The Case for an Offensive ADF Cyber Capability: beyond the Maginot mentality

Colonel Michael Lehmann, CSC, Australian Army

As our case is new, so we must think anew and act anew.

President Abraham Lincoln, 1862 [1]

Introduction

Australia faces a military technological environment arguably more challenging than at any time since World War 2. Asian economies are growing rapidly, albeit with temporary but painful setbacks, and are closing on Australia's. This shrinking economic gap brings with it potential increases in military expenditure, allowing Asian military forces to field advanced technology. China's People's Liberation Army (PLA) is the most obvious example of this trend, developing powerful conventional military capabilities, such as the J-31 fighter aircraft, the much-touted DF-21D 'carrier killer' missile, and its first aircraft carrier. As importantly, the PLA is training to use these new capabilities as systems in a networked, joint environment.[2] The PLA is a harbinger of what political will and money can achieve.

While Australia still believes it has a conventional military edge in its region—and is spending big on air, maritime and ground systems to maintain this edge—population-driven economics suggest that Australia will lose its comparative purchasing advantage over the long term. If Australia's future security depends at least partially on a military edge, then trying to outspend Asia is likely to be a dead-end strategy. One area where new technological opportunities and a privileged relationship with the US potentially coincide is offensive cyber 'weaponry'. Examining these factors, this article contends that the ADF should, indeed must, move rapidly to field an offensive cyber capability as an integral part of a truly joint force.

The logic of the dollar

For over 30 years, Australia's Defence White Papers have painted a picture of a military which could comfortably assume a technological edge over potential adversaries, largely due to our relationship with the US and access to its technologies. While regional militaries were something for the government to consider, they were not regarded as peers, possessing '[modest] capabilities appropriate to national defence and internal security'.[3] It was not until 2009 that a Defence White Paper raised substantial concerns, fretting that while Australia's technology advantage gave the ADF a 'war-winning edge', its sustainability was under 'increasing challenge'.[4]

This concern is based on economic near certainty. By 2030, Australia's economy is projected to slip from 19th to the 23rd largest in the world, slightly smaller than Thailand's, neck-and-neck with Malaysia's and The Philippines', and eclipsed by an Indonesian economy 18 ranks above it and over three times its size.[5] Assuming that the military expenditure of regional countries grows along with their economies, the existing technology gap will inexorably shrink. Australia's response needs new thinking and new actions.

The logic of cyberspace

To preserve Australia's military edge, the 2009 Defence White Paper placed considerable faith in the ADF's ability to use its technologies better. It foresaw a networked system whose sensors and data would give 'information superiority over an adversary so that our people can make critical decisions on the battlefield more quickly'.[6] This tantalising possibility is the world of a supercharged 'Boyd cycle', fuelled by digitalised information, pumped through secure and practically-unlimited communications pipes, filtered and presented by smart technologies, and exploited by technologically-savvy military staff.[7] The logic of the future dollar, however, suggests that a networked military will be affordable for regional countries as well. However, a networked military is also vulnerable to cyber attacks against that network,

causing potentially cascading disruption, where the corruption of one element of the system ripples through its interdependent whole.

But is this threat more than academic hype? Publicly-available evidence suggests so. In its dry bureaucratic language, the 2015 US *Cyber Strategy* notes that its offensive cyber capabilities are designed to inflict 'unacceptable losses' on an attacker.[8] It goes on to say that US cyber targets include 'command and control networks, military-related critical infrastructure, and weapons capabilities'.[9] More specifically, the *Cyber Strategy* highlights the potential vulnerability of weapons systems to cyber attack by saying that the US must 'mandate specific cybersecurity standards for weapons systems'.[10] This strongly suggests the US believes that weapons systems are able to be defeated by cyber attacks.

