Cyber Security and the 2016 Defence White Paper

Tim Scully

Australia has so tightly embraced the Internet that it is now indispensable to the conduct of public and private business at all levels—individual, small, medium and large. It will remain critical to our economic prosperity and, therefore, to our national security.

Any policy framework that seeks to protect Australian's well-being in cyber space must recognise that any organisation whose internet-connected network has commercial, strategic or operational information of value to a cyber threat actor is likely to have already been compromised. So, the notion that we can keep intruders on the outside of our networks is as outmoded and naive as the belief that everything on the inside can be secured.[1] Significant national coordination, collaboration and innovation is needed to overcome the seemingly unshakable vulnerabilities that riddle the internet architecture.

The 2016 Defence White Paper[2] cannot, by itself, articulate the long-term policy settings needed to achieve such resilience, but it can articulate how Defence meshes with national efforts to do so. The main purpose of the latest White Paper is to explain "how the Government is strengthening Australia's *defence capabilities* to meet the challenges of the more complex strategic environment Australia is likely to face in the years ahead" (para 1.1, emphasis added). Of significance to this article, it also serves to explain "how the Government will ensure that Australia has the critical industrial, scientific, technological and innovation capabilities *outside of Defence* that will be necessary to underpin Australia's security." (para 1.4, emphasis added)

Cyber security is one of the most serious security challenges we face as a nation—it affects all walks of life across our society—so it is reasonable to expect that the White Paper articulates the strategy, capabilities and resources needed for Defence to engage effectively with our national cyber resilience architecture. This chapter examines whether or not the 2016 Defence White Paper has done so.

[1] Tim Scully, 'The Cyber Threat, Trophy Information and the Fortress Mentality', *Journal of Business Continuity & Emergency Planning,* vol. 5, no. 3 (2011), pp. 195-207.
[2] Department of Defence, *2016 Defence White Paper* (Canberra: Commonwealth of Australia, 2016).

Fifth Domain of Warfare or not? Cyber Warfare or not?

Before addressing the implications of the 2016 Defence White Paper for Australia's cyber security industry and academia/research institutions, it is useful to reflect on cyber space as a contested domain. Where does cyber fit in relation to the more traditional war fighting domains; sea, land, air and space? A debate has also long simmered over whether cyber warfare even exists and, by extension, whether cyber space constitutes the fifth domain of warfare.

The US Department of Defense formally recognised cyber space as a fifth domain of warfare in 2010.[3] It is no doubt critical to Australia's national security and economic viability, but the White Paper gives us no hint as to whether Defence recognises cyber space as a discrete domain of warfare. In fact, in 2014, an interview with Defence's former Deputy Director Cyber and Information Security offered that "cyber war won't occur as such—it's just one method of disruption and destruction",[4] indicating that he did not agree with the US view. Unusually, the White Paper also puts 'Cyber and Space' into the same category, again indicating that neither are considered separate domains of warfare. Rather, cyber and space capabilities support or facilitate operations in the traditional 'kinetic' domains of warfare.

On cyber warfare, at one end of the spectrum, the debate is dominated by the view that there is no such thing as cyber warfare,[5] which leans on tenuous Clauswitzian conditions to define warfare. At the other end of the spectrum, we have the view characterised by the sensational prediction in 2012 by then incumbent US Secretary of Defense, Leon Panetta, that a "Cyber Pearl Harbour" was imminent.[6] Such predictions of warlike consequences and significance shows an elevation of cyber from the realm of security to warfare.

We do not know where Australia stands in these debates on cyber warfare and cyber space as a war fighting domain because the White Paper offers no information on them and the government has not previously articulated a clear view on the subject. One potential advantage of defining cyber space as a discrete war fighting domain is that it would allow policy makers and planners to first separate and develop strategy, capability and resources for cyber operations, and then integrate them with the main capability streams.

