2020 Discussion Paper Submission

What is your view of the cyber threat environment? What threats should Government be focusing on?

My view is that with ever expanding cyber entrenchment in modern society, internal threats posed by people are increasing at an alarming rate. These threats range from malicious activities from say burned former employees seeking vengeance, to the more benign and more pervasive threat of poor cyber hygiene. As 5G becomes implemented the threat surface in the cyber domain expands with it. Concurrently, interaction with the cyber domain from Australian citizens also rapidly increases[1]. Against this backdrop, state-based cyber attacks are a constant looming threat, and will gleefully exploit the vulnerabilities posed by a population that does not conduct itself well online, is poorly educated due to factors such as age or experience, and an overall system that prioritises atomisation of the cyber domain amongst persons, businesses, governments and all actors in the Australian tapestry. The proliferation of global-cybercrime related damages has surged, as ransomware attacks and other impressive breaches causing immense damage both in cost and with social or political ramifications[2].

The threats the government should be focussing on can be organised into states, state supported actors (APT's), malicious individuals and finally, oblivious individuals. Oblivious individuals are characterised as a threat as there is no question specifying addressing vulnerabilities. Concurrently, oblivious individuals with poor cyber hygiene can leave shocking exposures in networks and can threaten multiple networks at once. The decisions of companies and how they approach cyber security can also have dire consequences on the strength of Australia's defences – it is apparent that many do not realise that just because Company A may not be palatable to cyber attackers, Company B is, and there is a network connection between the two. This allows an attack pathway that Company A may not be considerate of. Poor management of computer networks is one of the most significant risks in the cyber domain in fact, the supposed asymmetry of cost is actually just lack of defensive coordination[3]. Poor management of security systems combined with poor understanding of hygienic

[1] "Securing a Connected Future: 5G and IoT Security ", SecurityWeek, 2019, accessed October 1, 2019, https://www.securityweek.com/securing-connected-future-5g-and-iot-security.

[2] "Cyber Hygiene 101: Implementing Basics Can Go A Long Way," SecurityWeek, updated August 7, 2019, accessed October 1, 2019, https://www.securityweek.com/cyber-hygiene-101-implementing-basics-can-go-long-way.

[3] Rebecca Slayton, "What Is the Cyber Offense-Defense Balance?," *International Security* 41, no. 3 (2017), https://doi.org/10.1162/ISEC_a_00267. p 89.

practices are a significant threat to Australia's cyber domain that need greater emphasis in future strategies.

The importance of good cyber hygiene is emphasised by the inherent difficulties of a corporate sector level cyber attack having a deterrence by punishment mechanism as a response. Who deploys this punishment mechanism, often referred to as a hack-back? Conversely, with the reticence that many in the private sector have about reporting breaches, if the government is the sole arbiter of cyber weapons (as many argue should be the case), then how entwined will government agencies like ASD need to be with the corporate sector to act as a punishment tool? For these reasons, cyber hygiene should be a much stronger consideration from a policy perspective[4]. There is very little framework in place that would alleviate anxieties about corporations conducting offensive cyber operations in their own right, nor is there any indication of capability to do so from much of the private sector. Deterrence by denial strategies like enhancing cyber hygiene will most likely be far more efficient for alleviating stresses on the private sector in the future.

Do you agree with our understanding of who is responsible for managing cyber risks in the economy?

Yes, however I would also like an acknowledgement that the government should step up its responsibility in this arena. The private sector has been woeful in establishing robust cybersecurity systems, is reliant on heavy government investment anyway, cannot withstand persistent threats like APT's (economic cyberwarfare is a noted Chinese strategy for reference), and in many cases seems outright bewildered by an incredibly rapidly developing field. The Australian government will be required to step up and fill this gap.

This will require some rethinking about who is responsible for managing cyber risks in the economy. The placement of responsibility on vendors who distribute and sell security products is worthwhile, but the government should lead in demanding a higher standard of product be available on the market. The procuring power of the government can establish rigorous standards on the products produced by the security sector, which can cause a lift in standards of excellence across the domain[5]. This approach in essence places responsibility on the government if nothing else, as they become the arbiters for excellence. The government must be active in determining the minimum standards of security

[4] "Countermeasure: Hack the Hacker?," Security Week, updated September 4, 2019, accessed October 1, 2019, https://www.securityweek.com/countermeasure-hack-hacker.

[5] Fergus Hanson, "Australia's Cyber Strategy, 2.0 ", *Australian Strategic Policy Institute*, September 18, 2019, https://www.aspistrategist.org.au/australias-cyber-strategy-version-2-0/.

products that it itself would accept, and then establish with the private sector that these standards should be met by them as well.

Do you think the way these responsibilities are currently allocated is right? What changes should we consider?

