Critical Infrastructure Public-Private Partnerships: When is the Responsibility for Leadership Exchanged?

Vaughan Grant

This paper examines the nexus between the Australia's public and private sectors regarding critical infrastructure. In the current dynamic threat environment resultant from the implementation of insecure technologies no clear point of hand over is discernible. By utilising examples and case studies this article amplifies this point. The private sector will not allow the public sector the network access required for the public sector to assume sole responsibility; therefore, the private sector must become committed beyond their first order responsibilities to their shareholders and acknowledge their fundamental involvement in collective security.

Australia's geographic location has had a notable influence on its approach to national security. The Defence White Paper of 1987 observed that Australia's security posture was "shaped in a unique and enduring way by basic facts of geography and location".[63] The advent of the information revolution has seen significant changes resulting in, amongst other things, the globalisation of information and increased privatisation which have had a marked effect on Australia.[64] The rate with which innovation in technology has been adopted has also led to unforeseen outcomes. Previously an attack on critical infrastructure was only viable if carried out via kinetic (i.e. physical such as explosives) means; however, by exploiting current technical vulnerabilities, a cyber attack against critical infrastructure can be launched by individuals, non-state organisations and by nation-states from any location that is connected to the Internet.[65]

Cyber security of critical infrastructure is balanced on the interface between the private and private sectors. Many governments rely on private companies to take the lead in delivering cyber security for critical

[63] Australian Department of Defence, *The Defence of Australia* (Canberra: Australian Government Publishing Services, 1987). Available: <www.defence.gov.au/Publications/wpaper1987.pdf>, p. 20.
[64] Madeline Carr, 'Public-Private Partnerships in National Cyber-Security Strategies', *International Affairs*, vol. 92, no. 1 (2016). Available: <academic.oup.com/ia/article-abstract/92/1/43/ 2199930/Public-private-partnerships-in-national-cyber?redirectedFrom=fulltext>, p. 46.
[65] US Department of Defense, *The DoD Cyber Strategy*, Washington, DC, April 2015. Available: <www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf>, p. 1.

infrastructure, working on the principle that these assets are privately owned or operated. Governments look to establish public-private partnerships which are based on collaboration and cooperation. If malicious cyber activity should escalate to the point that damage, death and significant disruption to critical infrastructure is imminent, or has occurred, it is expected that a transfer of responsibilities should result as the State assumes control; however, like the considerations shaping this nexus, the actual mechanism to identify and manage this handover point remains unclear.

The purpose of this paper is to identify and explore some of the considerations that impact on the nexus between the public and private sectors as they relate to Australian cyber security of critical infrastructure. At what point, when responding to malicious cyber activity, does the private sector hand over responsibility for an incident to the public sector? The examination of this question will be undertaken in the following manner. The first section explains key definitions. Following this, in the second section, I compare the advantages and disadvantages arising from either of the public and private sectors becoming the sole providers for critical infrastructure cyber security. This includes comparison of the benefits and limitations each sector faces within the cyber security paradigm. In the third section, I discuss what comprises an effective critical infrastructure private-public partnership. The fourth section provides an overview of the critical infrastructure private-public partnerships of the United States, the United Kingdom, and Australia, to contextualise the observations made in sections two and three. The final section concludes that, whilst the responsibility for collective security once resided firmly with the public sector, due to increased levels of globalisation and privatisation it is impossible for this to be achieved without collaboration and cooperation from the private sector. I further conclude that there is no easily identified single point of handover between the public and private sectors regarding the leadership responsibility to manage malicious cyber activity.

Definitions

The definitions applied to this field of enquiry remain contested. A cursory glance at the NATO Cooperative Cyber Defence Centre of Excellence indicates over forty different definitions of cybersecurity, cyber-security or cyber security;[66] however, a comparative discussion of the merits of definitions is beyond the scope of this paper. To allow an effective understanding for the positions being outlined in this paper the following definitions will be applied.

Cyber security, as drawn from the Australian Attorney-General's Department, is described as:

[66] 'Cyber Definitions', NATO CCD COE, 2017, <ccdcoe.org/cyber-definitions.html> [Accessed 13 June 2017].

