Australian Journal of Telecommunications and the Digital Economy

Australia’s Digital Skills for Peace and War

Greg Austin
East-West Institute (New York/Brussels/Moscow)

Summary: This article gives an overview of Australia's national military strategy for cyber space and the implied demands for a radical approach to development of our civil skills base. It then looks at developments in countries and groups of military interest to us in cyberspace. On this basis, the piece concludes with some recommendations for Australian policy.

Introduction

The last inspirational speech by an Australian Prime Minister on the country’s digital future was made seventeen years ago by Paul Keating, one year after the he left the job (Keating 1997). He offered a comprehensive view of the transformative power of the information revolution, touching on both a “thriving IT industry and an information-educated workforce” and the impact of those “on all our industries from farming to manufacturing to health care”. He said it would need “ideas and a strategic framework within which local and overseas businesses can operate” that would “accommodate and provide for a growing IT presence in our whole economy and society”. Above all, he said, “developing the information industry does mean developing our people”. This article is about that theme: the country’s digital skills. It reviews the broad policy settings in Australia for development of our digital skills for strategic gain at the national level in peace and war. We desperately need renewed political leadership for our digital future.

A country cannot hope to have cyber talents for war if it does not develop them in peacetime, and if it does not have a strategy for transitioning these skills from the civil economy to military uses when emergencies dictate. Moreover, the enhanced development of military cyber skills and strategies has flow-on effects to civil economy. This virtuous circle of innovation — what might be called our information technology (IT) industry base — is weak and definitely needs help. As elsewhere, we need to attract more venture capitalists, nationality unimportant, and get their money into university-based and industry-based R&D for IT. Weaknesses in our cyber security situation in the civil sector (vulnerabilities everywhere) are not unique to Australia, but our inability to provide the skills base we need to overcome them, and a lack of industrial options to address them, must translate into great dangers for the country, not just in peacetime

AUSTRALIAN JOURNAL OF TELECOMMUNICATIONS AND THE DIGITAL ECONOMY VOLUME 2 NUMBER 4, DECEMBER 2014
ISSN 2203-1693. Copyright © 2014 The Author(s). http://doi.org/10.7790/ajtde.v2n4.68

(cyber crime from overseas that may go unnoticed and unpunished) but most especially in the risk of large scale cyber attack on our civil economy during wartime.

The article gives an overview of our national military strategy for cyber space and the implied demands of that for a radical approach to development of our civil skills base. It then looks at developments in countries and groups of military interest to us in cyberspace. On this basis, the piece concludes with some recommendations for Australian policy.

The Civil Economy

The four Prime Ministers since Keating, to the extent that they even followed the issue of the digital world, have seen it more often as a threat than an opportunity. (To review all Prime ministerial speeches, see http://pmtranscripts.dpmc.gov.au and http://www.pm.gov.au/.) In 2011, the Gillard government released plans for a new White Paper focusing largely on cyber security (following a 2009 white paper on that subject), which it later said would have an expanded scope to look at the digital economy in the broad. The plan to expand its scope was announced by Julia Gillard as she closed a Prime Minister's *Forum on the Digital Economy* in October 2012. The resulting paper, *Advancing Australia as a Digital Economy* (Dept of Communications 2013), was an update to the National Digital Economy Strategy of 2011. Neither paper went much further than e-government, online access, the broadband network or small grants to ICT undertakings. Neither paper had any concept of IT education beyond providing online access. While the current Minister for Communications, Malcolm Turnbull, is engaged regularly and earnestly with a vision of Australia's digital future, in all of its dimensions, the country lacks political leadership across the board in this area of policy, especially for promoting ICT education and stimulating industry/university R&D linkages. The coalition's policy for the digital economy going into the 2013 election (Coalition 2013) did not address the main concerns raised by industry at the Forum a year earlier, notably a lack of software engineers, and lack of translation of advanced information technologies into key sectors like agriculture, education and health. Political leadership in Australia for the information society appears to have been captured by two narrow issues (the debate about national broadband infrastructure or online government), with occasional references to small grants for new spending on advanced ICTs for this or that sector.