No. It is my opinion that government needs to take stronger control of the cyber domain and enforce stricter quality demands on how the private sector engages with it. Currently, there is a significant disconnect between average users of the cyber domain and the comprehension levels needed from them. It is my opinion that much of this is caused by the government itself not taking as proactive a role as it could (despite significant recent efforts), and the private sector especially not taking as significant a role as it could. Across the board in the private sector it appears that devotion to cyber security and concepts like cyber hygiene are restricted to the security workforce – this is a BOGSAT[6]. There is little to be gained in cybersecurity experts talking amongst one another in an organisation and saying things should be better. Hygiene must be improved across the board. In this day and age there is little excuse for phishing attacks being successful other than users of the cyber domain are either recalcitrant, or the management systems made to assist them in engaging with the cyber domain are.

Currently, government should consider greatly increasing cyber hygiene practices through an all-of-domain approach. Every person engaging in the cyber domain needs some assistance in this regard. Concurrently, government should consider legislating changes that allow state authorities such as ASD having greater control over the cyber domain in Australia.

What role should Government play in addressing the most serious threats to institutions and businesses located in Australia?

Cyberdeterrence is a hot topic in the cyber domain at present and will likely remain that way. What deterrence itself requires is technical capability, political willpower, and communication of these facets. Therefore, the role the government should play in addressing threats is as the principle deterrent mechanism in the cyber domain. The Government must emphasise the development of technical capability, there must be a clear political willpower to deploy punishment mechanisms, and there must be clear communication of this. This will begin to satisfy a deterrence by punishment strategy. Concurrently, the promulgation of hygiene strategies across multiple sectors will make meaningful contribution to deterrence by denial – making Australia more difficult to attack

[6] Bunch Of Gurus Sitting Around Talking.

in the cyber domain will be a significant and necessary step to advance cybersecurity[7].

How can Government maintain trust from the Australian community when using its cyber security capabilities?

An increasing concern among both civilian populations and governments around the world alike is the proclivity to deploying advanced surveillance and cyber domain-oriented capabilities against a government's own civilian population. The protests in Hong Kong have illuminated the rejection that civilian populations have against advanced surveillance techniques in particular. If the government wish to maintain levels of trust amongst the civilian population then a clear commitment against using such methods against protesters and the like would be a good start. Technology in surveillance is advancing at an incredibly fast rate, and civilian populations risk becoming increasingly unaware of how they are being observed. Maintaining trust will require transparency, honesty and genuine justification for the deployment of cyber domain capabilities however, this will be most important should they be deployed against the Australian population themselves. When deploying these capabilities overseas, announcements should be very carefully considered. The nature of cyber capabilities is too much information relating to targets themselves can reveal attack vectors and nullify cyber weapons.

What are examples of best practice behaviours change campaigns or measures? How did they achieve scale and how were they evaluated?

A useful first step in addressing cyber hygiene deficits is first engaging with the key common issues to hygienic practices. Pfleeger et al posit that good hygiene requires developing good security habits for individuals and good security routines for organisations[8]. Other commentators like Singer discuss security breaches like an employee getting compromised by a memory stick left in the parking lot being attached to a workplace computer[9]. Sheppard stipulates that cyber hygiene is a mentality, that hygiene extends to an organisations supply chain and a lack of adequate hygiene will restrict the organisations ability to

[7] "'No more away game': Former Cyber Command official says Russia and China have leveled the playing field," updated September 20, 2019, accessed September 24, 2019, https://www.cyberscoop.com/brett-williams-cyber-command-no-more-away-games/.

[8] M. Angela Sasse Shari Lawrence Pfleeger, Adrian Furnham, "From Weakest Link to Security Hero: Transforming Staff Security Behaviour," *Homeland Security & Emergency Management* 11, no. 4 (2014), https://doi.org/10.1515, http://discovery.ucl.ac.uk/1460572/2/jhsem-2014-0035.pdf. p 496.

[9] "The "Oceans 11" of Cyber Strikes," Brookings Institute, 2012, accessed October 2, 2019, https://www.brookings.edu/articles/the-oceans-11-of-cyber-strikes/

respond[10]. These definitions will prove useful in constructing a cogent cyber hygiene programme for Australia.

Conclusion and recommendations

A useful starting point for establishing conduct habits among a workforce would be comparisons to other industries like mining. Inductions onto minesites are mandatory for every worker wishing to set foot anywhere in the workplace, they are required to be updated regularly, and workers must prove that they understand specific instructions to the site about how they will conduct themselves at work. This includes understanding various types of warning labels, general rules such as never walking under suspended loads, obvious rules that need reinforcing like no talking on a phone whilst driving. The purpose of these inductions and other workshops that workers have to go through is that there is a firm base of knowledge amongst all workers that start with "the obvious". Once this is established, inductions can then move on to site specific issues that workers may encounter, how they *must* act in these interactions, etc.