> one of Australia's national security priorities—Australia's national security, economic prosperity and social wellbeing rely on the availability, integrity and confidentiality of a range of information and communications technology.[67]

The term *cyber attack* has been generically applied to cover any malicious cyber activity involving unauthorised access to a computer, a network, or information. Such a broad definition can include cyber theft, cyber espionage or even 'hacktivism'. For the purposes of this paper the definition used will be as per the Australian Cyber Security Centre 2016 Threat Report, which provides the following definition of a cyber attack:

> a deliberate act through cyberspace to manipulate, disrupt, deny, degrade or destroy computers, or the information resident on them, with the effect of seriously compromising national security, stability or economic prosperity.[68]

As such any deliberate act via cyber space, utilising computers and networks that control and manage critical infrastructure, can turn off or damage systems. This would result in long-term or permanent disruption to essential services and in the potential destruction of the affected critical infrastructure. Dams and power utilities could suffer irreparable damage resulting in not just a disruption of supply, but also destruction of property and loss of life. The Australian Government, according to this definition, would most likely consider such an act as an attack and a threat to national security. It should also be noted that cyber attacks rely on malicious code being introduced to a computer system that initially requires either a deliberate, or unwitting, act of a person to carry out. Once introduced, and active, the malicious code might self-propagate and infect other computers that have similar vulnerabilities. One such example is the Stuxnet virus, which was initially employed against the Natanz nuclear enrichment facility in Iran, but after the attack was found to have spread to thousands of computers across the world.

Understandably each country has reserved its right to define *critical infrastructure* (CI) differently to reflect regional and strategic priorities. The Australian Government has provided the following definition:

> those physical facilities, supply chains, information technologies and communication networks which—if destroyed, degraded or rendered unavailable for an extended period—would significantly impact on the social or economic wellbeing of the nation, or affect Australia's ability to conduct national defence and ensure national security. Critical infrastructure can

[67] 'Cyber Security', Attorney-General's Department, 2017, <www.ag.gov.au/RightsAnd Protections/CyberSecurity/Pages/default.aspx> [Accessed 13 June 2017].
[68] Australian Cyber Security Centre, *ACSC 2016 Threat Report* (Canberra: Commonwealth of Australia, 2016). Available: <www.acsc.gov.au/publications/ACSC_Threat_Report_2016.pdf>, p. 5.

> include services that provide food, water, defence, transportation, energy, communications, public health, banking and finance.[69]

Critical infrastructure is now global and is no longer contained within a nation-state's sovereign borders. Nations rely on multinational companies to provide essential services sourced from other nations. As disclosed by WikiLeaks in 2010, the US Department of Homeland Security compiled an inventory of critical infrastructure located beyond the borders of the United States. Results showed that 259 companies supplied services considered critical to US national security, which included such items and services as ordnance, pharmaceuticals manufacturing, telecommunications and foreign ownership of major ports.[70] From an Australian perspective, the Port of Darwin has been leased for ninety-nine years to the Chinese company Landbridge[71] and, despite being a country with large natural resource reserves, Australia remains dependent upon other nations for oil.[72]

The final concept that requires defining relates to *public-private partnerships* (PPP). These are designed to link public and private sectors to increase efficiency, with the private sector providing expertise and efficiency within facilities and frameworks provided by the public sector.[73] Successful examples may be observed in Singapore, where government-led ICT projects such as the establishment of a government email system, or a Lifestyle Portal for the National Service Community, have been successfully outsourced to private industry.[74]

PPPs within the cyber security environment are less clearly defined as each sector is comprised of a multitude of different organisations.[75] In Australia, the public sector includes the federal government, state governments, industry specific departments such as Energy, Finance and Transport, as well as law enforcement and intelligence agencies and the military. The private sector is equally multifaceted, comprising major critical infrastructure providers, private cyber security companies, Internet Service Providers and