While speculative, this would presumably include any software-driven weapons function, such as target acquisition, external and onboard guidance systems, arming functions and fail-safes, and digital fly-by-wire control systems. These potential vulnerabilities are inherent to all so-called Fifth Generation platforms, such as Australia's new F35 Lightning II. This cutting-edge aircraft is the host for 'millions of lines of code' in 'an incredibly integrated design' which meshes its capabilities with others across the battlespace.[11]

Additionally, a significant strength of Fifth Generation platforms comes from shared databases, such as Intelligence Mission Data which, among other things, distinguish between friends, foes and civilians..[12] Although protected, Fifth Generation platforms highlight the potential for cyber attacks to target networked military systems and achieve cascading effects. By killing the code or corrupting data, incredibly expensive platforms may be rendered useless.

Coincidentally, apart from its concern over the sustainability of Australia's technological advantage, the 2009 Defence White Paper also raised cyberspace as an issue for national security, noting that the ADF had an 'increasing reliance on networked operations'.[13] However, no Defence White Paper has looked at these two concerns as an opportunity. Modernising regional militaries are also exposed to the inherent vulnerabilities of networked systems. Here lies the potential for continued military advantage if the ADF is bold enough to seize it.

The cyberspace race

> Everybody is moving towards developing offensive cyber capabilities.
>
> General Keith Alexander, Commander US Cyber Command, June 2014 [14]

With widespread reports of the Chinese using cyber attacks to steal the political, economic and security secrets of Western nations, with Russia alleged to have synchronised cyber attacks with military operations in Georgia, and the US and Israel said to have used the Stuxnet virus against the Iranian nuclear program, it is little wonder that a considerable number of nations are interested in offensive cyber capabilities. While claiming that 'everyone' is doing so is doubtless an exaggeration—and acknowledging that there are critics of the hype associated with 'cyberwar'[15]—a former US Deputy Secretary of Defense has stated publicly that over 30 countries are developing military cyber capabilities, some of which are offensive.[16]

The US appears to regard Russia as being the most advanced cyber threat it faces, rating it in early 2014 as 'more severe than we have previously assessed'.[17] China is also regarded as an advanced threat, followed by the 'lesser' capabilities of North Korea and Iran.[18] In the Indo-Pacific region, it is uncertain which countries have offensive cyber capabilities. Indonesia, for example has recently moved to set up both military and national cyber organisations but—at least publicly—their remits are defensive.[19] Regardless, it is logical that the more technologically advanced a country is, the more likely it is to have at least some offensive cyber capabilities.

US and Chinese offensive cyber capabilities

It is reasonable to ask, however, if offensive cyber capabilities have practical military use beyond digital espionage, information operations and niche disruption? If cyber attacks actually threaten modern

military systems and offer an appreciable operational advantage, then there should be doctrinal and practical evidence of this? There is. The Chinese and American militaries possess some of the world's most advanced warfighting capabilities, and their intellectual and practical investments in offensive cyber capabilities suggest that ignoring the place of cyber weaponry in 21st century joint warfare is akin to ignoring the place of the tank in combined arms operations nearly a 100 years ago.

The US position is based on the recognition that cyber weapons will be used against it in the future and 'assumes that a potential adversary will seek to target US or allied critical infrastructure and military networks to gain a strategic advantage'.[20] The US also intends to fight back and actively wage war in cyberspace. In April 2015, it stated that the Department of Defense's three cyber missions were defending military networks; assisting the US respond to cyber attacks against non-defense interests; and providing 'offensive cyber options'.[21] General Alexander had previously confirmed that the US Cyber Command was prepared to conduct 'full spectrum military cyber-space operations' against adversaries.[22] He went further and said that possessing the 'best' cyber weaponry is as important to battlefield success as having the 'best' tanks, artillery and infantry.[23]

The US is backing its words with resources, moving quickly to establish a substantial cyber force with both defensive and offensive capabilities. The Department of Defense's expansive cyber vision sees it establishing a 6200-person 'Cyber Mission Force' by 2018, comprising 133 cyber teams, of which 81 would have a primarily defensive role, 27 an offensive role, and 25 would be employed in analytical and planning roles.[24]

