2 plus cyber security" when in fact leading world powers are operating a C4ISTAR vision: command, control, communications, computers, intelligence, surveillance, target acquisition, reconnaissance – all enabling "strategic strike in milliseconds". In Australia, key strategy documents at the national level pay almost no attention to concepts like "information operations" and the word "digital" rarely appears.

The 2013 White Paper recalled the agreement in 2011 between the United States and Australia that the ANZUS treaty would apply to cyber attacks. It concluded as a result that Australia needed "capabilities that allow us to gain an advantage in cyberspace, guard the integrity of our information, and ensure the successful conduct of operations." It said that the "the net effect on Australia's position will depend on how well we exploit cyber power". It acknowledged that "Once deployed, our forces will need to operate as a networked force in a contested environment." But beyond these and other references to security against cyber attacks, there is little hint that the country has a deep appreciation of the revolutionary impact of the information age in military affairs. There are many references in the White Paper to things that might relate in the most general terms to the information revolution, and its authors might refer to these to rebut this criticism, but there is no strategy for visible in it for "how we exploit our cyber power", let alone build a force structure and a recruit base around it. (Navy recruiting has said it can't fill its vacancies with suitably qualified people to operate many of the advanced electronic systems.)

---

[4] "The physical dimension is composed of command and control systems, key decision makers, and supporting infrastructure that enable individuals and organizations to create effects. The informational dimension specifies where and how information is collected, processed, stored, disseminated, and protected. The cognitive dimension encompasses the minds of those who transmit, receive, and respond to or act on information."

[5] The paper presents arguments that complement those in an excellent article by Des Ball and Gary Waters, "Cyber Defence and Warfare", in *Security Challenges*, Volume 9, Number 2 (2013), pp. 91-98, which focuses on establishing a National Cyber Framework.

[6] Policy documents and procurement efforts of the single services are much closer to the international best practice.

By contrast, a paper by the Australian Army, *Future Land Warfare Report 2014*, reveals a highly sophisticated awareness of the realities of the information age. Here are just several excerpts:

- "Current cyber defence capabilities have not kept pace with technological change"

- "The land, sea and air domains will become further entwined with the cyber, electromagnetic and space domains. These domains will be the subject of constant competition, with land force operations increasingly enabled (or disabled) by access to digital networks."

- "A fully digitised force will depend on access to space-based capability for battlefield management, communications and precision navigation and timing (GPS, for example)."

- "To what degree is the Army prepared for an interconnected battle space in which deployed theatres are not quarantined from the homeland and force generation base?"

- "To what degree is the Army prepared to rebalance its force structure into non-traditional capabilities and units (such as boosting the capability of the intelligence battalion or adding an Army cyber capability) in order to build greater capacity for intelligence-led targeting?"

- "Is the Army willing to fundamentally change its traditional command, control and communication structures and processes, in particular the Army's unit and formation headquarters, to maximise the advantages of access to joint effects and the enhanced networking of digital systems?"

This last point ("jointness") is of particular importance. Single service tactical systems in Australia are becoming more "cyberised", and we can probably assume that our special forces are quite advanced, but the maximum potential gains in capability at the strategic level of war can only be realised if forces are organized for joint operations and if intelligence and reconnaissance are fully integrated with joint force commands which have a mission for strategic strike.

The gulf between the 2014 Army paper and the 2013 White Paper on cyber war is bridged somewhat by the Information Activities doctrine of the ADF, approved in November 2013 and later declassified. This manual does not appear to embrace the high end, transformationalist view of cyber power. It limits itself to "information activities" that are "are defined as the integration, synchronisation and coordination of two or more Information-related capabilities (IRC) that generate and sustain a targeted information advantage". The manual contains all of the right concepts, but manifests confusion at the top end of capability between what sounds like the public relations or propaganda aspects of information policy ("strategic communications") and the main purpose of high end information operations which is "strategic strike" to defeat or deter an enemy.