[69] ibid, p. 17.
[70] Dave Clemente, *Cyber Security and Global Interdependence: What is Critical?* (London: Chatham House, the Royal Institute of International Affairs, 2013). Available: <www.chathamhouse.org/publications/papers/view/189645>, p. 7.
[71] S. Everingham, 'Darwin's Port's 99-year Chinese Deal Fund $100 Million Boost to Northern Territory Economy', ABC News, 7 March 2016, <www.abc.net.au/news/2016-03-07/darwin-port-deal-funds-quick-hit-to-nt-economy/7228000> [Accessed 15 June 2017].
[72] Vlado Vivoda, 'Australia's Growing Oil Imports Are an Energy Security Issue', *The Conversation*, 20 June 2012, <theconversation.com/australias-growing-oil-imports-are-an-energy-security-issue-7749> [Accessed 15 June 2017].
[73] Jake Rogers, 'Public-Private Partnerships: A Tool for Enhancing Cybersecurity', Master's Thesis, John Hopkins University, Maryland, 2016. Available: <jscholarship.library.jhu.edu/bitstream/handle/1774.2/40245/ROGERS-THESIS-2016.pdf?sequence=1&isAllowed=y>, p. 14.
[74] Seah Chin Siong, 'Public Private Partnership (PPP)—The Singapore Experience'. IDA International, 2010, Available: <siteresources.worldbank.org/INFORMATIONANDCOMMUNICATIONANDTECHNOLOGIES/Resources/D1S3aP3-JosephTeo.pdf>.
[75] Carr, 'Public-Private Partnerships in National Cyber-Security Strategies', p. 45.

international IT companies such as Microsoft and Apple. Whilst acknowledging the diversity of the public and private sectors, observations made for the purposes of this paper will assume homogenous private and public sectors in order to provide conclusions and observations for future discussions.

The Public Sector as the Sole Provider of Critical Infrastructure (CI) Cyber Security

POSITIVES

A fundamental responsibility for any government is to provide security.[76] Prior to the impacts of cyber space, government confined this task to its people and interests, and was primarily focused within its sovereign border; however, security now encompasses a vastly different and expanded series of qualities. Cyber space has become the fifth dimension—it is manmade and in a continuous state of flux as technology is developed and adopted. Cyber space is embedded with the natural domains of land, sea, air and space[77] and is the "nervous system running through all other sectors, enabling them to communicate and function".[78] The security environment now includes increasing threats from actors with offensive cyber capabilities that can threaten the economy and CI. The Australian Signal Directorate detected in excess of 1,200 cyber security incidents in 2015 against military, energy, banking, transport and communications systems.[79]

Just as it is an immutable responsibility of the public agencies of law enforcement to protect, investigate and prosecute criminals who commit crime, so it should be the responsibility of a government to defend CI from cyber attack. No one expects the owner or operator of CI to protect it against a kinetic attack.[80] Public sector intelligence agencies have access to information that can allow them to provide advance warning of potential cyber attacks against CI. This intelligence product can and should be provided to law enforcement to be utilised as a basis for investigation and prosecution of individuals. If an attack sponsored by non-state actors or nation-states were to occur, a government can respond using a combination of diplomatic measures, economic sanctions, or cyber and kinetic options.

---

[76] Ibid. p. 44.
[77] Larry D. Welch, 'Cyberspace—the Fifth Operational Domain', *Research Note*, IDA, <www.ida.org/~/media/Corporate/Files/Publications/ResearchNotes/RN2011/2011%20Cyberspace%20-%20The%20Fifth%20Operational%20Domain.pdf> [Accessed 14 June 2017], p. 3.
[78] Clemente, *Cyber Security and Global Interdependence*, p. v.
[79] Australian Department of Defence**,** *2016 Defence White Paper* (Canberra: Commonwealth of Australia, 2016). Available: <www.defence.gov.au/WhitePaper/Docs/2016-Defence-White-Paper.pdf>, p. 52.
[80] Senol (Shen) Yilmaz and Kah-Kin Ho, 'Securing Cyberspace: Whose Responsibility', in D. Cheong (ed.), *Cybersecurity: Some Critical Insights and Perspectives* (Singapore: S Rajaratnam School of International Studies, Nanyang Technological University, 2014). Available: <www.rsis.edu.sg/wp-content/uploads/2015/02/Cybersecurity_Critical_Insights_Perspectives.pdf>, p. 40.