[3] William J. Lynn, 'Defending a New Domain: The Pentagon's Cyberstrategy', *Foreign Affairs*, September/October 2010, pp. 97-108.
[4] Interview with Major General Steve Day. See Nicholas Stuart, 'Cyber War Needs Cyber Soldiers Say Nicholas Stuart', *The Sydney Morning Herald*, 23 August 2014,
[5] Rid is a leading proponent of the argument against the existence of cyber warfare. See Thomas Rid, *Cyber War Will Not Take Place* (New York: Oxford University Press, 2013), p. x.
[6] Leon Panetta, 'Defending the Nation from Cyber Attack', Speech to Business Executives for National Security, New York, 11 October 2012, <archive.defense.gov/transcripts/transcript.aspx?transcriptid=5136> [Accessed 24 March 2016].

This, in turn, would offer the clarity that is essential for innovation and entrepreneurship for both research and industry efforts.

Why is Everyone Talking about Cyber Security except Defence?

The 2009 Defence White Paper gave cyber security a 'light touch', although it was the first Australian White Paper to address cyber operations[7] as a Defence capability and spawned the Cyber Security Operations Centre (CSOC). This was a welcome development, but the subsequent allocation of funding was such that Defence swallowed most of the funding pie leaving other government stakeholders bereft of resources to develop their equally important cyber resilience capabilities. The 'full costing' approach in the latest White Paper through the Integrated Investment Plan could mitigate this problem, although specific costing for cyber security initiatives—as opposed to full spectrum cyber capabilities— is not clear.

After Prime Minister Julia Gillard's January 2013 announcement, the 2013 Defence White Paper elaborated on the Australian Cyber Security Centre (ACSC) that draws on essentially the same government players engaged in the original CSOC, but committed to adding industry players to the mix. Apart from a move to the new ASIO building, the only tangible differences between the CSOC and ACSC from 2009 to 2013—as far as publicly available information goes—appear to be a new location but still entirely within a classified enclave, and new governance arrangements under the Cyber Security Operations Board, chaired by the Secretary of the Attorney General's Department. Three years later, its web site stated that "the ACSC *is considering* a number of models for partnering with industry".[8] As the most significant operational level cyber security asset available to Defence and the nation, it is important that Australians know how its work will mesh with and augment cyber resilience capabilities "outside of Defence" (para 1.4).

Overall, the 2016 Defence White Paper contains much of the usual rhetoric around cyber resilience in common with the 2009 and 2013 papers. The major addition this year is the commitment to rebalance the workforce "with around 1,200 new APS positions in areas critical to Defence's future capability, including intelligence, cyber security and space-based

[7] Cyber operations include cyber security/defence, cyber attack and cyber exploitation/espionage. Cyber security comprises those measures designed to protect the confidentiality, availability and integrity of information and information systems. Cyber exploitation or espionage is a clandestine activity aimed at stealing an adversary's information, or to establish the ground work for more decisive or damaging future activity. Successful cyber exploitation will not be discovered. A cyber attack is a covert activity intended to destroy, disrupt, deny, degrade or otherwise manipulate information or an information system. Its effects are usually apparent.

[8] 'Frequently-Asked Questions', Australian Cyber Security Centre, <www.acsc.gov.au/faqs.html>, [Accessed 24 March 2016] (emphasis added).

capabilities".[9] It is not known how many of these positions are dedicated to cyber security. And, as a policy paper, it falls short by not describing how Defence cyber security efforts will link with those of industry, academia and other government agencies. In terms of tangible action, it does not advance significantly in scope or detail from its predecessor papers. The ACSC gets two fleeting mentions. This is disappointing given the Prime Minister's and Minister for Defence's implicit alignment of the 2016 White Paper with the government's National Innovation and Science Agenda.

The 2016 Defence White Paper generally provides much needed policy clarity to engender certainty for the *broader* Australian defence industry, but it does not give industry and academia much to go on in regard to cyber security capabilities. Although the Prime Minister emphasised the need for more resilience in cyber space in his speech launching the White Paper, it contains little policy substance on the blend of strategy, capability and resources needed to achieve cyber resilience for Defence, let alone for the nation. It does not say how the cyber security industry will be engaged on this vital capability, nor does it provide any indication of how Defence will build its workforce at a time when cyber security professionals remain in extremely short supply with strategies to educate, train and recruit them few and far between. Traditional methods of recruitment and training will not likely grow the workforce in the short term, so new approaches will be needed.

