2023-2030 Australian Cyber Security Strategy

Discussion Paper Submission

By Roger Spence

- Cyber Security Professional and UNSW/ADFA Masters Student

Discussion Paper Question 1 - ***What ideas would you like to see included in the Strategy to make Australia the most cyber secure nation in the world by 2030?***

My suggestion - Australia has built a high-quality, middle-power cyber capability, but the cyber-skills gap demands innovative ideas such as a Defence Force Reserve ***"Cyber Militia"*** should be considered along with tighter integration between the public and private sectors.

Supporting Arguments

A Cyber Journey

Australia has arguably come a long way since first formally acknowledging the threat to its information infrastructure in the 2000 Defence Whitepaper, although it is both interesting and illuminating to note that at that time, cyber-attack was seen to be a "non-military" threat, albeit one that demanded a thorough and national strategy to be developed.[1] Even as early as 2001, the importance of government collaboration with private industry to help protect our "National Information Infrastructure" was highlighted through the E-Security Initiative, which allocated $2 million to the task in the 2001/2002 Federal Budget.[2] A paltry sum by today's standards, nonetheless, even then it was explicitly recognised that since the vast majority of this digital infrastructure was in the hands of private industries such as telecommunications, transport, distribution, energy, utilities, banking and finance, it would be critical to develop strong partnerships between the public and private sectors to ensure the security of Australia's national interests and the prosperity that the new digital information economy offered.

It wasn't until a Ministerially appointed, expert panel report on community consultation regarding defence policy issues was released in 2015 that cyber security was highlighted as a key area where

[1] Australian Government. "Defence 2000: Our Future Defence Force". 2000. Pages 8 & 30. Retrieved from : https://defence.gov.au/publications/wpaper2000.PDF

[2] Australian Government News Release, Attorney-General. "Budget 2001-2002. E-SECURITY INITIATIVE - PROTECTING THE NATIONAL INFORMATION INFRASTRUCTURE". 22 May 2001. Retrieved from : https://parlinfo.aph.gov.au/parlInfo/download/media/pressrel/IM446/upload_binary/im4461.pdf;fileType=application%2Fpdf#search=%22media/pressrel/IM446%22

"industry and civilians could make a growing contribution to the defence effort", including the potential for exchanges of highly skilled personnel between the military and the private sector.[3] The 2016 Defence White Paper continued to expand on the strategic assessment of *"non-geographic threats"* to national interests, which included specific mention that *"Defence will contribute to the Government's enhanced national cyber security efforts"* and that coordination would be improved between the public sector, industry and academia.[4]

Commitment to strategy and structural investment in Australia's cyber warfare preparedness was further reinforced in 2017 with the establishment of the Information Warfare Division (IWD) under the Joint Capabilities Group, reporting directly into the Australian Chief of Defence Force. It is the Division's explicit role to ensure ADF has the right mix of people, technology and process to *"combat the growing threat of information warfare to our warfighting capability and Australia's national interests"*.[5]

The Australian Signals Directorate has explicitly acknowledged the local cyber security skills shortage, even across both private industry and the public sector.[6] The ability for any national government or military organisation to attract and retain the best cyber-security talent will forever be a significant challenge due to the large wages disparity. It could also be reasonably assumed that many of the brightest potential candidates in this field may tend to be of an inventive and creative disposition that may make them unsuitable for public or military service.

A particularly innovative approach that the Australian Department of Defence has taken to addressing this issue is the "Australian Defence Force Cyber Gap Program", initially launched in 2020. This is a 12-month program offering financial support, mentoring and work experience with Defence while students undertake study towards eligible and relevant qualifications. Participants are not obligated to join Defence at the end of their program, however they will be exposed to the extensive employment opportunities available in the Defence cyber domain. If they choose not to join Defence, it is anticipated that the nation will nation will still benefit from their skills and expertise.[7]