NEGATIVES

If the public sector became the sole provider of cyber security for CI significant adjustments would be required by both the public and private sectors. Governments would need to increase their financial commitments to cyber security. Governments are limited by budgetary constraints and thereby have limits to the financial contributions they can make to a CI PPP.[81] The public sector would also require unfettered access to all computer systems and ICT utilised in each facility and industry. CI operators and owners would be resistant to allowing this as they would be concerned about the government having such widespread and sweeping access to confidential commercial information. In April 2015 a security engineer discovered a data breach at the US Office of Personnel Management (OPM). Subsequent investigations revealed that highly sensitive documents relating the background checks and security clearances as well as millions of digital fingerprints records and complete personnel files had been stolen. During the Congressional inquiry it was noted that OPM's security was porous and that the breach resulted due to systematic failures.[82] Data breaches such as this provide good reason for the private sector to be concerned about allowing public sector access to proprietary information.[83]

Finally, if the public sector was to become the sole provider of cyber security for CI, laws and regulations would have to be passed regarding the operations of the private sector to provide the appropriate frameworks in which the public sector could ensure its requirements were met. This would create a significant compliance burden and an increased cost in services.[84]

The Private Sector as the Sole Provider of CI Cyber Security

POSITIVES

As suggested by Clark et al., the solutions for cyber security will come from the private sector as they can respond faster and adapt more quickly. The

[81] G. Austin and J. Slay, 'Benchmarking Australia's Cyber Security Strategy: A Future Looking Checklist', Australian Centre for Cyber Security, UNSW Canberra, 19 April 2016. Available: <www.unsw.adfa.edu.au/australian-centre-for-cyber-security/sites/accs/files/uploads/BENCHMARKING AUSTRALIAN CYBER SECURITY POLICY_0.pdf>, p. 9.
[82] B. Koerner, 'Inside the Cyberattack that Shocked the US Government', *Wired*, 2016, <www.wired.com/2016/10/inside-cyberattack-shocked-us-government/> [Accessed 13 April 2018].
[83] Jody Westby, 'The Government Shouldn't Be Lecturing Private Sector On Cybersecurity', *Forbes*. 15 June 2015, https://www.forbes.com/sites/jodywestby/2015/06/15/the-government-shouldnt-be-lecturing-the-private-sector-on-cybersecurity/#1cbd919a621b> [Accessed 6 June 2017].
[84] Amitai Etzioni, *The Private Sector: A Reluctant Partner in Cybersecurity* (Washington, DC: Institute for Communitarian Policy Studies, The George Washington University, 2014), <icps.gwu.edu/private-sector-reluctant-partner-cybersecurity> [Accessed 6 June 2017], p. 73.

private sector has a greater pool of people to draw upon.[85] Etzioni observes that the private sector does not have constitutional restrictions that regulate government investigations, that there are already numerous private security companies able to investigate cyber attacks, and that the private sector has confidence that it can handle their own cyber security.[86] Germano provides an economic justification that as cyber crime exposes the private sector to financial and intellectual loss, it is something the private sector is best positioned to address.[87] Private companies who run CI are the first responders and, together with major IT vendors and private cyber security companies, have defensive capabilities comparable to the military.[88]

NEGATIVES

If responsibility for provision of cyber security for CI rests solely with the private sector a major ethical adjustment would be required. Corporate participants would need to attempt to divert their focus from profit and shareholder demands and give greater attention to the common good of national security. The social benefits derived from cyber security for CI does not readily translate into economic benefits. The private sector has always balanced the cost of a cyber attack against the cost of preventing one.[89] To expand on this point it is worth considering the US nuclear energy industry, as many commonalities exist to CI in Australia.[90] Cyber risks to nuclear facilities require constant monitoring and evaluation. Most nuclear power plants generally have the same process control systems as conventional power plants; however, conventional power plants generally have hardened hardware and cyber security. Although nuclear power plants have more stringent safety requirements they upgrade their hardware less frequently—usually long after the expected life span. This means that the nuclear industry is not keeping up with technological advances and is vulnerable to cyber attack.[91] In other CI industries infrastructure is being modernised

