Bridging the gap between cyber strategy and operations: a missing layer of policy

Major Christopher Wardrop, Australian Army

Introduction

Whether one is a proponent of the 'information revolution' or a more gradual evolution in the development, use and reach of information communications technology, there can be no denying that the emergence of cyberspace and the ever-increasing interconnectedness of technology has had significant social, economic and political effect in Australia and globally.[1]

In 2005, Charles Weiss detailed how advances in science and technology have subtly yet fundamentally altered concepts of security, sovereignty and power.[2] Developed and developing nations are coming to understand, prioritise and deal with these changes differently, as reflected through the variety of approaches taken in national cyber strategy documents.[3]

The Australian Government recognises that the cyber threat is increasing and presents a genuine risk to Australia's national security and economic prosperity, as well as the ADF's warfighting capability.[4] Indeed, the unique characteristics of cyber operations present one of the most significant challenges to modernisation of the ADF, with the *2016 Defence White Paper* emphasising the importance of strengthening national cyber capabilities.[5]

Australia's current cyber security strategy commits $400 million to strengthening cyber capabilities over the next ten years but does not include any specific tasks, roles or responsibilities for the ADF.[6] As observed by then Brigadier Marcus Thompson, the *2016 Defence White Paper* 'emphasises the development of cyber security capabilities'—and Australia's investment program funds such development—yet 'an additional layer of actionable policy is required to ensure appropriate implementation of the Government's intent at the operational and tactical levels'.[7]

This article seeks to identify who is responsible for formulating and enacting the policy to

bridge the gap between strategic intent and operational planning and implementation. It also defines the cyber domain and threats, identifies the key challenges of military cyber operations, and examines the trajectory for the growth of cyber capabilities within the ADF.

One of the challenges of this analysis in the Australian context is the lack of operational policy and doctrine in the public domain. It is likely that many of the considerations discussed below have already been made and that a large body of work has been completed or is well underway. This is, of course, a problem in itself, as the limited distribution of such policy does little to raise awareness or encourage discussion of cyber security and operational issues more broadly among Defence commanders and their headquarters staff.

Responsibility

In a sign of the importance that the Australian Government places on cyber security, its most recent cyber security strategy was released by the Department of the Prime Minister and Cabinet, rather than the Attorney-General's Department (which had previous carriage of cyber policy).[8]

Within Defence, responsibility for the development of policy on cyber operations has not always been clear, with no champion until relatively recently. However, the Vice Chief of the Defence Force is now the capability manager, with the newly-formed Information Warfare Division, part of Joint Capabilities Group, having responsibility to identify existing cyber capabilities and gaps, develop a coherent joint capability, and integrate cyber operations into and across Defence.[9]

It is recognised, however, that the development of policy and doctrine has a broad range of stakeholders, including the Prime Minister and Cabinet, law-enforcement agencies, strategic intelligence agencies, Headquarters Joint Operations Command, the three Services, and defence industry and its commercial partners, as well as Australia's allies and coalition partners.

This means that while the Vice Chief of the Defence Force is ultimately responsible for the development and implementation of military-related cyber capabilities, policy must be developed with broad consultation and cooperation in order to be effective.

Characteristics of the cyber domain

To formulate any policy to bridge the gap between Australian cyber strategy and operational-level requirements, it is vitally important to first understand both the technological context in which Defence operates and the key characteristics of cyberspace and the cyber domain.

Since 2008, the ADF has made significant progress in improving its command, control, computing, communications, intelligence, surveillance and reconnaissance (C4ISR) capabilities.[10] Much of this progress has been made through the acquisition of major platforms by Navy and Air Force, and ongoing efforts to digitise and modernise Army's command, control and communications systems.[11]

Modern Western military forces have relied on communications networks and technology to enable 'decision superiority' to bring overwhelmingly lethal force to bear at decisive moments in space and time, with the conventional joint land combat phases of the 1991 Gulf War and the 2003 Iraq War often cited as striking examples of the military success that decision superiority can afford.[12] More recent experiences, notably in Iraq and Afghanistan, have shown the inherent difficulties in achieving the degree of situational awareness required to enable decision superiority when engaged against insurgent and irregular forces capable of concealing themselves within the population.[13]

The complex, interconnected systems that modern military forces have become reliant on to gain and maintain a high degree of situational awareness are increasingly vulnerable to infiltration and disruption through cyberspace. As noted by Major General Fergus McLachlan in 2015, '[modern C4ISR systems are] no longer stand alone or isolated'.[14] Current adversaries, such as Islamic State—and future adversaries, be they state or non-state actors—will attempt to exploit these systems for their own military advantage through cyberspace.