The dearth of detail on cyber capabilities in the White Paper is not due to a lack of substantial options. It is more likely due to the ingrained reticence of our intelligence and security agencies to publicly discuss such matters due to a 'classify-by-default mentality'. Such reticence is a positive attribute in an intelligence officer, but is an impediment when transparency and open collaboration is needed. Mike Burgess, Chief Information Security Officer for Telstra and, significantly, the first Deputy Director Cyber and Information Security at the Australian Signals Directorate, recently echoed this sentiment when referring to the more open discussion in the United States on cyber security. He said, "I'd like to see more of our agency heads talking on this subject, but I understand perhaps why they don't."[10] The Australian Strategic Policy Institute's Tobias Feakin says that

> to have been "truly visionary", or at least to keep pace with the defence policies of other advanced nations, the 2016 Defence White Paper would have to have engaged in a more holistic discussion across the spectrum of

[9] Department of Defence, *2016 Defence White Paper*, p. 23.

[10] Burgess was addressing the 2016 Australian Information Industry Association Summit in Canberra. See Stilgherrian, 'Australia Needs a "National Discussion" on Security and Civil Liberties', *ZDNet*, 16 March 2016, <tiny.cc/b8b79x> [Accessed 24 March 2016].

> cyber capabilities … to reveal a great deal more about how those nations deal with cyber both offensively and defensively.[11]

This is a common grievance by those in our media and academic sectors where sensitive information eludes them. It is appropriate that offensive capabilities, such as cyber attack and cyber exploitation, are not given a public airing. After all, in the intelligence business "the secret to success is keeping your success secret."[12] Even discussion of the effects that these offensive capabilities can produce should be kept under wraps.

The same cannot be said of cyber security, a matter that affects our whole society. It can and should be treated more openly. There are certainly elements of cyber security capability that must be kept under wraps, but Australians, particularly those in industry and academia, deserve to know how Defence connects with national efforts to protect the nation's information and IT systems. The Australian Centre for Cyber Security at the University of New South Wales (UNSW) was very pointed in its criticism of the White Paper's treatment of cyber for this reason:

> The government did not lay out a strategic approach to cyber-enabled warfare. It did not give a strong lead on the urgency of repairing our cyber skills deficit. Above all, while recognising that the "most basic Strategic Defence Interest is a secure resilient Australia", the document is virtually silent on how Defence must change to achieve resilience under sustained cyber-attack.[13]

Defence's adoption of a low profile on cyber security could exacerbate what has been a long drawn out process that requires strong leadership in government, industry and academia, and it runs counter to the rekindled spirit of 'contestability' espoused in the *First Principles Review*.[14] The push for openness and a national approach by Defence on cyber security is not new. In 2014, Gary Waters presciently encapsulated what was needed (but obviously not heeded). He said that the next Defence White Paper:

> should address the need to integrate cyber power into national strategy, describe how this might be achieved, and set the scene for an improved whole-of-nation effort. It should address just how Defence contributes to the National Cyber Security Strategy, what its cyber posture is, and how it is addressing any gaps through planned remediation and implementation plans. It might describe how a national cyber effort and a national Intelligence, Surveillance and Reconnaissance (ISR) construct can be brought together and just what Defence's role might be in realising a more

[11] Tobias Feakin, 'Matching Rhetoric with Action: Cyber and the 2016 Defence White Paper', *The Strategist*, Australian Strategic Policy Institute, 25 February 2016, <tiny.cc/xbs59x>.
[12] John Blaxland, 'Protecting Secrets: Inside Australia's Mysterious Spy Agency', *The Conversation*, 20 November 2014, <tiny.cc/rkn5sx> [Accessed 24 March 2016].
[13] 'Defence White Paper Exposes Civil-Military Gap in Australia's Cyber Defences', University of New South Wales (UNSW) Newsroom, 29 February 2016, <www.unsw.adfa.edu.au/defence-white-paper-exposes-civil-military-gap-australia's-cyber-defences> [Accessed 24 March 2016].
[14] Department of Defence, *First Principles Review: Creating One Defence* (Canberra: Commonwealth of Australia, April 2015).