[85] Steve Clark, Anthony Court, Mark Tims and Gordon Archibald, 'Cyber Security: Designing a Government-Business Partnership in Australia', KPMG, 2016. <assets.kpmg.com/content/dam/kpmg/pdf/2016/03/cyber-security-business-government-partnership-2016.pdf> [Accessed 6 June 2017], p. 4.
[86] Judith H. Germano, 'Cybersecurity Partnerships: A New Era of Public-Private Collaboration', The Centre on Law and Security, New York University School of Law, 2014. Available: <www.lawandsecurity.org/wp-content/uploads/2016/08/Cybersecurity.Partnerships-1.pdf>, p. 2.
[87] Amitai Etzioni, 'Cybersecurity in the Private Sector', *Issues in Science and Technology*, vol. 28, no. 1 (2011), pp. 58-62. <papers.ssrn.com/sol3/papers.cfm?abstract_id=2356955>, p. 58.
[88] Sean D. Carberry, 'Why the Private Sector is Key to Cybersecurity', FCW, 1 March 2017, <fcw.com/articles/2017/03/01/why-the-private-sector-is-key-to-cybersecurity.aspx> [Accessed 6 June 2017].
[89] Carr, 'Public-Private Partnerships in National Cyber-Security Strategies', p. 57.
[90] Caroline Baylon, with Roger Brunt and David Livingstone, *Cyber Security at Civil Nuclear Facilities: Understanding the Risks* (London: Chatham House, the Royal Institute of International Affairs, 2015), <www.chathamhouse.org/sites/files/chathamhouse/field/field_document/20151005CyberSecurityNuclearBaylonBruntLivingstoneUpdate.pdf. p. v.
[91] Brent Kesler, 'The Vulnerability of Nuclear Facilities to Cyber Attack', *Strategic Insights*, vol. 10. no. 1 (2011), <large.stanford.edu/courses/2015/ph241/holloway1/docs/SI-v10-I1_Kesler.pdf>, pp. 18-19.

using affordable but vulnerable and insecure off-the-shelf software and hardware. The private sector is sanguine about capturing the ICT dividends (for example, banks have moved to e-commerce and reduced staff and facilities, and energy utilities companies no longer need to send staff to remote locations to manually activate valves and switches) but is not reinvesting this dividend from reduced costs in security.[92]

Owners and operators are also concerned about exposure to liability should a cyber attack occur. The US nuclear energy industry is reluctant to publicly declare malicious cyber activity as they do not want to damage the public perception of this industry.[93] This management of public perception is also apparent in other nations. In December 2014 the DPRK (North Korea) commenced malicious cyber activity against nuclear facilities in the ROK (South Korea). Fortunately, the malware was detected and contained; however, this incident exposed insufficient monitoring of standards by the ROK authorities, and corruption regarding unreported or misreported compliance by the owners and operators of the CI.[94]

The private sector remains uncomfortable with information sharing and declaring data breaches as this creates opportunities for competitors to gain a market advantage, and fuels damaging publicity and lawsuits.[95]

Effective CI PPP

As illustrated in the previous sections, neither the public nor private sector are able to take sole responsibility for delivering CI cyber security without significant prohibitive adjustments. Effective CI PPPs should have four elements. One; collaboration and sharing of information and best practices. Two; facilitation of commercial incentives, such as tax breaks and low interest loans, in order to maximise private sector investment. Three; regulations that are developed in close cooperation so as to ensure cyber security standards are met in a manner that does not inhibit profit-making.[96] Four; a clear understanding of when, and how, the leadership responsibility will change between the public and private sectors.

---

[92] Alexander Klimburg (ed.), *National Cyber Security Framework Manual* (Tallinn: NATO CCD COE, 2012). Available: <ccdcoe.org/publications/books/NationalCyberSecurityFramework Manual.pdf>, p. 36.
[93] Caroline Baylon, 'Cybersecurity Threats to Critical Infrastructure: A Case Study of Nuclear Facilities', in Cherian Samuel and Munish Sharma (eds), *Securing Cyber Space: International and Asian Perspectives* (New Delhi: IDSA, Pentagon Press, 2016). Available: <www.idsa.in/ book/securing-cyberspace_csamuel-msharma>, p. 170.
[94] Kyung-bok Lee and Jong-in Lim, 'The Reality and Response of Cyber Threats to Critical Infrastructure: A Case Study of the Cyber-terror Attack on the Korea Hydro & Nuclear Power Co., Ltd', *KSII Transactions on Internet and Information Systems*, vol. 10, no. 2 (2016), pp. 857-80. <www.itiis.org/digital-library/manuscript/1262>.
[95] Etzioni, *The Private Sector: A Reluctant Partner in Cybersecurity*. pp. 70-72.
[96] Yilmaz and Ho, 'Securing Cyberspace: Whose Responsibility', pp. 40-41.