Within the US Army, serious efforts to institutionalise cyber capabilities have been taking place since at least 2010, when the Army directed the establishment of an Army Cyber Command. These efforts have only accelerated over the past few years with the Army in the process of fielding 62 cyber teams, aiming to have them fully operational by the end of September 2017. The regular Army's 41 teams will have both offensive and defensive capabilities, while the Reserve teams will be focused on 'cyber protection'.[25]

The US Navy has taken a similar approach, trying to mainstream cyber capabilities in an Information Dominance Corps, publishing a cyber *Strategic Plan 2015-2020*, and committing to the establishment of 40 cyber teams by 2017.[26] Like their counterparts in the Army, some of these Navy teams will have the dedicated offensive role of delivering cyber warfighting effects as part of Navy's integrated fires. Navy's plan for these cyber teams appears ambitious, as it has committed to increasing their effectiveness by 75 per cent, against unknown internal benchmarks, by mid-2016.[27]

The US Air Force's long-term strategy is more coy on its plans for offensive cyber capabilities, while acknowledging that cyberspace promises a 'true breakthrough in our approach to Air Force core missions' and may offer 'more attractive (non-kinetic) options' to commanders to strike adversaries.[28] However, greater insight is offered in a 2008 US Air Force strategic cyber vision which says that it will use cyber attacks to disrupt sensors and command and control systems, manipulate data, and degrade weapon systems.[29] These plans are more than aspirational. The 24th Air Force has demonstrated the ability to deliver cyber 'payloads' from aircraft, from space, and by 'traditional means'.[30] So practical cyber weaponry exists.

One of the notable aspects of the US approach to building its cyber capabilities is its urgency. The fielding of the US Army's first 1200 cyber soldiers in its three new cyber specialties is being done before the Army has the courses or facilities to train them, in a learning-by-doing approach.[31] Similarly, the US Navy's strategic cyber plan implicitly recognises the embryonic nature of its cyber force, using words and phrases like 'create', 'establish and mature', 'institutionalize', and 'develop' in its goals. These approaches mirror those of the US Department of Defense, with its Secretary outlining plans for substantial growth in military cyber forces even while noting that 'we're just beginning to build and imagine this cyber force'.[32]

Indeed, the foundations for this cyber force are not fully set, with the Department acknowledging that its legal and policy authorities are not yet finalised, its structures are not yet mature, its career paths not yet fully viable, its training requirements undefined, and its teams not yet integrated into the Department.[33] Yet instead of being seen as a failing, risky as it may be, this approach is bold, agile and future focused. The US cyber vision is one of a force that is not limited by the domain-constrained thinking of individual Services; a force that is aggressively modern, that embraces risk, that seeks change, and goes beyond joint to be truly national.

The US emphasis on offensive cyber operations as part of an integrated modern force is also shared by the PLA. The Chinese embrace of offensive cyber operations is explicitly stated in its 2013 near-doctrinal *The Science of Military Strategy*, which has a chapter on cyber warfare, including cyber attack.[34] The conceptual antecedents of this thinking can be clearly seen in the PLA's goal of being able to 'win local wars under conditions of informationalisation'.[35] They are also discernible in the even earlier writings of Chinese strategists who predicted that cyberspace would become a warfighting domain and that cyber attacks were a necessary 'new concept' weapon.[36]

Like the US military, the Chinese have moved beyond words to actions. Doctrinally, the PLA has elevated cyberspace to the same status as the other domains of land, air, maritime and space. Practically, to operate in this new domain, the PLA fields extensive defensive and offensive cyber forces. While their structure and numbers are uncertain, it is believed that the PLA's Fourth Department is probably responsible for cyber attack, along with its more traditional electronic warfare mission.[37]

Additionally, the PLA's Third Department has 'one of the largest and most sophisticated … [signals intelligence] and cyber collection infrastructures in the world', which may include the ability to conduct cyber attacks in addition to its cyber espionage role.[38] Finally, there are PLA cyber elements known as Technical Reconnaissance Bureaus in the seven Military Regions and in the Army, Navy, Air Force and the strategic missile force (the Second Artillery). These bureaus are known to have cyber security and collection roles but any offensive role is only inferred from doctrine.