[3] Defence Minister appointed External Panel of Experts. *"GUARDING AGAINST UNCERTAINTY: AUSTRALIAN ATTITUDES TO DEFENCE. Report on community consultations."*. 2015. Page 9. Retrieved from : https://www.defence.gov.au/sites/default/files/2021-08/GuardingUncertainty.pdf

[4] Australian Government. *"2016 Defence Whitepaper"*. 2016. Page 69-73. Retrieved from : https://www.defence.gov.au/sites/default/files/2021-08/2016-Defence-White-Paper.pdf

[5] Australian Government Department of Defence Website. "Information Warfare Division." Accessed 25 Oct 2021 : https://www.defence.gov.au/jcg/iwd.asp

[6] Australian Government website, "Inspiring a new generation", Australian Signals Directorate: Australian Cyber Security Centre, December 4, 2018. Accessed July 26, 2021 : https://www.cyber.gov.au/acsc/view-all-content/news/inspiring-new-generation

[7] Australian Government Website. ""Australian Defence Force Cyber Gap Program". Accessed : https://www.digitalprofession.gov.au/cybergap

In parallel, and in recognition that the Government can help play a major role in helping the private sector help itself, the Australian Cyber Security Centre (ACSC) released the *"Essential 8 Maturity Model"* in 2017 as a minimum standard framework for organisations (public and private) to assess themselves against. Updated regularly, the *"Essential 8"* provides a series of cyber-risk mitigation strategies that can greatly assist an organisation in terms of prioritising their effort and expenditure on cyber security and has become the de-facto cyber-security standard framework for many businesses that may not obviously fall under the domain of industry information security standards and benchmarks such as ISO-27001 or the NIST Framework.[8]

International Experiences

Following the 2016 Defence White Paper release, Greg Austin (currently Senior Fellow for Cyber Power and Future Conflict at the International Institute for Strategic Studies), raised the idea of developing an Australian Defence Force Reserve "Cyber Militia", similar to what the Estonian Government had successfully done following an attack by Russian hackers in 2007.[9] The Cyber Defence Unit of the Estonian Defence League is often held up as an innovative example of how the public sector can leverage civilian cyber security experts as part of a volunteer force to strengthen defensive cyber capability in times of crisis, as well as raising awareness of cyber security principles and practices across the general population.[10] The Estonian Defence League is a volunteer force that works alongside and augments the professional Estonian Defence Force, similar to Australia's Army, Navy and Airforce Reserve units. Organisational supervision and legal oversight are controlled by the Government and Minister for Defence in the same way that Estonia's regular Defence Force is managed and with the same degree of relative transparency and accountability.

Israel is also often cited as an example of tight public/private collaboration in cyber security, however for different reasons. Whilst it is not known to maintain a "Cyber Militia" in the way that Estonia does, Israel's Defence Force is itself extremely porous in the sense that most adults are required to serve a mandatory period of time in the armed forces, primarily because Israel considers itself a nation surrounded by enemies that are sworn to destroy it, by any means necessary.[11] The best and brightest

[8] Australian Signals Directorate, Australian Cyber Security Centre website. "Essential Eight Maturity Model". Last updated 6 Oct 2021. Accessed : https://www.cyber.gov.au/acsc/view-all-content/publications/essential-eight-maturity-model

[9] Oriti, Thomas. "*Rise of ransomware attacks prompts expert calls for governments to establish 'cyber militia'*". ABC News, The World Today. 9 Jun 2016. Retrieved from : https://www.abc.net.au/news/2016-06-09/call-for-cyber-militia-to-deal-with-rising-ransomware-attacks/7496242

[10] Kaska, K., Osula, A. and Stinissen, J. "The Cyber Defence Unit of the Estonian Defence League - Legal, Policy and Organisational Analysis". NATO Cooperative Cyber Defence Centre of Excellence. 2013. Page 5. Retrieved from : https://ccdcoe.org/uploads/2018/10/CDU_Analysis.pdf