A well-formed and pragmatic concept of cyberspace is the logical starting place for any policy attempting to bridge the gap between national strategic intent and operational implementation. In the Defence context, cyberspace is more commonly referred to as the cyber domain. This fits with the past conceptualisation of land, sea, air and space as warfighting domains.

Defence is presently grappling with the emergence of cyber as an additional domain for its military planning, even while the multi-domain warfare construct comes under increasing criticism, including from Australia's current Vice Chief of Defence Force.[15] Indeed, neither the *2016 Defence White Paper* nor Australia's current cyber security strategy provide an adequate conceptualisation of the cyber domain for Defence's operational purposes. However, feasible definitions and concepts can be found in the strategy documents and doctrine of others, and among a range of academic works, which are explored below.

Firstly, it is useful to recognise that the cyber domain is both physical and non-physical. Physical aspects of the domain include international submarine communications cables, satellites, network routers, wireless infrastructure, servers, computers, industrial control modules and every smart device with Internet connectivity. Non-physical aspects of the cyber domain include the data and knowledge that is created in or flows through cyberspace; software for the creation, collection and dissemination of data; codes for the control of financial and industrial systems; and malicious software, cyber weapons and the codes to counter them.[16]

While this duality sets the cyber domain apart from land, sea, air and space, it is not a completely unique concept. ADF operational doctrine currently includes domain concepts which comprise both physical and non-physical components.[17] So the cyber domain could easily be adapted as an additional domain, connected with the existing domains of land, sea, air and space.

Secondly, it must be understood that the cyber domain is man-made, continually increasing in complexity, and in a state of 'constant flux based on the ingenuity and participation of [its] users'.[18] In many ways, this sets the cyber domain apart from the traditional domains, as the cost of participation can be exceptionally low, technological growth and application may occur in non-linear ways, and actors and their actions are difficult to identify.

Finally, there is significant overlap between the cyber domain and the existing domains. This is true with both physical connection to land, air, sea and space domains, and physical and non-physical interactions with the information and human domains. The role of Internet communications and social media in galvanising public unrest—from Tunisia to Wall Street—demonstrates the clear overlap between the cyber and information domains, and the cyber and human domains.[19]

The real world impact of cyber weapons, exemplified in the reported physical effects of the Stuxnet virus in its attack on Iranian nuclear facilities, is an unequivocal illustration of the overlap between the physical domain and the vulnerability of 'stand-alone' systems.[20] While Stuxnet remains an outlier in terms of sophistication, complexity and consequence, it nevertheless serves to demonstrate the vulnerability of 'stand-alone' systems and the potential military and national security implications of threats generated through the cyber domain.

Any policy intended to bridge the gap between strategic intent and operational capabilities and objectives should contain a concept of the cyber domain that accounts for Defence's technological context and the characteristics of the cyber domain. The development of such a concept from the existing information domain concept, rather than from the environmental domains, would seem to be more in line with Vice Admiral Grigg's views on designing and building an integrated force.[21] Furthermore, it would clearly show how 'cyber space unifies all domains of warfare, especially its political control and political impacts',[22] as presented schematically at Figure 1.