The Australian perspective on cyber attacks – prevention without cure?

Given these exemplars, how should Australia respond? What should it think? What should it do?

To this point, Australia's approach to military power in cyberspace has been largely that of a victim. The preponderance of government policy and public discussion has focused on protecting internet-facing systems and data against attack, while often acknowledging that such efforts cannot be absolute and may well be quixotic. An example is Marcus Thompson's article 'The Cyber Threat to Australia', which lays out Australia's strategic and military vulnerability to cyber attacks but—with the exception of one sentence—is focused on prevention.[39] Similarly, a recent call for an update to Australia's 2009 *Cyber Strategy* almost exclusively assumes that cyber security is defensive.[40]

There is no question that Australia's cyber interests need comprehensive, integrated and world-class defensive capabilities. But the risk in limiting the discussion of cyber security to defensive measures is that this strategy advocates, probably unthinkingly, a cyber 'Maginot line', ceding the initiative to any attacker beyond the reach of law enforcement. There is no cyber deterrent and there are no options for government in such an approach.

However, some have begun to call for Australia to develop cyber offensive capabilities. In a 2013 article, Nick Rose wrote about US concepts for offensive cyber operations and suggested that military planners should consider incorporating cyber reconnaissance and attacks into their thinking.[41] In mid 2014, ADF doctrine suggested that offensive cyber operations had a place in Information Operations, providing a tantalising glimpse of what a resourced offensive cyber capability might achieve, while limiting the vision of what these capabilities could do in a networked future by subordinating them to existing military thinking.[42]

More recently, in early 2015, Rory Metcalf argued that Australia should seek 'asymmetric security advantages' to meet the challenges of a networked, uncertain world, and called for significantly greater investment in emerging military capabilities, including cyber.[43] Similarly, former ASIO chief David Irvine echoed the need for a 'huge' resourcing of cyber capabilities and, notably, advocated for offensive capabilities as part of this mix.[44]

An ADF offensive cyber capability

So if an ADF offensive cyber capability would be a potential warfighting edge for Australia, what should it look like and how should the ADF go about trialling it? The first thing that Australia needs is an ongoing debate on the place of cyber weaponry in ADF operations, including the legal and policy guidelines for the

accountable and principled use of such capabilities. While specifics of cyber capabilities may be highly classified, the ubiquity of the internet and the issues surrounding offensive cyber attacks for military purposes warrant frank and inclusive discussion.

However, the legal, policy and conceptual issues around military cyber attacks should not prevent the ADF from immediately establishing a prototype offensive cyber unit. The purpose of this unit would be to develop and evaluate a trial offensive cyber capability to support ADF operations, providing decision makers with an agile and cutting-edge 'laboratory' to assess the desirability and practicality of a longer-term investment in this area.

The formation of this unit would need to be supported by a unique approach to finding personnel with the necessary knowledge, skills and attitude for cyber warfare. The cyber attack unit should be staffed by a mixture of people from the Services, the Reserve, contractors, secondees from private industry and, possibly, academia. An Australian cyber unit should draw its people from wherever expertise, enthusiasm and security clearance requirements coincide.

Additionally, to remove the cyber unit from the possibility of existing parochial interests, it should be under the command of the Vice Chief of the Defence Force, reflecting that cyberspace appears to be a genuinely new domain. This would also establish the capability as truly and inarguably joint, provide a senior 'champion' to drive it, and remove the capability from capture by existing interests. But this should not be done in a way that effectively isolates the unit from existing knowledge and experience. In particular, the ADF must leverage the extensive cyber security expertise of the Australian Signals Directorate, including its familiarity with legislative and policy compliance.[45]

Finally, if the ADF is to develop an effective offensive cyber capability, it should approach the US to leverage off its military programs. This would appear to be a half-open door. The US has noted that it cooperates in cyber defence with 'Five Eyes' nations and it has incorporated partnerships into the fabric of its cyber future by including them as one of its five strategic goals.[46] Perhaps tellingly, the first photograph in the US *Cyber Strategy* features two uniformed ADF personnel working with US counterparts.