Apart from needing political leadership, the country will need time to be able to reverse the slide in Australia's digital competitiveness since 2007 that the coalition policy document of 2013 noted. 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 (WEF 2004, 2013, 2014). In 2014, the affordability of our access to network infrastructure was one of the most costly in the world (we were ranked at 49th with 1st being the least costly). Between 1999 and 2013, our annual corpus of new domestic student graduates in information technology (IT) fell by 46 per cent (Dept of Education 2104a), though there has been an upturn in the last two years. (This reference to IT graduates does not include electrical engineers which saw an increase.)

We have been able to compensate for the sharp decline in IT graduates in part by temporary ICT migrants to Australia, which in 2009-10 numbered 8,530 – double the number of our own IT graduates for that year (ACS 2011: 27-28). (Data for later years does not allow a similarly granular comparison.) In terms of student satisfaction with our IT tertiary offerings, data for 2005 to 2012, the latest available, shows that the completion rate for students enrolled in information technology over the period was only 61 per cent, significantly lower than for any other of ten general categories of study (Dept. of Education 2014b). The real situation of Australia's digital economy and society is much more complex than these few statistical snapshots suggest, but these are useful, if disappointing reference points. The 2014 WEF report observed about Australia: "Compared with individuals, businesses and government are less dynamic in taking up ICTs" (WEF 2014: p. 23). This decline in digital competiveness has been accompanied by a loss of scholarly interest in the subject. A review of the literature on Australia and the digital economy or information society reveals a decline in the volume of material on this issue. In academia in Australia, the issue is more or less out of fashion, barring a few brave souls, "crying in the wilderness".

Australia's Chief Scientist, Professor Ian Chubb, observed in September 2014 that Australia is the only country in the OECD without a national plan for science, technology or innovation (Chief Scientist 2014a). In the report he released at that time, on *Science, Technology, Engineering and Mathematics: Australia's Future*, Chubb outline an education plan for education with 21 recommendations (Chief Scientist 2014b: 20-22). These recommendations paint a picture of a country that is falling off the pace in education for a technological future. In a newspaper article that same month, he went further: "Where science is concerned, I must part company with some of our economists. To transform our nation, we need to facilitate innovation in science on a scale we've never achieved. That's too important to be left to chance, or to 'market signals" (theguardian.com 08/09/2014). As our universities become more marketised and privatised, Australia will need not just political leadership to maintain our civil skills base in IT, it will need radical policy measures.

In 1989, a rather prescient economist in Australia anticipated the long term trend. He wrote: the "service economy in Australia is petering out as it does not offer much scope for undertaking information-intensive projects that will expand output, income or employment, rapidly. The impact analysis also reveals conflicts between long term goals of structural change and short-term stabilisation goals of maximising income and employment. (Karunaratne 1989: 473). While there have been clear advances, captured well in a 2014 report by Price Waterhouse Coopers (PWC 2014), development of our IT skills base is still hostage – a quarter of a century later – to an overriding political ethic of full employment and traditional notions of a work force.

In War as in Peace

A country's military capability and strategic planning cannot escape the general trend of development in its economy and human resources. While the civil sector can compensate for a 50 per cent drop in IT graduates by massive increases in work visas for non-nationals, the national security sector cannot. Australian citizenship is usually a requirement for the sector. The low penetration rate of IT professionals in all echelons of military and strategic planning, a symptom of our desultory outcomes in information technology education, produces defence policy that looks strangely out of step with the emerging digital realities.

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 latest White Paper (Dept of Defence 2013) gives cyber warfare a primarily defensive function akin to physical protection of military command and control (C2) networks and other systems from cyber attack. 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. Policy documents and procurement efforts of the single services are much closer to the international best practice.

The 2013 Defence 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 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.)

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 (Australian Army 2014). 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

ISSN 2203-1693. Copyright © 2014 The Author(s). http://doi.org/10.7790/ajtde.v2n4.68

> 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 organised 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 (ADF 2014). 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 (Watson 2007). 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" (Watson 2007: 96). :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" (Watson 2007: 93). But he correctly identified the main problem as a lack of commitment to the cognitive aspect of information operations: changing how the enemy

ISSN 2203-1693. Copyright © 2014 The Author(s). http://doi.org/10.7790/ajtde.v2n4.68

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 organisation was in danger of being swamped by the "transformationalist" approach (the idea that informatisation changes everything) that is now dominant in the U.S. doctrine (Watson 2007: 93). 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 modernise 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 (United States 2012a). 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".