The 2013 ADF doctrine is not clear on this bigger set of questions. It does not fill the gap identified ably in a 2007 analysis of Australian cyber warfare strategies written by Lieutenant

Commander Chris Watson, a former Royal Navy officer then serving in the Royal Australian Navy. Writing in the *Australian Army Journal*, he concluded: "The unresolved issue now is not so much how to integrate Information Operations into military operations, but rather how to persuade politicians and public servants to coordinate the efforts of their respective departments into a National Effects Based Approach so as to provide whole-of-government forward planning with the direction, legitimacy and promise of success a nation is entitled to expect." As just one example of the deficiencies, he mentioned that within Australia's smaller intelligence community, "there remain significant changes to be made if Information Operations planners are to be provided optimal rather than ad hoc intelligence support." But he correctly identified the main problem as a lack of commitment to the cognitive aspect of information operations: changing how the enemy leaders think by directly attacking their knowledge environment and command relationships by cyber and other means. He said that one problem was that the Defence organization was in danger of being swamped by the "transformationalist" approach (the idea that informatisation[7] changes everything) that is now dominant in the U.S. doctrine. The 2013 ADF doctrine on information operations borrows from U.S. doctrinal manuals, but does not in its totality reflect the core concept of cyber warfare as reflected in U.S. strategy or in emerging worldwide realities. One reason may be, as the Army publication mentioned above has suggested, that Australia is not ready to modernize its force structure to accommodate the changing reality of military affairs. There is little mention of the concept of cyber warfare or information operations in a 2012 Force Posture Review commissioned by Defence from two former Secretaries of the Department. Arguably, their terms of reference did not allow them the opportunity though the section of ADF capabilities might have been an obvious place to cover this ground.

United States

Australia appears out of step with its principal ally, the United States, which has a military strategy premised on information dominance as the foundation for strategic strike. Our ally is investing heavily in military uses of cyberspace. In classic cyber war terms, this refers not just to the Internet, computers and networks, but also to conventional telecommunications networks on the one hand and, on the other, to processors and controllers in any automated system. "Cyber effect operations" in wartime seek to impair the confidentiality, integrity or availability of not just the machines but the data contained therein. This can include penetrating enemy intelligence systems and altering the information about one's own forces or even information about the disposition of the opposing country's forces. A Presidential Directive says that the United States will seek to apply "cyber effect operations" (COE) in all spheres of national activity affecting war, diplomacy and law enforcement. It says that offensive COE (OCOE) "can offer unique and unconventional capabilities to advance U.S. national objectives around the world with little or no warning to the adversary or target and with potential effects ranging from subtle to severely damaging".

[7] "Informatisation" (from the French) is not a common word in English, perhaps because we take it for granted. It refers to the application of advanced information and communications technologies to all walks of life in a way that has the ability to change them in some fundamental way if only because of superior access to and exploitation of information. This somewhat jarring word has the value of causing the reader to reflect about the social impact of the information ("knowledge is power") as well as the technology.

But there is a deeper dimension to the concept of cyber war. It relates to the role of information and how a country's military power and strategic impact in war can be magnified by cyber means. In November 2012, the U.S. Joint Chiefs of Staff issued a new joint training manual on "Information operations". It identified the information environment as the aggregate of "individuals, organizations, and systems that collect, process, disseminate or act on information". This is a strategic level orientation in which the United States aims above all else to disrupt the enemy's decision-making as a prelude to and adjunct for kinetic operations: the integrated employment during military operations of information capabilities "in concert with other lines of operation, to influence, disrupt, corrupt, or usurp the decision making of adversaries and potential adversaries while protecting our own."

One key element of U.S. military policy is its recognition in a 2011 "Department of Defense Strategy for Operating in Cyberspace" of the need to "Leverage the nation's ingenuity through an exceptional cyber workforce and rapid technological innovation".