However promising this may be, US willingness to go beyond cyber security cooperation is unclear. Although there is some evidence that the US has worked with partners in delivering offensive cyber effects, there is no specific mention of partners in any of the *Strategy's* language on offensive capabilities.[47] Regardless, Australia has relied considerably on privileged access to US technology and this could reasonably be expected to continue for cyber weaponry.

Conclusion

The air-sea gap is irrelevant to Australia's cyber security. Australia has multiple cyber 'borders' interfacing with the globe in ways that no-one truly understands. What is clear, however, is that modern military systems whose effectiveness depends on their networked nature are potentially vulnerable to cyber attacks. Leading militaries have already wrapped cyber attacks into their military operating concepts and are investing heavily in cyber forces.

For Australia, which relies on technology to maximise the capability of its small military, there is both a threat and an opportunity in these developments. There is no question that the ADF needs world-class defensive capabilities. However, as it is for any military capability, it is not enough that the ADF be able to take a punch. The ADF should, indeed must, move rapidly to field offensive cyber capabilities as an integral part of a truly joint force.

In the era of a new Defence White Paper and fiscal constraint, this is undoubtedly a challenge for Defence's leadership. The comfort of investing in familiar capabilities that see more, go faster and shoot further is likely to be misleading in a networked future. The question for the ADF is one of vision. Can the ADF marry a new opportunity with new thinking and new action?

Colonel Mick Lehmann has served in a variety of staff, command and operational positions in Australia, overseas and on operations. He is a graduate of the Defence and Strategic Studies Course, has three Masters degrees and is currently the Senior Military Advisor in the Office of NATO's Senior Civilian Representative in Kabul, Afghanistan.

Notes

1 From his Second Annual Message, delivered to the Senate and House of Representatives in December 1862, available at <http://www.presidency.ucsb.edu/ws/?pid=29503> accessed 9 September 2015.

2 Jonathan Holslag, 'Trapped Giant: China's military rise', *Adelphi Papers*, Vol. 50, No. 416, 2010, pp. 40-1 and 63-5.

3 Department of Defence, *The Defence of Australia*, Commonwealth of Australia: Canberra, March 1987, p. 13.

4 Department of Defence, *Defending Australia in the Asia Pacific Century: Force 2030 (Defence White Paper 2009)*, Commonwealth of Australia: Canberra, 2009, pp. 67 and 131. These concerns are also echoed in Department of the Prime Minister and Cabinet, *Australia in the Asian Century White Paper*, Australian Government: Canberra, October 2012, pp. 7 and 226, albeit that document has subsequently been 'archived' by the current government.

5 Price Waterhouse Coopers, 'The World in 2050: will the shift in global economic power continue?', *PricewaterhouseCoopers* [website], February 2015, p. 8, available at <http://www.pwc.com.au/consulting/assets/publications/World-in-2050-Feb15.pdf> accessed 6 June 2015.

6 Department of Defence, *Defending Australia in the Asia Pacific Century*, p. 131.

7 Boyd's key concept was that of the decision cycle or OODA (observe, orient, decision, action) loop, the process by which an entity (either an individual or an organisation) reacts to an event: see, for example, 'John Boyd (military strategist)', available at <https://en.wikipedia.org/wiki/John_Boyd_(military_strategist)> accessed 9 September 2015.

8 US Department of Defense, *The Department of Defense Cyber Strategy*, April 2015, p. 11, available at <http://www.defense.gov/News/Special-Reports/0415_Cyber-Strategy> accessed 8 May 2015.

9 US Department of Defense, *The Department of Defense Cyber Strategy*, p. 14.

10 US Department of Defense, *The Department of Defense Cyber Strategy*, p. 21.

11 Cheryl Pellerin, 'Kendall: F-35 marks US-Australia milestone', *DoD News* [website], 25 July 2014, available at <http://www.defense.gov/news/newsarticle.aspx?id=122756> accessed 17 May 2015.