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" (United States 2012b). It identified the information environment as

ISSN 2203-1693. Copyright © 2014 The Author(s). http://doi.org/10.7790/ajtde.v2n4.68

the aggregate of “individuals, organisations, 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” (United States 2011: 11). In fact, this is one of the Department’s five principal strategies for cyberspace. While the United States is clearly in a different and superior league of cyber military power from Australia, we might learn from its plans for developing our cyber war skills. It makes the obvious commitment to catalysing new education opportunities in a situation of high and unmet) demand: “catalyse U.S. scientific, academic, and economic resources to build a pool of talented civilian and military personnel to operate in cyberspace”. But it says that its plans in this area of skill development will be paradigm changing and will include the private sector:

- streamline hiring practices for its cyber workforce
- exchange programs to allow for “no penalty” cross-flow of cyber professionals between the public and private sectors to retain and grow innovative cyber talent
- adoption and scaling of cross-generational mentoring programs
- the development of Reserve and National Guard cyber capabilities
- infusing an entrepreneurial approach in cyber workforce development
- preserving and developing DoD’s intellectual capital
- replicate in the DoD the dynamism of the private sector
- harness the power of emerging computing concepts (especially speed and incremental development rather than a single deployment of large, complex systems)
- opportunities for small and medium-sized businesses and entrepreneurs to move concepts rapidly from innovative idea, to pilot program, to scaled adoption across the DoD enterprise
- emphasise agility, embrace new operating concepts, and foster collaboration across the scientific community.

ISSN 2203-1693. Copyright © 2014 The Author(s). http://doi.org/10.7790/ajtde.v2n4.68

Japan

In June 2013, Japan released a new national cyber security strategy (Japan 2013). 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 defence 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.

This has its implications for development of the skills base. In what may be a unique national qualitative audit of IT skills, the paper says the country by itself will not meet its personnel needs in information security and that much more than half of its work-force don't have the right skills: "approximately 265,000 individuals are employed in information security within Japan, however there is a potential deficiency of approximately 80,000 such security personnel. In addition, of these 265,000 individuals, the number of individuals who actually possess the required level of skills is thought to be slightly over 105,000, meaning that some sort of education or training is necessary for the remaining 160,000 individuals" (p10).

In addition, the role of Japan and its international alliances and military partnerships are of some significance to Australia. In October 2013, the defence ministers of Japan and the United States called for the US military to provide cybersecurity training to Japanese forces in the context of a broader new policy to cooperate in developing the right human skills base (Japan Times 2013).

China

In August 2014, China's President, Xi Jinping, told a Politburo meeting that the country needed a new cyber military strategy (Reuters 2014a). China's 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 (Austin 2014). 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)

ISSN 2203-1693. Copyright © 2014 The Author(s). http://doi.org/10.7790/ajtde.v2n4.68

approved a new doctrine for war "under conditions of informatisation" (cyber war), it did so without wanting to sacrifice the efforts being made to catch up in classic forms of military capability (mechanised forces on land and power projection forces at sea and in the air). For this reason, the CMC approved a dual track policy of "mechanisation and informatisation". This was a sop to the traditionalists in China's armed forces who did not want a wholesale commitment to cyber war.

The pace of penetration of automated systems in China's 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). The slow pace in the armed forces mirrors an equally dilatory pace of informatisation 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 (WEF 2014, WEF 2011).

The statement from Xi in August 2014 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 mechanised warfare".

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" (Reuters 2014b). 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. Also in September 2014, the U.S. Special Envoy for the coalition against IS, retired General John Allen, told a meeting in Kuwait that there needed to be a cyberspace strategy from its members (Haaretz 2014). The need for Australia to combat irregular and low-technology forces is not a reason to de-emphasise information warfare. On the contrary, clever exploitation of advanced ICT technologies can be used to undermine any organised 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.