While certainly not being the only possible conceptualisation of the cyber domain, it is the author's view that this model, or one similar to it, would prove most useful in any policy intended to bridge the gap between Australian cyber strategy and the application of the Government's intent at the operational and tactical levels. In this model, the cyber domain underpins

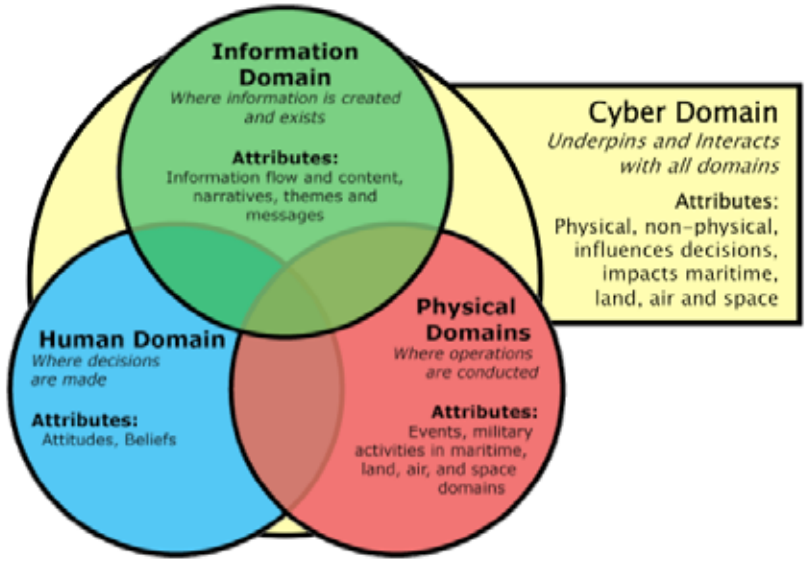

Figure 1: How cyber can unify the traditional domains of warfare (as adapted by the author)

and interacts with the information, human and physical domains. The level of interaction would increase over time as individual and societal levels of inter-connectedness continue to increase.

Understanding the threats

With a model of the cyber domain in place, the next logical step in bridging the gap between strategic intent and operational effects is an understanding of the likely threats. There is little by way of consensus to be found in allied policy and doctrine or academic works regarding threat models. Several commentators have identified 'attack vectors' or 'types of attacks', while US doctrine identifies specific countries and groups as 'threat actors'.[23] Neither approach, however, is particularly well suited to policy intended to bridge the gap between national strategy and operational capabilities and effects.

Ronald Deibert and Rafal Rohozinski identify 'risks to cyberspace' and 'risks through cyberspace' although, in a military policy and doctrinal context, they are in fact discussing threats.[24] Their threat model lends itself well to operational policy and doctrine, where threats to the cyber domain would include any threats to the physical elements of cyberspace, including networked military hardware and stand-alone government, military and industrial systems. Expanding on this idea, these threats may come from cyber weapons being used to infiltrate and disrupt information communications technology, or as physical attacks on network infrastructure, hardware or power supplies.

One of the more obvious examples of threats through the cyber domain is the spread of extremist ideology inspiring disenfranchised individuals to conduct attacks in Western countries. The spread of knowledge and ideas via the cyber domain has been exploited by issue-motivated groups to mobilise protests which triggered regime change in Egypt and, separately, in Tunisia in 2011.[25] While the cyber domain was not the decisive domain in either example, both serve as case studies to illustrate how the cyber domain underpins and interacts with the physical, information and human domains. Other threats through the cyber domain include fraud, blackmail, unauthorised disclosure and espionage.

While the above model is an effective treatment of the types of threats, it does not address the potential threat actors. For this, the work by Richard Harknett is useful in his categorisation of threat actors as state actors, state proxies or non-state actors.[26]

For example, the US has identified China, Russia, Iran and North Korea as the most prominent states actors in the cyber domain. States

are somewhat constrained by international law, norms, diplomacy and deterrence; however, they may take increased risks in the cyber domain due to the inherent difficulty in attributing and responding to attacks.

State proxies are reliant on states for funding, training and technological access. State proxies are able to conduct cyber operations while their sponsor maintains plausible deniability. China, in particular, has focused on making maximum use of the skills present in its civilian workforce to develop 'cyber militias', which could potentially be categorised as state-proxies depending on how they are employed.[27]

Non-state actors range from criminal groups committing fraud via the Internet to violent extremists, such as Islamic State, which pursue aggressive intelligence gathering and propaganda campaigns. The absence of state control reduces the constraints on such groups, with the cyber domain enabling them exponentially to increase their reach.