12 US Department of Defense, 'Management of Intelligence Mission Data (IMD) in DoD Acquisition', Directive No. 5250.01, *Department of Defense* [website], 22 January 2013, available at <www.dtic.mil/whs/directive/corres/pdf/525001p.pdf> accessed 17 May 2015.

13 Department of Defence, *Defending Australia in the Asia Pacific Century*, p. 83.

14 Christopher Joyce, 'Interview transcript: former head of the NSA and commander of the US cyber command, General Keith Alexander', *The Australian Financial Review* [website], 8 June 2014, available at <www.afr.com/Page/Uuid/b67d7b3e-d570-11e3-90e8-355a30324c5f> accessed 8 May 2014.

15 Examples of the arguments of critics can be found at Thomas Rid, 'Cyber War Will Not Take Place', *Journal of Strategic Studies*, Vol. 35, No. 1, February 2012, pp. 5-32; and Martin C. Libicki, 'Don't Buy the Cyberhype: how to prevent cyberwars from becoming real ones', *Foreign Affairs* [website], 14 August 2013, available at <https://www.foreignaffairs.com/articles/united-states/2013-08-14/dont-buy-cyberhype> accessed 6 June 2015.

16 William J. Lynn III, 'The Pentagon's Cyberstrategy, One Year Later', *Foreign Affairs* [website], 28 September 2011, available at <www.foreignaffairs.com/articles/68305/william-j-lynn-iii/the-penatgons-cyberstrategy-one-year-later> accessed 19 August 2014; also Ash Carter, 'Rewiring the Pentagon: charting a new path on innovation and cybersecurity' Drell Lecture at Stanford University, 23 April 2015, available at <http://www.defense.gov/Transcripts/Transcript.aspx?TranscriptID=5621> accessed 25 April 2015.

17 Tony Capaccio, 'Iran behind cyberattack of Las Vegas gambling juggernaut, US says', *The Canberra Times* [website], 27 February 2015, available at <http://www.canberratimes.com.au/act/it-pro/security-it/ian-behind-cyberattack-of-las-vegas-gambling-juggernatut,us-says-20150227-13q7xa.html> accessed 2 March 2015.

18 Capaccio, 'Iran behind cyberattack of Las Vegas gambling juggernaut, US says'.

19 Prashanth Parameswaran, 'Indonesia's cyber challenge under Jokowi', *The Diplomat* [website], 21 January 2015, available at <http:the diplomat.com.2015/01/indonesias-cyber-challenge-under-jokowi/> accessed 22 January 2015.

20 US Department of Defense, *The Department of Defense Cyber Strategy*, p. 2

21 Carter, 'Rewiring the Pentagon'.

22 Joyce, 'Interview transcript'.

23 Joyce, 'Interview transcript'.

24 US Department of Defense, *The Department of Defense Cyber Strategy*, p. 6.

25 David Vergun, 'Cyber chief: Army cyber force growing "exponentially"', *US Army* [website], 5 March 2015, available at <http://www.army.mil/article/143948/Cyber_chief__Army_cyber_force_growing__exponentially> accessed 5 March 2015.

26 US Fleet Cyber Command/10th Fleet, *Strategic Plan 2015*-2020, available at <http://www.navy.mil/strategic/FCC-C10F%20Strategic%20Plan%202015-2020.pdf> accessed 10 September 2015.

27 US Fleet Cyber Command/10th Fleet, *Strategic Plan 2015*-2020, pp. 3 and 16.

28 US Air Force, 'America's Air Force: a call to the future (30 year strategy)', *Department of the Air Force* [website], July 2014, p. 17, available at <http://airman.dodlive.mil/files/2014/07/AF_30_Year_Strategy_2.pdf> accessed 7 June 2015

29 Air Force Cyber Command, *Strategic Vision*, February 2008, p. 12, available at <www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA479060> accessed 7 June 2015.