Conclusion

Outside Australia, military actors of high interest to us are moving rapidly into higher levels of digital war and operations. Inside Australia, the environment for decision-making on defence policy for the information age is severely hamstrung by the national environment in the civil domain. The picture in that domain is one of falling competitiveness and only medium (to low) levels of innovation. Australia needs a digital age strategy for its civil sector before it can have a digital military strategy. Australia is falling behind the pace in entrenching digital innovation in our society. Perhaps the Defence organisation in Australia can take something of a lead to reverse this situation in the country as a whole. But it would need to recognise at the outset that the level of expertise in Australia in military applications in this field, as in many other countries, is low. We need new foreign allies in this field. The experience levels that key decision-makers in defence policy have of the IT sector do not in many cases match the nature of the problem. There would have to be a commitment to deeper organisational change, especially in force structure. The effort would need to be multi-national, multi-sector (including the Communications and Education Departments) and private-public. Stuart Robert, the current Minister Assisting the Minister for Defence, and a former military officer, does have a Master's degree in Information Technology. Perhaps he could help drive the policy changes needed. Above all, the Australian government needs to match its obsession with cyber espionage threats with an equal passion for IT innovation across the board: in health, in agriculture, and in education.

The following steps of high relevance to the defence sector may be usefully considered:

- As a matter of urgency, appoint a specialist panel to analyse Australia's digital work force and to develop a new national strategy dedicated exclusively to its rapid development
- Use the Chubb 21-point plan for STEM education as the foundation for that report
- Use the Chubb 21-point plan for STEM education as the national benchmark for evaluating Australia's year on year educational improvements in our civil IT skills base
- As a matter of urgency, commission a report on community and business attitudes to cyberspace as they pertain to national security needs.
- Invite the Australian 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
- 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)
- Consider the establishment of powerful but flexible digital militia forces (reservists) capable of rapid mobilisation in major capital cities in highly secure spaces in the capitals or other nearby locations.

References

ADF. 2014. *Information Activities*, ADDP 3.13, Canberra: Australian Defence Force. Available at: http://www.defence.gov.au/FOI/Docs/Disclosures/330_1314_Document.pdf

Australian Army. 2014. *Future Land Warfare Report 2014.* Available at: http://www.army.gov.au/~/media/Files/Our%20future/Publications/FLWR_Web_B5_Final.pdf

ISSN 2203-1693. Copyright © 2014 The Author(s). http://doi.org/10.7790/ajtde.v2n4.68

ACS. 2011. Australian Computer Society, *Australian ICT Statistical Compendium 2011*. Available at: http://www.acs.org.au/__data/assets/pdf_file/0019/9307/Australian-ICT-Statistical-Compendium-2011.pdf

ACS. 2013. Australian Computer Society, *Australian ICT Statistical Compendium 2013*. Available at: https://acs.org.au/__data/assets/pdf_file/0004/28570/Australian-ICT-Statistical-Compendium-2013.pdf

Austin, Greg. 2014. *Cyber Policy in China*. Cambridge: Polity Press

Chief Scientist. 2014a. "Professor Chubb Releases 'Science, Technology, Engineering and Mathematics: Australia's Future', Press Release, Office of the Chief Scientist, Canberra, 2 September 2014. Available at: http://www.chiefscientist.gov.au/2014/09/professor-chubb-releases-science-technology-engineering-and-mathematics-australias-future/

Chief Scientist. 2014b. *Science, Technology, Engineering and Mathematics: Australia's Future*, Office of the Chief Scientist 2014, Australian Government, Canberra. Available at: http://www.chiefscientist.gov.au/wp-content/uploads/STEM_AustraliasFuture_Sept2014_Web.pdf

Coalition. 2013. "The Coalition's Policy for E-Government and the Digital Economy". Brian Loughnane, Canberra ACT, August 2013

Dept. of Communications. 2013. *Advancing Australia as a Digital Economy*,. Available at: http://apo.org.au/files/Resource/Advancing-Australia-as-a-Digital-Economy-BOOK-WEB.pdf.