> integrated national effort. Without this, cyber and ISR capability gaps will emerge that will hinder the ability to plan for and conduct effective operations in future.[15]

Australia's track record of getting national cyber security initiatives off the ground is lamentable. The last decade has seen a long void during which we waited to see what the United States would do instead of taking the initiative to sort out its own cyber backyard. Since then, we have seen the 2009 Cyber Security Strategy that was devoid of innovation or imagination, as well as the only attempt at a Cyber Security White Paper that bounced between government departments until it disappeared. Not much occurred in the cyber policy domain until the release of the Australian Cyber Security Strategy on 21 April 2016, nearly eighteen months after it was urgently initiated. At last, the new Strategy provides a long-awaited coherent approach to national cyber resilience; not only is it accompanied by a solid "Action Plan", it is couched in lucid language devoid of the technical jargon that normally accompanies any discourse on cyber security.

The reticence shown in this latest White Paper on cyber security does not augur well for understanding how Defence will engage with broader national initiatives to build confidence in our nation's cyber resilience. While it is true that a white paper cannot include detail on all capabilities, given the Government's strong and frequent emphasis and rhetoric about cyber security, this latest White Paper could have been more forthcoming on the topic. More effort must be made by Defence and the government to separate cyber security from the more general 'cyber' topic; it should be excised from classified stovepipes that inhibit stakeholder engagement and innovation.

Defence Engagement with the Cyber Security Industry

The 2016 Defence White Paper is accompanied by the Integrated Investment Plan and the Defence Industry Policy Statement, which will be followed by the release of an inaugural Defence Industry Capability Plan in 2017. Together these documents will help deliver the clarity and certainty that defence industry needs to remain viable and innovative, and to build its international competitiveness.

The Defence Industry Policy Statement lays the foundation for Defence

> to reset and refocus the Defence and industry partnership for improved delivery of defence capability, to ensure we are maximising opportunities for competitive Australian businesses and streamline the delivery of defence

[15] Gary Waters, 'Pressing Issues for the 2015 Defence White Paper', *Discussion Paper Series,* Kokoda Foundation, 28 February 2014.

> industry programs. an opportunity rationalises the support framework for industry.[16]

The initiatives described in the Policy Statement are very encouraging in terms of promoting innovation and entrepreneurship, and have significant potential to draw more deeply on small to medium enterprises (SMEs), which "is important as a large repository of untapped capability in the cyber security industry resides in our SMEs."[17] The initiatives also attest to Defence's resolve to change the way it engages industry and, as it takes two to tango, to subtly push industry to rethink how it engages with Defence and reorganise itself to do so.

The creation of the Centre for Defence Industry Capability (CDIC) is the first such initiative. The fact that the Centre will be led jointly by industry and Defence shows that Defence is serious about tapping industry capability at all levels. A challenge for the Centre leaders will be to ensure that SMEs in the cyber security industry get a stronger voice and are not drowned out or corralled by the defence industry primes. Included in the CDIC initiative is the recognition of industry as a 'Fundamental Input to Capability' (FIC).

> The intent behind making industry a FIC is to drive more formal consideration of industry impacts through the early stages of the capability development life cycle. In this way, Defence will better match the development of new capabilities with industry's ability to deliver them.[18]

The recognition of industry as a FIC has as much to do with imagery as it does with substance. Industry already pervades all of the existing eight FICs, nonetheless formal recognition as a FIC, combined with strong leadership in the CDIC, will help Defence achieve its aim of earlier engagement with industry in capability procurement, something that has been elusive due to the pervasive and risk averse 'probity mindset' in Defence and a similar attitude in industry to intellectual property.