The most important element of the CI PPP is information sharing as this develops trust and confidence. The public sector needs to ensure that intelligence is analysed, classified correctly, and that its passage to relevant parties is timely. The private sector needs confidence that information sharing will not expose companies to predatory market competitors or to unnecessary litigation.[97]

Incentives and regulations are vital to any CI PPP. These provide an understanding of responsibilities, expectations and standards and establish the framework in which information sharing can occur. Regulations can be created in two ways. One way is for the public sector to establish the conditions required to facilitate cyber security and the private sector to employ voluntary measures to ensure cyber security. Voluntary uptake has only public perception and approval of participating organisations as an incentive. A second way is for governments to regulate through law private sector standards for technical development, internal security controls and disaster recovery plans. The second of these methods may be encouraged through the introduction of tax breaks, stimulus grants, low-cost loans, subsidies, reduced insurance premiums and liability protection to provide financial relief to the owner and operators of CI.[98]

Overview of the US, UK and Australian CI PPP

By 2001, 85 per cent of US CI was privatised. With privatisation came increased discretion on the part of those managing the infrastructure to be selective if and how they moved systems and technologies from proprietary systems to generic and unsecured computer systems.[99] US President Bill Clinton declared that cyber security was based on CI PPP. This description of CI PPP as a 'cornerstone' of national cyber security[100] has been upheld by every subsequent US President. During President Obama's administration, several Presidential Policy Directives and Executive Orders related to CI PPP were signed. These aimed to facilitate an integrated approach between private and public organisations to ensure better security and resilience against cyber attacks, acts of terrorism, pandemics and natural disasters,[101] and acknowledged the importance of balancing cyber security with the competing needs to encourage innovation and economic prosperity.[102] In 2015 the US National Security Strategy declared that a strong and innovative economy was one of its four national interests and a

[97] Carr, 'Public-Private Partnerships in National Cyber-Security Strategies', p. 58.
[98] Klimburg, *National Cyber Security Framework Manual*. p. 38.
[99] Carr, 'Public-Private Partnerships in National Cyber-Security Strategies', p. 52.
[100] Ibid. p. 44.
[101] Department of Homeland Security, *Presidential Policy Directive 8: National Preparedness*, Washington, DC, 2011. Available: <www.dhs.gov/presidential-policy-directive-8-national-preparedness>.
[102] Executive Order No. 13,636, 3 C.F.R., 11,739 (2013)—'Improving Critical Infrastructure Cybersecurity', 12 February 2013. Available: <obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity>.

catastrophic attack on critical infrastructure placed at the top of its strategic risks.[103] This document elaborates that cyber security will be achieved by using a whole-of-government approach emphasising that the Internet is a shared responsibility between the states and private sector, with civil society and internet users as key stakeholders.[104]

The US approach appears fragmented because different CI industries interface with different government departments.[105] There has also been marked resistance from the private sector to the introduction of regulations, and proposals introduced in Congress have not been passed into laws. In 2009 President Obama stated that "my administration will not dictate security standards for private companies".[106]

The UK National Cyber Security Strategy 2016-2021 articulates that cyber risks are not properly understood or managed, and that the UK Government, working with other responsible authorities, will ensure that CI is sufficiently secure and resilient. However, neither the government nor other public bodies will take on the responsibility of providing cyber security for CI. They believe that responsibility sits with the boards, operators and owners of the CI. The UK Government will provide support, in the form of information sharing, guidance and training. The UK Government will also monitor assurance via exercises to test cyber security. The private sector must secure their own systems or expect that the UK Government will intervene in the interests of national security.[107]

Australia's Cyber Security Strategy 2016 and its 2017 Update[108] describe the foundation policy articulating the federal government's approach to national cyber security. The ideas that are presented in this document are drawn from a classified Cyber Security Review led by the Department of the Prime Minister and Cabinet[109] and are presented as part of a whole-of-nation approach to assist in the establishment of CI PPP. This strategy acknowledges that the public and private sectors will set the strategic agenda and that information sharing, collaboration and cooperation,