[11] "Surrounded by enemies, but protected by God", *Jewish Voice*, November 3, 2017. Accessed from : https://www.jewishvoice.org/read/blog/surrounded-enemies-protected-god

of its recruits are often sent to serve in the elite "Unit 8200", tasked with undertaking Israel's offensive cyber activities and the largest unit of the Military Intelligence Directorate.[12] After completing their compulsory service period (usually between two and three years), operators are actively encouraged to move directly into the cyber-tech industry to monetise their learnings.[13] It is not surprising then, that Israel is the second largest exporter of cyber technology behind the United States and in a recent "Hot 150" list of the most innovative cyber companies globally, 30 of them are either headquartered or have their Research and Development based in Israel.[14]

The Chinese Government has very explicitly outlined the emphasis it places on a strong cooperation between civilian and military cyber-security capability. In 2017, the Cyberspace Administration of China (CAC) released prescriptive instructions to implement civil-military integration, specifying the need to *"Promote the deepened development of military-civilian integration for cybersecurity and informatization."*[15]

There is considerable international precedent for the active interplay between the public and private sectors to enhance nation-state war fighting capability, and many governments around the world, Australian included, have long identified the importance of ensuring there is adequate organisational connectivity between civilian and military bodies to enable this collaboration. The challenges of enlisting private industry for taking on direct, offensive operations against national adversaries are very significant however, and as such most nations are proceeding with caution in this area (and rightly so).

Conclusion

Australia has over 20 years of official focus on cyber-security as an explicit priority for the defence of national interests and critical information infrastructure. We have long recognised that since most of these assets reside in private ownership, that preparedness for a modern war demands close cooperation and collaboration between the public and private sectors. From small beginnings and tiny budgets at the turn of the century, the Australian Government has built a significant and

[12] "Cyber Capabilities and National Power: A Net Assessment." 2021. *IISS*. June 28, 2021. Page 71. Retrieved from : https://www.iiss.org/blogs/research-paper/2021/06/cyber-capabilities-national-power

[13] Kane, Alex. (2016). "How Israel Became a Hub for Surveillance Technology." *The Intercept*, 18 October, 2016. Retrieved from : https://theintercept.com/2016/10/17/how-israel-became-a-hub-for-surveillance-technology/

[14] "Hot 30 Israeli Cybersecurity Companies To Watch in 2021 Announced by Cybercrime Magazine". EIN Presswire (Cybersecurity Ventures). January 13, 2021. Retrieved from : https://www.einnews.com/pr_news/534447804/hot-30-israeli-cybersecurity-companies-to-watch-in-2021-announced-by-cybercrime-magazine

[15] Theoretical Studies Center Group, Cyberspace Administration of China. Translation of *"Deepening the Implementation of General Secretary Xi Jinping's Strategic Thinking on Building China into a Cyber Superpower: Steadily Advancing Cybersecurity and Informatization Work"*. Translated by Kania, E., Sacks, S. and Webster, G. New America, Cybersecurity Initiative – *"China's Strategic Thinking on Building Power in Cyberspace"*. Retrieved from : https://www.newamerica.org/cybersecurity-initiative/blog/chinas-strategic-thinking-building-power-cyberspace/

internationally respected Cyber Security Strategy and invested in multiple organisations and programs to foster close working relationships between industry and government at all levels. Other governments around the world have also identified civil and military partnership as critical to their own cyber-warfare strategies, however this has primarily been limited to defensive operations.

There has been some limited discussion of Australia forming a “Cyber Militia” in the past, however I am not aware of any formal plans to implement such a thing. Whilst Australia has started building better structure and organisation around the sharing of information, as well as resilience and response support between the public and private sectors, I suggest an active, co-ordinated and transparently managed “Cyber Militia” is an idea that is very worthy of discussion. This is especially true given the widely reported cyber-skills shortage in this region, and indeed around the world. Overall, Australia has built a high quality middle-power cyber capability, but can benefit from further investment in public/private integration and a Defence Force Reserve “Cyber Militia” could greatly enhance our current Government’s stated objective of making Australia the most cyber-safe country in the world by 2030.