The Defence Industry Policy Statement also rationalises the plethora of defence industry development programs. These programs were designed to give industry a leg up to become more focused on defence capability needs, and more creative and internationally competitive. However, the dozens of programs seemed to lack direction and oversight with many programs being bereft of clear and measurable objectives and lacking oversight. The new policy will bring clarity and focus as Defence helps industry develop its capabilities, especially for SMEs, and will reduce the waste associated with the previous suite of programs.

---

[16] Department of Defence, *2016 Defence Industry Policy Statement* (Canberra: Commonwealth of Australia, February 2016), p. 10.
[17] Mike Kalms, 'DWP 2016: Room for Optimism in Australian Defence Industry', *The Strategist*, Australian Strategic Policy Institute, 10 March 2016, < http://www.aspistrategist.org.au/dwp-2016-room-for-optimism-in-australian-defence-industry/> [Accessed 24 March 2016].
[18] Department of Defence, *2016 Defence Industry Policy Statement*, p. 19.

The second important initiative is the Defence Innovation Hub. Through this Hub, "Defence will build collaborative programs with academia, publicly funded research agencies, industry (particularly small to medium enterprises), and our allies to create a vibrant and interlocking research and innovation capability that is focused on driving Defence outcomes."[19] The focus on SMEs is very encouraging as the strength of Australia's cyber security industry lies in the potential of its SMEs. Any effort to engage with cyber security SMEs and help engage with Defence is very welcome. The new Defence Innovation Portal, in particular, should assist them to overcome the perceived herculean hurdle of dealing with the complex Defence machine.

It is, therefore, disappointing that the Defence Industry Policy Statement mentions "cyber" twice and then only in the context of next generation capabilities; it does not touch on what is needed now and in the short term. Given that industry is expected to co-lead in building national cyber resilience, one can hope that this shortfall will be addressed in the forthcoming Defence Industry Capability Plan.

Cyber Security Industry: White Knights and Rent Seekers

This article so far has centred on the lack of visibility in the White Paper on how Defence will engage with national cyber security initiatives and industry. Of course, it is not a one-sided engagement—the nature of Australia's cyber security industry is not necessarily conducive to fluid collaboration with Defence, other government agencies and research bodies.

The global cyber security industry has not covered itself in glory. In democratic, market economies, and with supportive government policy, industry should be the 'boots on the ground' in combatting the cyber security threat, but it has not risen to the challenge.[20] Over the last decade, large multinational companies have seized the opportunity to enter the cyber security market with the goal of turning small, high-volume/low-margin companies into the opposite, namely low-volume/high-margin lines of business. Many small, specialist cyber security companies have been absorbed into these global behemoths, but the cyber security industry remains fragmented and the broader business world's cyber security posture has improved only marginally.

Vulnerabilities in software applications, including cyber security products, are ubiquitous[21] with the services provided by cyber security companies to

[19] Ibid., p. 32.
[20] Tim Scully, 'The Cyber Security Threat Stops in the Boardroom', *Journal of Business Continuity & Emergency Planning,* vol. 7, no. 2 (2014), pp. 142-3.
[21] Hundreds of vulnerabilities of varying severity in common software applications are reported every week by the US Computer Emergency Readiness Team (CERT) alone. The summary reports known vulnerabilities; it cannot possibly report the vast number of undiscovered

detect them frequently failing. For example, in the Auditor General's review of cyber security in fifteen Western Australian Government agencies in 2011, "a number of agencies had paid third party service providers and contractors to manage their cyber security. However, our tests proved this management was ineffective."[22] The Auditor General's subsequent review in 2015 did not show a marked improvement.[23]

The vast volumes of literature and advertising available on so-called 'best practice' cyber security tools, techniques and procedures can overwhelm an organisation, particularly their security practitioners. Vendors are filling the market with myriad claims as they seek to add a differentiator to their product or service in order to get the buyers' attention. For example, the Internet is now littered with cyber security industry 'white papers' that are often thinly disguised marketing tools that define a problem that is tailor-made for the vendor's solution. This also begs the question of whether market competition itself undermines effective cyber security as leaders and technicians are not adequately equipped to assess competing products and services based on the claims of competing providers. Nor is competition in industry conducive to the level of sharing that is essential for cyber resilience. Such sharing includes data and information on threats, vulnerabilities, malware, attack/exploitation vectors, trends and solutions. However, the need to differentiate from one's competitors often precludes such sharing as surely as reticence on the part of government agencies does.