The potential threat posed by any of these threat actors needs to be analysed in relation to the specific operational context. Any group may pose a threat to the cyber domain or a threat through the cyber domain, depending on their capability and intent. For example, threats to stand-alone industrial control systems, intended to cause physical damage, require greater skills, knowledge, resources and time than hasty propaganda campaigns intended to sway public opinion. A depiction of the potential targets of threat actors is shown at Figure 2.

The incorporation into ADF doctrine of a cyber domain concept and threat model similar to that discussed above would provide military intelligence professionals, planners and commanders with pragmatic tools for understanding the cyber operating environment, analysing threats to and through cyberspace, and developing concepts of cyber operations.

Challenges of cyber operations

The nature of the cyber domain, its characteristics and the threat types and actors all combine to create a series of challenges for the

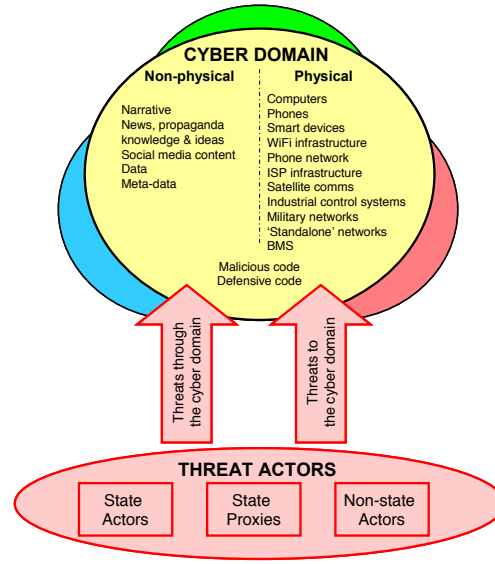

Figure 2: The potential targets of threat actors in the cyber domain (as adapted by the author)

application of cyber effects in a military context. It is these challenges that will be the most difficult for policy to address. The ubiquitous and borderless nature of the cyber domain, combined with the relative anonymity of actors and inherent difficulties in technical, legal and political attribution, have potentially fundamental effects on traditional national security concepts of defence and deterrence.[28]

Traditional notions of deterrence through military power are likely to be ineffectual against dispersed non-state actors and state-proxies that fear neither attribution nor retaliation.[29] Even ignoring the difficulties of attribution, effective deterrence requires the threat actor to understand to some degree the retaliatory capabilities of their target. The current level of secrecy surrounding Australian offensive cyber operations prevents that, and potentially undermines any deterrent effect.

Effective geographic defence of the cyber domain is technically not feasible, meaning the extension of sovereignty into the cyber domain is highly problematic. Traditional notions of defence are reliant on military power to seize and hold territory, control sea lines of communication and exert air superiority. Such actions are not possible in a borderless, highly complex and constantly evolving domain. Instead the cyber

domain offers ever-increasing opportunities for weak military powers and non-state actors to infiltrate, disrupt and degrade stronger adversaries.[30]

With the increasing importance of the cyber domain to Western notions of war, and a desire for decision superiority (or at least ever-increasing situational awareness), comes the many challenges of 'distributed warfare'.[31] Through the development of cyber capabilities, military units are likely to possess increased coercive powers. There will be increased cross-over between military and civilian organisations, and blurred lines between state, state proxies and non-state actors. Furthermore, deployed units will not be able to rely on a permanent link with higher headquarters in a disputed cyber and information environment. This serves to add to the complexity and uncertainty of military operations.

It is these challenges, and likely many others that have not yet been identified, that must be addressed—in terms of force structure, authorities, training and education, as well as platform and technical superiority—in any policy that aims to bridge the gap between strategy and operations.

Policy and force structure

As the ADF grows its cyber operations capability, commensurate policy and doctrine will be required to ensure continuing alignment with strategic objectives. Much of what has been discussed under the characteristics of the cyber domain and understanding the threat would neatly fit into joint doctrine. But doctrine alone will only partially bridge the gap between strategic intent and operational and tactical implementation. Specific policy, formulated by Joint Capabilities Group and endorsed by the Service chiefs, will be required to ensure that force structure, rules of engagement, research and development, and recruitment, among other considerations, are aligned with strategic intent.