Dept. of Defence. 2013. *Defence White Paper 2013*. Available at: http://www.defence.gov.au/whitepaper2013/docs/WP_2013_web.pdf

Dept. of Education. 2014a. 2013 Award Course Completions, 14 July 2014. Available at: http://docs.education.gov.au/node/35987

Dept. of Education. 2104b. Completion Rates of Domestic Bachelor Students: A Cohort Analysis, 2014, p. 15. Available at: http://docs.education.gov.au/system/files/doc/other/completion_rates_of_domestic_bachelor_students_-_a_cohort_analysis_1.pdf

Haaretz. 2014. “U.S. unveils new cyber coalition aimed at combating ISIS”, 28 October 2014. Available at: haaretz.com, http://www.haaretz.com/news/middle-east/1.623096

Japan. 2013. “Cybersecurity Strategy: Towards a World-leading, Resilient and Vigorous Cyberspace”, Tokyo: Information Security Policy Council. Available at: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/JAP_NCSS2.pdf

Japan Times. 2103. “Japan, U.S. agree to beef up cybersecurity”, *Japan Times*, 3 October 2013. Available at: http://www.japantimes.co.jp/news/2013/10/03/national/politics-diplomacy/japan-u-s-defense-chiefs-meet-on-cybersecurity/#.VFQKzxbgU71

Karunaratne, Neil Dias 1989. “A Rapid Informatisation Strategy for Australia: An Impact Analysis”, *Economic Systems Research*, Vol. 1 (4), 465-79.

Keating, Paul L. 1997. “Cyberpolities - Australia, Asia and the Information Revolution”, SUGA ‘97 Conference, Hilton Hotel, Sydney, 5 August 1997. Available at: http://www.keating.org.au/shop/item/cyberpolities-the-information-revolution---5-august-1997

PWC. 2014. *Deciding with data: How data-driven innovation is fuelling Australia’s economic growth*, Price Waterhouse Coopers on behalf of Google. Available at: http://www.pwc.com.au/consulting/assets/publications/Data-drive-innovation-Sep14.pdf

Reuters. 2104a. “China's Xi urges army to create strategy for information warfare”, 30 August 2014. Available at: http://www.reuters.com/article/2014/08/30/us-china-xi-defence-idUSKBN0GU0H020140830

Reuters. 2104b. Doina Chiachu, “U.S. NSA chief says monitoring tech-savvy Islamic State”, 16 September 2014. Available at: http://www.reuters.com/article/2014/09/16/us-cybersecurity-usa-islamic-state-idUSKBN0HB22A20140916

United States. 2011. “Department of Defense Strategy for Operating in Cyberspace”, Washington DC. Available at: http://www.defense.gov/news/d20110714cyber.pdf

United States. 2012a. “Presidential Policy Directive 20: U.S. Cyber Operations Policy”, The White House, 2012, Available at: http://fas.org/irp/offdocs/ppd/ppd-20.pdf

United States. 2012b. "Information Operations", Washington DC: The Joint Chiefs of Staff, November 2012, Joint Publication 3-13, Available at: http://www.dtic.mil/doctrine/new_pubs/jp3_13.pdf

Waters, Gary; Ball, Desmond; Dudgeon, Ian. 2008. *Australia and Cyber-Warfare*, Canberra Papers in Strategy and Defence, Australian National University ePress. Available at: http://press.anu.edu.au/wp-content/uploads/2011/08/whole_book5.pdf

Watson, Chris. 2007. "Joint Information Operations: The Way Ahead", *Australian Army Journal*, Vol. 4 (1), 77-98. Available at: http://www.army.gov.au/Our-future/Publications/Australian-Army-Journal/Past-editions/~/media/Files/Our%20future/LWSC%20Publications/AAJ/2007Autumn/07-JointInformationOperati.pdf

WEF. 2004. *Global Information Technology Report 2003-2004*, New York: Oxford University Press, for the World Economic Forum and others, 2004. Available at: http://www-wds.worldbank.org/servlet/WDSContentServer/IW3P/IB/2005/11/17/000090341_20051117162002/Rendered/PDF/343090GITR2003.pdf

WEF. 2011. *Global Information Technology Report 2010-2011*, New York: Oxford University Press, for the World Economic Forum and others, 2011. Available at: http://www3.weforum.org/docs/WEF_GITR_Report_2011.pdf

WEF. 2013. *Global Information Technology Report 2013*, New York: Oxford University Press, for the World Economic Forum and others. Available at: http://www.weforum.org/reports/global-information-technology-report-2013

WEF. 2014. *Global Information Technology Report 2014*, New York: Oxford University Press, for the World Economic Forum and others. Available at: http://www.weforum.org/reports/global-information-technology-report-2014

ISSN 2203-1693. Copyright © 2014 The Author(s). http://doi.org/10.7790/ajtde.v2n4.68