30 24th Air Force Public Affairs, 'Integrated operations hit cyber bull's-eye', *Air Force Print News Today* [website], 5 November 2014, available at <www.24af.af.mil/news/story.asp?id=123430672> accessed 7 June 2015.

31 Fort Gordon Public Affairs Office, 'Army Cyber branch offers soldiers new challenges, opportunities', *US Army* [website], 24 November 2014, available at <http://www.army.mil/article/138883/Army_Cyber_branch_offers_Soldiers_new_challenges__opportunities> accessed 17 March 2015.

32 Carter, 'Rewiring the Pentagon'.

33 US Department of Defense, *The Department of Defense Cyber Strategy*, pp. 7 and 17.

34 See, for example, Steven Aftergood, 'Secrecy News: China's Science of Military Strategy (2013)', *Federation of American Scientists* [website], 3 August 2015, available at <https://fas.org/blogs/secrecy/2015/08/china-sms/> accessed 10 September 2015.

35 Information Office of the State Council, 'The Diversified Employment of China's Armed Forces', April 2013, p. 3, available at <http://news.xinhuanet.com/english/china/2013-04/16/c_132312681.htm> accessed 22 April 2013.

36 Qiao Liang and Wang Xiangsui, *Unrestricted Warfare*, PLA Literature and Arts Publishing House: Beijing, February 1999, pp. 68-9 and 24-6 respectively, available at <http://www.c4i.org/unrestricted.pdf> accessed 10 September 2015.

37 Peter Mattis, 'The Analytic Challenge of Understanding Chinese Intelligence Services', *Studies in Intelligence*, Vol. 56, No. 3, September 2012, p. 50.

38 Bryan Krekel, Patton Adams and George Bakos, *Occupying the Information High Ground: Chinese capabilities for computer network operations and cyber espionage*, Northrop Grumman: Falls Church, 7 March 2012, p. 47; Mark A. Stokes, Jenny Lin and L.C. Russell Hsiao, 'The Chinese People's Liberation Army Signals Intelligence

and Cyber Reconnaissance Infrastructure', *Project 2049 Institute* [website], 11 November 2011, p. 4, available at <http://project2049.net/documents/pla_third_department_sigint_cyber_stokes_lin_hsiao.pdf> accessed 28 April 2013.

39 This is not meant as a criticism of the article nor its conclusions but as an example of the nature of professional discussion on cyber capabilities: see Marcus Thompson, 'The Cyber Threat to Australia', *Australian Defence Force Journal*, No. 188, 2012, p. 63.

40 Chris Brookes, 'Cyber Security: time for an integrated whole-of-nation approach in Australia', *Indo-Pacific Strategic Papers* [website], March 2015, available at <http://www.defence.gov.au/ADC/Publications/IndoPac/150327%20Brookes%20IPS%20paper%20-%20cyber%20(PDF%20final).pdf> accessed 10 September 2015.

41 Nicholas Rose, 'Shaping the Future Battlespace: offensive cyber warfare tools for the planner', *Australian Army Journal*, Summer edition 2013, Vol. X, No. 4, pp. 53-68.

42 Philip Dorling, 'Military backs cyber warfare against foes', *The Age*, 8 May 2014.

43 Rory Metcalf, 'Towards a New Australian Security: speech by Professor Rory Metcalf', *ANU* [website], 17 March 2015, available at <http://www.anu.edu.au/news/all-news-towards-a-new-australian-security-speech-by-professor-rory-metcalf> accessed 17 March 2015.

44 Mark Eggleton, 'Confronting the new face of war', *The Australian Financial Review*, 16 March 2015.

45 Dorling, 'Military backs cyber warfare against foes'.

46 US Department of Defense, *The Department of Defense Cyber Strategy*, pp. 4 and 8.

47 James R. Burleigh, 'Cyber goes to war', *Air Force Print News Today* [website], 7 December 2012, available at <www.24af.af.mil/news/story.asp?id=123329133> accessed 7 June 2015.