US Cyber Command has provided some good insights into what that policy might cover.[32] However, to be truly useful, any Australian equivalent would need to be less aspirational and include quantifiable tasks. Drawing on the US example, Australian policy should also emphasise that cyber capabilities are 'not administered but rather led by commanders who understand they are always in real or imminent contact with [their] adversaries'.

That would ensure that cyber security and the cyber domain moves beyond the realm of technical specialists and into the common understanding of all military commanders and headquarters staff. Achieving this will require supporting direction in relation to cyber education, training and exercises, as well as force structure to ensure commanders are adequately supported to enable them to lead cyber alongside conventional capabilities.

Australian military cyber operations policy must also address the mission or, perhaps more appropriately, likely cyber tasks or cyber actions. Currently, there is scant discussion of the cyber mission in the public domain beyond an 'aim to retain freedom of manoeuvre in cyberspace, accomplish the joint force commander's objectives, deny freedom of action to adversaries, and enable other operational activities'.[33]

To date, cyber actions discussed publicly have been 'cyberspace defence', 'cyberspace security', and 'routine actions in cyberspace'.[34] However, such actions require considerable elaboration to be applicable to operational and tactical commanders. Furthermore, there is an obvious lack of discussion regarding offensive cyber capabilities that must be addressed more openly if the ADF is to catch up with the US and meet the stated strategic objective of Australia's defensive and offensive cyber capabilities as '[enabling deterrence and response] to the threat of cyber-attack'.[35]

However, directions to commanders, the development of policy to increase cyber education, training and exercises, and a defined cyber mission and detailed tasks will all be of little practical relevance without the manning and force structure to support them. The $400 million committed to strengthen cyber capabilities over the next ten years pales in comparison to the US Department of Defense's $6.7 billion budget for cyber operations in 2017.[36]

Even ignoring the order-of-magnitude funding disparity, the ADF is simply too small for the establishment of a Cyber Command similar to the US model. In his 2015 presentation on the

Australian Army's future force structure options, Major General Fergus McLachlan contended that the Army cannot rely on size to achieve advantage but must use cooperative activities to 'achieve strategic mass'.[37] The same obviously holds true for the ADF's cyber capabilities. Bridging the gap between strategic intent and operational application will require a policy that maximises cooperation with allied nations, other government agencies and industry stakeholders, and contains a means for 'mobilising cyber-capable reservists or civilians in times of military crisis'.[38]

A radical technological transformation of the ADF to meet the challenges of cyber operations is not feasible given competing Defence priorities, funding and manning limitations, declining education standards across society, and a general lack of science, technology, engineering and maths qualifications and experience across the workforce.[39]

Details of Australia's cyber force development plan are not publicly available, preventing meaningful analysis of force structure options. Nevertheless, deliberate growth of a cadre of specialist cyber operators, combined with increased cyber education of commanders, intelligence professionals and planners over the next ten years is a realistic path.

A force structure that sees Headquarters Joint Operations Command, Deployable Joint Force Headquarters and the deployed Joint Task Force Headquarters supported with fully integrated cyber operations teams would enhance the ADF's interoperability with its allies and the achievement of cyber defence tasks. Manning, funding, education and training, and policy currently dictate that slow and steady growth is the most rational path for the ADF to take.

Conclusion

Australian national strategy and cyber strategy documents place a clear emphasis on the development of cyber capabilities within the ADF. While Joint Capabilities Group has the lead in translating this strategic intent into operational capability and effects, bridging the gap between strategic intent and operational capability is currently hindered by the lack of public conversation and understanding of the cyber domain.

In that regard, joint doctrine clearly has an important role in raising awareness of cyber operations and bridging the gap between strategic intent and operational and tactical applications. It is also the appropriate vehicle for addressing the nature of the cyber domain, types of cyber threats and categories of threat actors.

It has been argued in this article that agreement on a cyber domain concept and threat model would undoubtedly increase engagement and awareness of cyber operations across Defence, with policy then being developed to bridge the remaining gap between strategic intent and operational and tactical capabilities and effects. Such policy should address the unique challenges of military cyber operations and cover force structure and development, measures for cooperation, and cyber education, training and exercises.