[103] President of the United States of America, *National Security Strategy 2015* (Washington, DC: The White House, 2015). Available: <nssarchive.us/wp-content/uploads/2015/02/2015.pdf>. pp. 2-3.
[104] Ibid. pp. 12-13.
[105] Harry D. Raduege, 'The Public/Private Cooperation We Need on Cyber Security', *Harvard Business Review*, 18 June 2013, <hbr.org/2013/06/the-publicprivate-cooperation> [Accessed 6 June 2017].
[106] Etzioni, *The Private Sector: A Reluctant Partner in Cybersecurity*, pp. 73-74.
[107] HM Government, *National Cyber Security Strategy 2016-2021.* London: HM Government, 2016). Available: <www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf>, pp. 40-41.
[108] Department of the Prime Minister and Cabinet, *Australia's Cyber Security Strategy: First Annual Update* (Canberra: Commonwealth of Australia, 2017), <cybersecuritystrategy.dpmc.gov.au/first-annual-update/>.
[109] Department of the Prime Minister and Cabinet, *Australia's Cyber Security Strategy* (Canberra: Commonwealth of Australia, 2016), <cybersecuritystrategy.dpmc.gov.au/>. p. 5.

facilitated by the Australian Cyber Security Centre, the Australia Computer Emergency Response Team, law enforcement and intelligence agencies, and business and private security companies, will make resilient and resistant computer networks and systems.[110]

While this strategy delivers normative statements,[111] insufficient attention is given to the allocation of responsibility, authority, or the monitoring of standards and outcomes. Strategic statements should include tangible outcomes defined in terms of who, what, when and how.[112] Yet despite this apparent shortcoming, the Australian Cyber Security Centre 2016 Threat Report provides a brief example of an AUSCERT (Cyber Emergency Response Team for Australia) coordinated response to an intrusion of a critical infrastructure network that suggests that successful collaboration and cooperation between the public and private sectors is occurring.[113]

The private sector has been elevated to co-leader in the Australian Government's Cyber Security Strategy 2016. Both sectors will co-design voluntary standards and operate new cyber threat sharing centres whilst undertaking combined cyber incident exercises. Any future success for Australian CI PPP will require the public sector to clearly articulate policy goals, otherwise the private sector will raise concerns—particularly if the costs outweigh the benefits.[114]

Where is the Nexus?

Successful partnership is based on clear demarcation of responsibility. Governments at all levels struggle to deal effectively with changes in technology as they are not adequately funded and can be sluggish to respond. This is why much of the responsibility to defend the internet resides with private organisations.[115] Clear statements that outline legal authority, responsibility and rights are essential. CI PPPs that work do so either because they have shared goals, such as the US and Australian model, or they have regulations in place, as seen in the UK example.[116]

---

[110] Ibid. p. 6.
[111] Ibid.
[112] Chris Brookes, *Cyber Security: Time for an Integrated Whole-of-Nation Approach in Australia*, Indo-Pacific Strategic Paper (Canberra: The Centre for Defence and Strategic Studies, Commonwealth of Australia, 2015), <www.defence.gov.au/ADC/Publications/IndoPac/150327 Brookes IPS paper - cyber %28PDF final%29.pdf>, p. 47.
[113] Australian Cyber Security Centre, *ACSC 2016 Threat Report*, p. 18.
[114] Liam Nevill, 'Pushing a New Model For Public–Private Cyber Partnerships', *The Strategist*, Australian Strategic Policy Institute, 2016, <www.aspistrategist.org.au/pushing-a-new-model-for-public-private-cyber-partnerships/> [Accessed 6 June 2017].
[115] Anthony H. Cordesman and Justin G. Cordesman, *Cyber-Threats, Information Warfare, and Critical Infrastructure Protection: Defending the US Homeland* (Washington, DC: Centre for Strategic and International Studies, 2002), p. 151.
[116] Carr, 'Public-Private Partnerships in National Cyber-Security Strategies', p. 62.