The Australian government should seriously consider taking these standards of practice and insisting on their application in the workplaces not only of the government but of the private sector also. When workers are hired, they must be inducted into the cyber domain and how they must use their computer at the workplace. These inductions must be repeated. A base standard for how all workplaces should be inducted would be an exceptionally helpful document for businesses across all spectrums and sizes. This is especially useful for mitigating unsophisticated cyber attacks like phishing attacks which frankly, are far too effective this far into the 21st century. Clicking on suspicious links in emails is an activity that individuals should do on their personal computers (if at all), most certainly not workplace computers. A small business could still be something like a start up legal firm. This means that confidential data is entrusted to the company. The individuals working there should be inducted in at least the basic code of conduct for adequate cyber hygiene to develop resiliency against attacks as menial as phishing attacks. It would be a poor reason for the data on a clients sensitive case being compromised as someone "fell asleep at their email" and opened something they should not have.

To mitigate the costs of these inductions that small businesses especially would have, a base induction template could be a useful tool distributed by ACSC or Dept. of Home Affairs. This could be accessed directly by either entity, or distributed as a package to say, banks. As the primary distributors of loans, the

[10] Ben Sheppard, Mary Crannell, and Jeff Moulton, "Cyber first aid: Proactive risk management and decision-making," *Environment Systems and Decisions* 33 (12/01 2013), https://doi.org/10.1007/s10669-013-9474-1.

banks could insist to their new clients that they engage this cyber domain induction package as an essential part of opening their business. This package could also be distributed widely to pre-existing companies. What's more, with pre-existing such strategies already existing the information contained within would be useful for creating such an induction presentation.

Another difficulty with this induction process is engagement. It is all well and good to propose such strategies for mitigating cyber attacks but without engagement from public and private sector, they are meaningless. Here the government has many options, but my recommendation is litigation. Litigating cyber hygiene much the same as safe workplaces are legislated is forceful, direct, and insists on speed in engaging these cyber strategies. Minesites must be complaint with Worksafe practices the entirety of their existence, and with good reason. People can be severely injured if not outright killed in their line of work. Whilst the cyber domain isn't threatening people's lives, it does affect their livelihoods. Cyber Worksafe is not an unreasonable pathway for the government to take, establishing ranges of punishment mechanisms to not only non-compliant businesses but also non-compliant individuals. Individuals that repeatedly have offences such as serial phishing attack victim will at first obviously need extensive training to mitigate their habit, if not outright punishments tied to their incapability to remain vigilant on a workplace computer. This system already exists in Worksafe practices – individuals who are routinely unsafe can find themselves out of a job if it's serious enough. Litigating a Worksafe practice in the Australian business sector not only enforces a higher minimum standard amongst the Australian workforce but also, provides businesses with legitimate strategies for dealing with individuals who constantly fall victim to cyber-attacks.

These submissions are of course not intended as a silver bullet to resolving cyber security issues in Australia however, it is my submission that significant gains would be made in improving the cyber defences by drastically increasing cyber hygiene. It would diminish vulnerability amongst individuals and make a significant contribution to deterrence by denial mechanisms, something underappreciated in cyber deterrence strategy so far.

Bibliography

"Countermeasure: Hack the Hacker?" Security Week, Updated September 4, 2019, accessed October 1, 2019, https://www.securityweek.com/countermeasure-hack-hacker.

"Cyber Hygiene 101: Implementing Basics Can Go a Long Way." SecurityWeek, Updated August 7, 2019, accessed October 1, 2019, https://www.securityweek.com/cyber-hygiene-101-implementing-basics-can-go-long-way.

"Securing a Connected Future: 5g and Iot Security " SecurityWeek, 2019, accessed October 1, 2019, https://www.securityweek.com/securing-connected-future-5g-and-iot-security.

Hanson, Fergus, "Australia's Cyber Strategy, 2.0 ". *Australian Strategic Policy Institute*, September 18, 2019, https://www.aspistrategist.org.au/australias-cyber-strategy-version-2-0/.

"'No More Away Game': Former Cyber Command Official Says Russia and China Have Leveled the Playing Field." Updated September 20, 2019, accessed September 24, 2019, https://www.cyberscoop.com/brett-williams-cyber-command-no-more-away-games/.

Shari Lawrence Pfleeger, M. Angela Sasse, Adrian Furnham. "From Weakest Link to Security Hero: Transforming Staff Security Behaviour." *Homeland Security & Emergency Management* 11, no. 4 (2014): 489-510. https://doi.org/10.1515. http://discovery.ucl.ac.uk/1460572/2/jhsem-2014-0035.pdf.

Sheppard, Ben, Mary Crannell, and Jeff Moulton. "Cyber First Aid: Proactive Risk Management and Decision-Making." *Environment Systems and Decisions* 33 (12/01 2013). https://doi.org/10.1007/s10669-013-9474-1.

"The "Oceans 11" of Cyber Strikes." Brookings Institute, 2012, accessed October 2, 2019, https://www.brookings.edu/articles/the-oceans-11-of-cyber-strikes/

Slayton, Rebecca. "What Is the Cyber Offense-Defense Balance?". *International Security* 41, no. 3 (2017): 72-109. https://doi.org/10.1162/ISEC_a_00267.