A two-pronged approach along those lines should serve to ensure that considerations of the cyber domain and cyber operations move beyond the realm of technical specialists, and that the Australian Government's strategic intent is successfully translated by the ADF into operational objective and tactical actions.

Major Christopher Wardrop is an Australian Intelligence Corps officer, currently posted to the Intelligence Branch of Headquarters Joint Operations Command. His postings have included 4th Field Regiment, North West Mobile Force, Headquarters 1st Brigade, Headquarters 1st Division, 1st Intelligence Battalion and the Warrant Officer and Non-Commissioned Officer Academy. He has served on operations in Uruzgan and as an Intelligence Staff Officer on Australian Joint Task Force Headquarters in both Kabul and the Middle East region. Major Wardrop holds a Bachelor of Arts in History and Politics.

Notes

1 Myriam Calvety and Elgin Brunner 'Information, power and security – an outline of debates and implications', in Myriam Cavelty, Victor Mauer and Sai Krishna-Hensel (eds.), *Power and security in the information age: investigating the role of the state in cyberspace*, Ashgate: Farnham, 2013, 2007, pp. 201-493.

2 Charles Weiss, 'Science, technology and international relations', *Technology in Society*, Vol. 27, No. 3, August 2005.

3 A great number of which are available on the NATO Cooperative Cyber Defence Centre of Excellence website,

available at <https://ccdcoe.org/cyber-security-strategy-documents.html> accessed 20 June 2017.

4 [Australian] Department of Defence, 'White Paper at a glance: intelligence, surveillance and reconnaissance, space, electronic warfare and cyber security', *Department of Defence* [website], p. 1, available at <http://www.defence.gov.au/Whitepaper/AtAGlance/ISR-Cyber.asp> accessed 10 October 2017.

5 Commonwealth of Australia, *2016 Defence White Paper*, Department of Defence: Canberra, 2016.

6 Commonwealth of Australia, *Australia's cyber security strategy: enabling innovation, growth and prosperity,* Department of the Prime Minister and Cabinet: Canberra, 2016, p. 3.

7 Marcus Thompson, 'The ADF and cyber warfare', *Australian Defence Force Journal*, No. 200, 2016, p. 47.

8 Commonwealth of Australia, *Australia's cyber security strategy*.

9 See 'Information Warfare Division', *Department of Defence* [website], available at <http://www.defence.gov.au/jcg/iwd.asp> accessed 10 October 2017; see also Andrew Davies and Malcolm Davis, 'ADF capability snapshot 2006: C4ISR–winning in the networked battlespace', *Australian Strategic Policy Institute (ASPI)* [website], 21 June 2016, p. 3, available at <https://www.aspi.org.au/report/adf-capability-snapshot-2016-c4isr-winning-networked-battlespace> accessed 10 October 2017;

10 Davies and Davis, 'ADF capability snapshot 2006', pp. 2-4.

11 Michael Clifford, Michael Ryan and Zoe Hawkins, 'Mission command and C3 modernisation in the Australian Army: digitisation a critical enabler', *ASPI* [website], 17 December 2015, p. 9, available at <https://www.aspi.org.au/report/mission-command-and-c3-modernisation-australian-army-digitisation-critical-enabler> accessed 10 October 2017.

12 Davies and Davis, 'ADF capability snapshot 2006', p. 4

13 Major General Fergus McLachlan, 'Address to Australian Strategic Policy Institute's "Army's Future Force Structure Options Conference"', Canberra, 25 June 2015, available at <https://www.army.gov.au/our-work/speeches-and-transcripts/head-modernisation-strategic-planning-address-to-aspi-conference> accessed 10 October 2017.

14 McLachlan, 'Address to Australian Strategic Policy Institute's "Army's Future Force Structure Options Conference"'.

15 Ray Griggs, 'Building the integrated joint force', *ASPI* [website], 7 June 2017, available at <https://www.aspistrategist.org.au/building-integrated-joint-force/> accessed 10 October 2017.

16 Myriam Calvety, 'Is anything ever new? – Exploring the specificities of security and governance in the information age' in Cavelty *et al*, *Power and security in the information age*.