Until the cyber security industry can build more cohesion, it will be difficult for Defence to effectively engage with it. The 2016 Defence White Paper initiatives described above may provide some impetus in this regard, but a national approach is needed. One such initiative whose omission from the White Paper is perplexing is the establishment of the Cyber Security Growth Centre. The Centre was announced by the Prime Minister in December 2015 and was apparently extracted from the draft Australian Cyber Security Review released later in April 2016.

The Cyber Security Growth Centre will bring together industry, researchers and government to create a national cyber security innovation network; develop a national strategy for Australia's cyber security industry to become a global leader and attract investment from multinationals; and coordinate cyber security research and innovation to reduce overlap and maximise

---

vulnerabilities. For example, see 'Vulnerability Summary for the Week of January 19, 2015, Bulletin SB15-026', US CERT, US Department of Homeland Security, 26 January 2015, <www.us-cert.gov/ncas/bulletins/SB15-026>.

[22] Western Australian Auditor General, *Information Systems Audit Report*, Report 4 (Perth: Office of the Auditor General Western Australia, June 2011).

[23] Western Australian Auditor General, *Information Systems Audit Report*, Report 23 (Perth: Office of the Auditor General Western Australia, November 2015).

impact.[24] Its mission is complementary to that of the CDIC and Defence Innovation Hub, so collaboration between Defence and the new Cyber Security Growth Centre is clearly a matter that the White Paper could have addressed.

The Growth Centre will require a CEO with deep experience in the cyber security industry, but who must also be possessed of skills and experience in building links across government (especially Defence), industry and the research and development community to produce real solutions that can be commercialised. This will be a daunting task because our cyber security industry—albeit strong on innovative capability—is fragmented, lacks cohesion and, so far, has no clear incentive or value proposition to join collaborative efforts to build national cyber resilience (the numerous failed attempts to establish a Cyber Security Cooperative Research Centre attest to industry's reluctance to join such collaborative initiatives).

Cyber Warriors and Cyber Security Professionals

The most tangible, identifiable cyber security initiative that carries through the 2016 Defence White Paper and its companion documents is the investment in "Cyber Security Capability Improvement" of $300-400 million over the next decade.[25] The specific personnel cost for cyber security is not stated, but it would be expected to be a large proportion of that amount. This growth in itself presents a significant challenge that is not addressed, namely recruiting skilled cyber security practitioners from a very shallow talent pool, training and skilling them internally, and getting them security cleared. According to Professor Jill Slay of the Australian Centre for Cyber Security, UNSW,

> government should have addressed all of the cyber skilling challenges faced by Australia in the Defence White Paper, but when it comes to national resilience in cyber space, which is part of our highest Defence objective, the government must follow up its new commitments on cyber military issues with a strategy for educating a massively increased cyber work force in the civil sector.[26]

Educating the workforce is an enormous challenge not just for Defence but for industry and academia. A failure to demonstrably plan for this challenge would undermine the intent of the White Paper for cyber security and other cyber war fighting skills, so it is hoped more detail will be included in the Defence Industrial Capability Plan in 2017.