When considering a generalised workflow of malicious cyber activity, the following division of leadership responsibilities, as it relates to Australian CI PPP, are apparent:

Table 1: Leadership Responsibility

Stage	Activity	Responsibility Lead	
		Public	Private
1	Set standards, incentives and regulations. Collect/share intelligence.	✔	✔
2	Train Workforce. Test/Upgrade/Manage CI resilience. Notify ALL malicious cyber activity to AUSCERT. Respond to malicious cyber activity.		✔
3	Monitor/Assess and provide advice. Liaise with public/private security organisations to coordinate responses.	✔	
4	Repair damage/Restore services.		✔
5	Investigate, prosecute and respond.	✔	

It is worth noting that at each stage the leadership responsibility alternates and that these stages should not be considered in a strictly sequential manner. Many of these activities require concurrent support from other activities within other stages. As such this adds additional dimensions when considering at what point a hand over of responsibility occurs. This ambiguity of responsibility is further demonstrated with a linear model, see Figure 1 that positions the public and private sectors at opposite ends and employs the previous five stages.

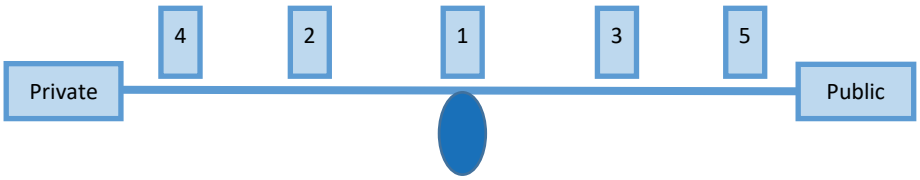

Figure 1: Leadership—A Linear Model

As incidents occur and responses are developed and enacted, the nexus will, by necessity, slide towards either end of the model dependent upon where the balance of responsibility lies. At different stages, in reaction to ongoing developments, both the private and public sectors will alternate as the principle responders. The nexus for the handover of responsibility cannot be situated at a static location and nor can it be in two places at the same time.

Malicious cyber incidents include hacktivism, IP theft, espionage and attack. Unfortunately, the nature of these incidents is such that in the initial stages it is not always apparent what the intent may be. This is further complicated due to the anonymity of the attacker's identity and a potential lack of intelligence regarding motivation, as without these details a comprehensive threat assessment is not possible. Failures of CI such as electrical black outs are usually temporary and are a part of everyday life.[117] Malicious cyber incidents, such as those against the US energy sector in 2014—Energetic Bear and Black Energy—were campaigns designed not to destroy, but rather to carry out reconnaissance for future malicious cyber activity.[118] Effective and timely communication of similar incidents to ACSC or AUSCERT will allow coordination with different agencies and reduce any impacts that might threaten national security.

Conclusion

This paper has presented examples and case studies that illustrate that the responsibility for the protection of CI remains divided between the public and private sector. If a malicious cyber attack develops, the actual leadership responsibility will also change from the private to the public sector, or in fact be shared. Unless regulations, laws and policies compel the private sector to allow the public sector full access to systems and networks, it is unlikely that the public sector will be capable of assuming sole responsibility for the protection of CI. The public sector's responsibility should be to develop policy and strategy and to provide intelligence to assist the private sector in improving resilience and then to investigate, prosecute and respond as required. The Australian private sector has a critical role to play in national security but should become more willing to contribute to the common good.

I have examined CI PPPs to consider the factors that influence the nexus between the public and private sectors as it relates to Australian cyber security of CI. Relevant examples from other countries, such as the United States and the United Kingdom, have been used to assist with illustrating common themes regarding Australian CI PPP. This analysis leads to the conclusion that the nexus for responsibility of CI PPP leadership between the public and private sectors in Australia remains, at the very least, dynamic and will vary according to the threat assessment of individual incidents.

Vaughan Grant is a Captain in the Australian Army. He holds a Master's in Cyber Security, Strategy and Diplomacy, a Master's in Defence Studies, both from ADFA@UNSW and Bachelor Degrees in Arts and Music from the University of Melbourne. CAPT Grant is a member of the Royal Australian Signal Corps.

[117] Cordesman and Cordesman, *Cyber-Threats, Information Warfare, and Critical Infrastructure Protection: Defending the US Homeland*, p. 4.
[118] Clint Witchalls, 'How Can We Protect Infrastructure From Cyber Attacks?', World Economic Forum, 29 September 2015, <www.weforum.org/agenda/2015/09/how-can-we-protect-infrastructure-from-cyber-attacks/>.