Japan

In October 2013, the Defence ministers of Japan and the United States called for the US military to provide cybersecurity training to Japanese forces. The moves announced are in line with the U.S. global pattern of strengthening alliances on cyber preparedness before being able to make significant progress on tension-reducing measures with potential adversaries. In June 2013, Japan released a new national cyber strategy. It is largely civil in character, but it represents something of a landmark for Japan. On the diplomatic front, it talks of strengthening the active collaboration with the United States while leaving open a broad strategy of cooperation with other countries. But its military defense element is just as prominent. It pays attention not just to the Japanese armed forces but to the country's critical cyber infrastructure. It identifies ten sectors -- ICT, finance, aviation, railway, electricity, gas, government-to-government services (including regional municipalities), medical, water, and logistics. This evolution has been inevitable but it also forces interested observers to understand that for Japan the operational environment for military scenarios will now be a more heavily cybered one.

China

In August 2014, China's President, Xi Jinping, told a Politburo meeting that the country needed a new cyber military strategy. The news is understandable given that the country is relatively weak in cyber military power compared with the United States and its global alliance system. The leaders are concerned about U.S. and Western technological superiority in the ICT sector and about China's difficulty in building a high-performing national innovation system. China's speed in exploiting cyber technologies for espionage has not been matched in the pace of the overall development of its armed forces for cyber warfare. When in 2003 the Central Military Commission (CMC) approved a new doctrine for war "under conditions of informatization" (cyber war), it did so without wanting to sacrifice the efforts being made to catch up in classic forms of military capability (mechanized forces on land and power projection forces at sea and in the air). For this reason, the CMC approved a dual track policy of "mechanization and informatization". This was a sop to the traditionalists in China's armed forces who did not want a wholesale commitment to cyber war.

It took until 2006 for the CMC to approve training regulations for the new doctrine approved in 2003. The level of penetration of automated systems in the armed forces has been slow, evidenced by relatively slow introduction of simulators for weapons training. In 2008, the CMC approved a new regulation on space security, since the United States was giving pride of place in its cyber military strategies to space based assets. China lags behind the United States in space-based military assets. In 2011, China made important changes to its General Staff Department to begin to mirror the development by the United States of its Cyber Command. It was only in June 2013 that China conducted its first joint military exercise using digital technology to simulate "non-contact assaults" (that is cyber attacks intended to disable opposing military forces).

Further evidence of the slow pace of take up of cyber war capability is readily available in Chinese open sources. This slow pace in the armed forces mirrors an equally dilatory pace of informatization in the civilian economy. China ranks 62nd of 148 countries, according to the World Economic Forum's 2014 Global Information Technology Report, having slipped progressively from 36th in 2011.

The statement from Xi in August 2104 about China's need to do better in cyber war capability is being driven by the leadership's conviction that the United States is better at cyber war than China and that it could probably undertake a disabling strike against China's command and control systems using a combination of cyber and kinetic means. Xi's announcement followed several related announcements in the past year, including in February 2014 when he took over the leadership group directly responsible for all of China's cyber development, civilian and military. His statement is especially noteworthy for two reasons. He called on the armed forces to do better at innovation in general, especially because of the problems (unspecified) with the reform process. But the more radical measure was his call to "change our fixed mindsets of mechanized warfare".

China is now determined to cut the size of its armed forces, including if need be its navy, so that it can produce a more high-tech capability across the board, primarily in cyber warfare (across the entire electromagnetic spectrum). The new coded language from Xi represents a radical turn by the Chinese armed forces, to give offensive cyber capability the dominant priority over all else, including the traditional goal of mechanization. Xi's announcement is evidence that China knows that it will not keep pace in the advanced science of the ICT sector, including in cyber war capability, without radical changes in policy.

Islamic State

The forces of Islamic State (IS) depend on a range of communications systems that are susceptible to disruption by opposing forces. According to the new Director of the National Security Agency (NSA), Admiral Mike Rogers, "We need to assume that there will be a cyber dimension increasingly in almost any scenario that we're dealing with". Rogers, who is also head of the U.S. Cyber Command, an operational joint command under the President, told a Congressional Committee in September 2014 that NSA was actively "involved in" the cyber dimension of IS capabilities, meaning both monitoring and attacking them. These capabilities include not just social media platforms and web-based activities, but also traditional forms of communication, including encrypted communication.