While the cyber security skilling challenge is difficult enough, Defence cannot afford to lose potential cyber security recruits due to an antiquated personnel

[24] 'Cyber Security Growth Centre', Department of Industry and Science, <tiny.cc/2pw79x>.
[25] It is not clear if this includes only cyber security capabilities or offensive capabilities as well.
[26] 'Defence White Paper Exposes Civil-Military Gap in Australia's Cyber Defences', UNSW Newsroom, 29 February 2016, <http://tiny.cc/s2mray> [Accessed 24 March 2016].

security vetting process, nor can industry afford to have employees 'sitting on the bench' waiting for security clearances. The security vetting process is still based upon human investigative measures and has failed to keep up with demand for clearances for more than a decade. Defence, and government more broadly, needs to introduce machine-enabled collection, analysis and automatic, continuous reporting to support the security vetting process, leaving humans to examine the highest risk cases. Furthermore, as industry is now expected to pay for security clearances, "there is scope for Defence to develop a clear pathway to strengthen [its] capacity to deliver services, and improve quality control over aspects of vetting practice and decision-making."[27] This challenge is not addressed in the White Paper or Policy Statement.

Conclusion

The alignment of strategy, capability and resources to meet Australia's national security challenges is always a contentious issue eliciting many and varied views from a plethora of commentators, whose ideological predispositions are often based on their own experience in the development of past Defence white papers. So, it is not surprising to sniff a faint odour of 'we did it better in my day' among the many critiques that have flourished since the seventh Australian Defence White Paper was launched in February 2016.

It seems there is a strong consensus that this White Paper will be very effective if implemented as intended, especially from an industry perspective. In fact, the former Australian Ambassador to the United States and Labor politician, Kim Beazley, described the White Paper as a "superb strategic statement" and was equally complimentary of the paper's industry focus.[28] But as expected there are contrarian viewpoints such as Greg Raymond's well-argued opinion that "the Defence White Paper overrates the significance of recent developments and thereby grossly misrepresents our overall historical trajectory."[29]

The industry-related policy contained in the 2016 Defence White Paper and its companion documents will do more than its predecessors to create the certainty in policy direction that is craved by the Australian Defence industry and other enabling industry sectors. This alone is a key achievement as industry has long been a fundamental input to defence capability and, now, is formally declared as such by Defence and the government.

---

[27] Australian National Audit Office, *Central Administration of Security Vetting: Department of Defence*, The Auditor-General ANAO Report No.45 2014–15 Performance Audit (Canberra: Commonwealth of Australia, 9 June 2015).
[28] Kim Beazley, at the Australian Strategic Policy Institute's international conference, 'Defence White Paper: From the Page to Reality', Canberra, 7-8 April 2016.
[29] Greg Raymond, 'Political amnesia is damaging Australia's national security', *The Interpreter,* Lowy Institute, 5 April 2016, <http://tiny.cc/dfmray> [Accessed 24 March 2016].

However, given how tightly Australia has embraced the Internet, the exposure the cyber security capability as a separate component of 'cyber' has received is inadequate. It is not suggested that cyber security be elevated to the level of a capability stream, but as a key enabler for our national security and economic viability it deserves more transparent and detailed treatment. This would make it easier for all stakeholders to talk about what is possible rather than dwell on what is wrong.

The release of Defence Industrial Capability Plan in 2017—coupled with the release of the Australian Cyber Security Strategy, the establishment of the Cyber Security Growth Centre and the future policy statement on Science and Innovation for National Security—presents an opportunity for Defence to more clearly articulate how it will build cyber security capability in collaboration with national cyber resilience efforts across government, industry and academia. But it needs to overcome its inherent reticence if it is to achieve this—cyber security is a social problem, not just a military one.

Tim Scully is a senior leader with thirty-nine years' experience building and leading operational capabilities in government and industry to meet national and international intelligence and security challenges. He is currently Chairman of the Data to Decisions Cooperative Research Centre and Director of Stoneleigh Consulting. He has served as both CEO Stratsec and Head of Cyber Security in BAE Systems Australia, Head of the Defence Security Authority, inaugural head of the Government's Cyber Security Operations Centre and a range of senior intelligence roles in the Australian Signals Directorate, both as a public servant and Army officer. He holds a Masters of Defence Studies from UNSW. tim.scully@anu.edu.au.