17 Department of Defence, 'Operation Series: Information Activities', Edition 3, Australian Defence Doctrine Publication 3:13, *Department of Defence* [website], 2013, available at <http://www.defence.gov.au/FOI/Docs/Disclosures/330_1314_Document.pdf> accessed 10 October 2017.

18 Ronald Deibert and Rafal Rohozinski, 'Risking security: policies and paradoxes of cyberspace security', *International Political Sociology*, Vol 4. Issue 1, 15 March 2010, p. 16, available at <https://deibert.citizenlab.ca/2010/03/risking-security-policies-and-paradoxes-of-cyberspace-security/> accessed 10 October 2017.

19 Manuel Castells, *Networks of outrage and hope: social movements in the internet age*, 2nd Edition, Wiley: Milton, 2015.

20 Nicolas Falliere, Liam Murchu, and Eric Chien, 'W32. Stuxnet dossier', *Symantec* [website], February 2011, available at <https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf> accessed 10 October 2017.

21 Department of Defence, 'Operation Series: Information Activities', pp. 1-6.

22 Greg Austin, *Australia rearmed! Future needs for cyber-enabled warfare*, Australian Centre for Cyber Security: Canberra, 2016.

23 See, for example, Marcus Thompson, 'The cyber threat to Australia', *Australian Defence Force Journal*, No. 188, 2012, pp. 59-61; Austin, *Australia re-armed!,* pp. 5-6; and US Department of Defense, 'The DOD Cyber Strategy', *Department of Defense* [website], April 2015, p. 9, available at <https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf> accessed 10 October 2017.

24 Deibert and Rohozinski, 'Risking security', pp. 18-24.

25 Castells, *Networks of outrage and hope*.

26 Richard Harknett, 'Integrated security: a strategic response to anonymity and the problem of the few', *Contemporary Security Policy*, Vol. 24, No. 1, 2003, pp. 29-32.

27 Austin, *Australia rearmed!*, p. 11.

28 Nicholas Tsagourias, 'Cyber-attacks, self-defence and the problem of attribution', *Journal of Conflict & Security Law*, Vol. 17, No. 2, Summer 2012, pp. 229-44.

29 Forrest Hare, 'The significance of attribution to cyberspace coercion: a political perspective', in C. Czosseck, R. Ottis and K. Ziolkowski (eds.), *Proceedings of the 4th International Conference on Cyber Conflict*, NATO: Tallinn, 2012, p. 126.

30 Austin, *Australia rearmed!*, p. 21.

31 Austin, *Australia rearmed!*.

32 US Department of Defense, 'Beyond the build: delivering outcomes through cyberspace. The Commander's vision and guidance for US Cyber Command', *Department of Defense* [website], 3 June 2015, p. 5, available at <https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/docs/US-Cyber-Command-Commanders-Vision.pdf> accessed 10 October 2017.

33 See, for example, Michael Riedy, 'Defence Cyber Coordination Centre', presentation to Military Communications and Information Systems Conference 2015, available at <https://milcis-twenty.squarespace.com/s/2015-3-2_3.pdf> accessed 20 June 2017.

34 Riedy, 'Defence Cyber Coordination Centre'.

35 Commonwealth of Australia, 'Australia's cyber security strategy', p. 28.

36 *Military and Aersopace Electronics*, '2017 DOD budget calls for 15 per cent increase in military cyber

security spending', *Military and Aerospace Electronics* [website], 24 February 2016, available at <http://www.militaryaerospace.com/articles/2016/02/cyber-security-dod-budget.html> accessed 21 June 2016.

37 McLachlan, 'Address to Australian Strategic Policy Institute's "Army's Future Force Structure Options Conference"', p. 3.

38 Austin, *Australia rearmed!*, p. 29.

39 Australian Council of Learned Academies, 'The role of science, research and technology in lifting Australia's productivity', *Australian Council of Learned Academies* [website], 2014, pp. 102-8, available at <http://www.acola.org.au/PDF/SAF04Reports/SAF04%20Role%20of%20SRT%20in%20lifting%20Aus%20Productivity%20FINAL%20REPORT.pdf> accessed 10 October 2017.