The need for Australia to combat irregular and low-technology forces is not a reason to de-emphasize information warfare. On the contrary, clever exploitation of advanced ICT technologies can be used to undermine any organized military and political force regardless of its level of technology. At its most basic, advanced cyber espionage techniques allow more effective and timely preventive action of an irregular enemy. But the opportunities for disinformation and disruptive cyber operations are also enormous.

Strategic Stability and Cyber Space

In Jun 2013, Russia and the United States agreed to set up a cyber-risk reduction center (a hot line) staffed by technical specialists inside the existing bilateral nuclear risk reduction center. This link between cyber risk reduction and nuclear threats goes a long way to explaining rhetoric like a “cyber Pearl Harbor” used by former CIA Director Leon Panetta in October 2012. Also in June 2013, retired Admiral Mike Mullen, a former Chairman of the Joint Chiefs of Staff, reiterated in public his earlier warnings about the urgency and seriousness of the military and diplomatic problems in cyberspace. Mullen said that the cyber menace is “the only existential threat of concern”. He said that cyberspace is “incredibly dangerous” and that threats travel at light speed. In March 2013, a senior military official told Congress that the United States was using cyber assets to defend against missile attack, and that might be happening even before a conflict goes hot. He went on to say that “we are very concerned with the potential of a cyber-related attack on our nuclear command and control and on the weapons systems themselves”. In June 2009, another American military leader said that if U.S. military networks were subject to a disruptive cyber strike, “we'd need to respond rapidly, at network speed, before the networks could become compromised”.

As observed in a 1996 article in *Foreign Affairs* by Professor Joe Nye and Admiral William Owens, “The information technologies driving America’s emerging military capabilities may change classic deterrence theory.” The United States went on to develop information dominance of the battlefield as a fundamental part of its nuclear military strategy. It was quite within its rights to do so. But events since 1996 have shown how profoundly this change of strategy to pre-emption and almost zero warning time has shifted the calculus of deterrence between nuclear weapons states.

Cyber attack against command and control systems for military nuclear systems would be very difficult but it is the public testimony of the U.S. government that it seeks to acquire that capability. It can be assumed that other countries, such as Russia, China, India, Pakistan, Israel and North Korea pursue similar goals.

The nuclear weapons stand-down between the United States and the USSR that presaged the end of the Cold War was only possible because of shared commitment by the two governments to concepts like strategic equivalence and strategic stability, and later the idea of “common security”. No government in the world has yet articulated a renewed commitment to similar concepts of strategic equivalence or stability that apply specifically to command and control of strategic nuclear missiles in the age of cyber–weapons.

One reason for this is that the old ideas of nuclear equivalence and strategic stability were both only a useful figleaf. They provided an artificial construct for a plateau of imagined equivalence that enabled a defusing of tension through negotiation of limits on certain weapons. The two governments appreciated that the idea of military balance was a dynamic concept and that relativities in military power could be fundamentally transformed quite quickly through stratagems like pre-emption, surprise attack or successful decapitating strikes.

The advent of the cyber age – with time frames of milliseconds – has exhausted the limits of usefulness of concepts like "strategic equivalence" from Cold War days. U.S. diplomats admit in public that they are now searching for the new definition of strategic stability in cyber space. As the authoritative Cyber Conflict Studies Association noted in a 2012 report *Addressing Cyber Instability*, the core policy problem is that the "evolution of the technological architecture has vastly outpaced the corresponding set of conceptual, doctrinal, organizational, and legal structures'. The result, according to the report has been a "reactive and atavistic policy dynamic".

Australian Policy Responses

In Australia, the environment for decision-making on defence policy for the information age is severely hamstrung by the national environment. The picture in the country is one of "falling digital competitiveness". According to annual edition of the Network Readiness Index published by the World Economic Forum, Australia slipped from a ranking of 9th in 2004 to 18th in 2013 and 2014. Between 2003 and 2010, our corpus of new ICT graduates fell 53 per cent. We were able to compensate in part by temporary ICT migrants to Australia, which in 2009-10 numbered 8,530 (double the number of our own IT graduates). The situation is much more complex than this, but these are useful reference points. Australia needs a digital age strategy before it can have a digital military strategy. Australia is falling behind the pace of digital ideas.

Perhaps Defence in Australia can take something of a lead to reverse this situation. But it would need to recognize at the outset that the level of expertise in Australia in military applications in this field, as in many other countries, is low. The experience levels of key decision-makers in defence policy do not in many cases match the nature of the problem. There would have to be a commitment to deeper organizational change, especially in force structure. The effort would need to be multi-national, multi-sector (including the Communications and Education Departments) and private-public.

The following steps may be usefully considered:

- Invite the Army to answer the questions posed in its 2014 paper about cyber warfare
- Invite the Army to do an audit of Australia's military digital readiness, especially focused on the White Paper concept of "how we exploit our cyber power" for military advantage
- Review the membership qualifications, the agenda and decisions of the Strategic Effects Targeting Board (which could be the primary vehicle in the ADF for guiding information policy and operations)
- Set up a high level review team including distinguished U.S. serving and/or retired military personnel (four star level) to report in two phases on improvements to

Australia's military digital readiness: one short term (say 6-12 months) and the second in the medium term (say two years)

- Promote the convening of a public inquiry by the Australian Senate Committee on Foreign Affairs, Defence and Trade into Australia's military digital readiness
- Establish a working group with peak industry bodies on the contribution of the private sector to Australia's military digital readiness (to complement existing bodies looking merely at cyber security)
- Revise curricula at military staff colleges and academies to reflect the arrival of the information age and to tease out implications for Australia
- Expand funding for related analysis in ADF research centres (such as the Land Warfare Studies Centre or Air Power Development Centre) and universities to emphasize the issue of national level capability transformation for the cyber age
- Consider the establishment of powerful but flexible digital militia forces (reservists) capable of rapid mobilization in major capital cities in highly secure spaces in the capitals or other nearby locations
- As a matter of urgency, commission a report on the quality and depth of Australia's digital work force (the recruit base for the ADF and related government departments)
- As a matter of urgency, commission a report on community and business attitudes to cyberspace as they pertain to national security needs.

****

Author's Biographical Note: Dr Greg Austin is a Professorial Fellow at the EastWest Institute and author of the new book, *Cyber Policy in China* (Polity 2014). He held an appointment as Visiting Senior Fellow in the Department of War Studies at King's College London while writing the book. He has had a prominent career in international policy research, including a concentration on information security since 2009. He has published six books on international security, four as author or co-author and two as editor or co-editor. He has held academic posts and worked for government in the UK and Australia, and held leadership posts in prominent international NGOs operating from Brussels and London. His recent journal articles and chapters include:

- "Managing Asymmetries in Cyber Power between the United States and China", *Georgetown Journal of International Affairs*, October 2014
- "Internationally protected facilities in cyber space: a proposal for stock exchanges and clearing houses" (2014), under review by the EastWest Institute
- "China's Security in the Information Age" in Lowell Dittmer and Yu Maochun (eds), *China Security Handbook*, Routledge, in publication, due 2015
- "China's Cyber Espionage: The National Security Distinction and U.S. Diplomacy", (September 2104), under review by *Asian Survey*
- "A measure of Restraint in Cyberspace: The Case of Civil Nuclear Assets", co-authored, EastWest Institute Policy Report 1/2014, 20 pp, briefed in plenary to the nuclear Knowledge Summit in Amsterdam, an official pre-event of the Heads of State Summit
- "Make Highly Secure Computing the Dominant Paradigm in International Cybersecurity", EastWest Institute Discussion Paper 1/2014, co-authored with Sandro Gaycken, 20pp

- “Cyber Detente between the United States and China”, EastWest Institute, New York/Brussels/Moscow, co-authored with Franz Stefan Gady, November 2012, 20pp
- “Russia, the United States, and Cyber Diplomacy: Opening the Doors”, EastWest Institute, New York/Brussels/Moscow, co-authored with Franz Stefan Gady, September 2010, 20pp