Australia's 2020 Cyber Security Strategy

This response to *Australias 2020 Cyber Security Strategy*[1] [2] is a personal critique by Ian Falconer.[1] This paper provides crititque of current capabilities and provides suggestions for capabliity enhancement. This paper focusses on describing and categorizing the problem space and challenges and does not provide any product recommendations.

This document includes the following content:

- Executive summary
- SWOT[2] analysis of Australia's capabilities in tackling cyber security related things
- An influence diagram[3] that highlights the circular and interconnefted dependencies of the cyber security problem space
- A PESTEL[4] [3] narrative providing context, challenges and options
- Bibliography of key references and evidence to support this review
- Disclaimer and Bio

This review does not provide specific product recommendations, vendor specific messaging or other 'project or product' information. Others will, I'm sure, 'boil that ocean'. This review considers Australia's cyber security as a wicked problem [4] and uses Sterman's complex systems methodology to 'connect the dots' of the broader wicked problem space. [5]

Executive Summary

Australia faces innumerable challenges in being able to exploit, manage and protect against cyber security events. The ongoing 'arms race' of protection and attack is not new. There are opportunities and risks on offer if the government is brave enough to move from 20th century centralized control and 'walled garden' thinking. Much of the media, industry and government thinking around cyber security, and technology more broadly, is generally of very poor quality, not based on sound technical principles and continues to frustrate and alarm Australians. Especially those of us who understand the problem space, enabling technologies and failure modes. The status quo is stuck in the 20th century, acts as if proven digital solutions are witchcraft and refuses to acknowledge their knowledge gaps.

Legislation such as the Access and Other Legislation [6] highlights the incompetence and lack of system thinking by decision makers. The use of the word 'Other'[sic] in the title of this legislation suggests the authors could not even come up with a proper title. Self proclaimed media experts talk of a 'centralized database' and draconian violation of individuals' rights as things to implement.[7] This demonstrates Australia's obsolete thinking in this space. Command and control is a poor strategy in this age of digital assymetry.

Government needs to sideline the lobbyists, partisan politics and hysterical media and implement a decentralized cyber security capability that allows individuals to protect their personal data, implement technologies based on suitability, not lobbying, and eliminate the covert exploitation of individuals' data by entitites not acting in the individuals' best interest. Individuals should own their identity, not the government. Government should advocate for individuals before organizations and vested interests.

Government also needs to think big and equip agencies tasked with protection of Australians' with the tools, information, processes and resources to be effective. Intelligence agencies need broad surveillance capabilities, enforcement agencies need targeted capabilities for evidence gathering and the judiciary needs to be able to and be seen to punish those who violate an individual's trust. There needs to be independent oversight of all agencies by non partisan entities.

[1] https://www.linkedin.com/in/leftbrainstuff/

[2] Strength, Weakness, Opportunities and Threat analysis

[3] Visual network or cyclic graph that contains hierarchical and circular relationships that helps visualize complex wicked problem spaces

[4] Categorization of problems using Political, Economic, Security, Technical, Environmental (the domain and not the 'green' environment) and Legal

SWOT

The SWOT[8] summarizes the strengths, weaknesses, opportunities and threats that Australia faces in implementing a cyber security strategy. Key insights of the SWOT include:

- It's great to see that the Australian Government has conducted reviews of ASX 100 businesses but what has changed? The completion of a review is not a milestone that delvers a benefit. What changes have implemented and how have Australian's benefited?
- One highlight is the trust Australian's seem to have in our court system. Although our Judiciary is ill equipped to understand digital technologies in light of the less than impressive Australian legislation.
- Australia's under performance in the 'D' in R&D is woeful. Research without Development provides very little benefit for Australia. Other nations have benefited from our investment in Research and failure to exploit said research for the benefit of the country. The loss our our automotive industry. CSIRO's loss of Intellectual Property around Wifi are just two examples. Our mining industry sees us export 'gravel' and add almost no value to our exports.
- The negative influence of lobbying needs to be addressed. Government should look to protect and provide a benefit for Australian's first.
- If Australia fails to address our weaknesses then external forces will negatively influence our standard of living, our economy and our lives. 'Do Nothing' is not an option.

swot-analysis-dutton-cybersecurity-review

ifal | October 30, 2019

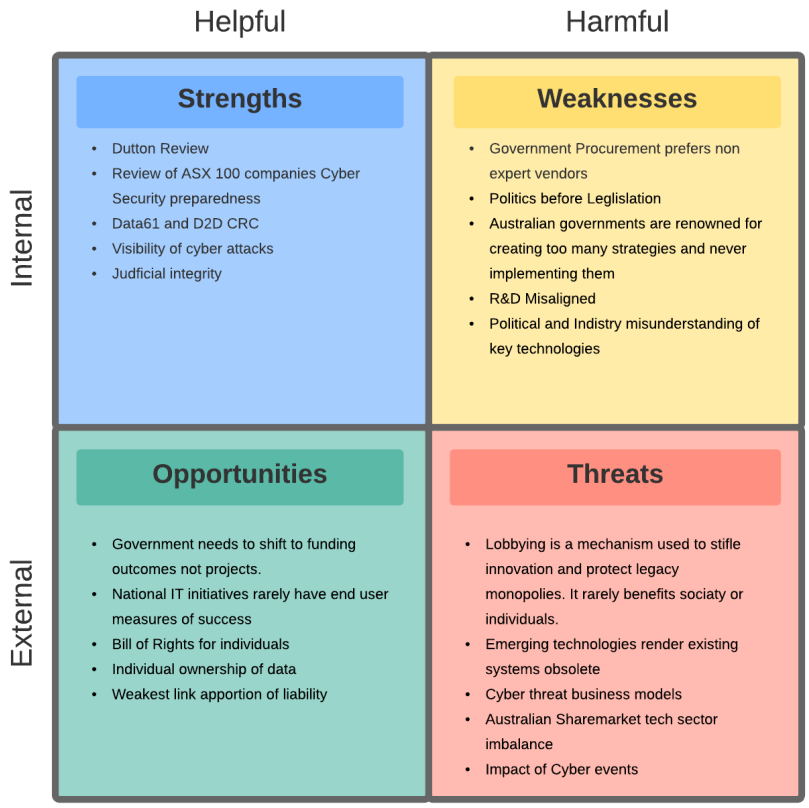

Figure 1: SWOT

Cyber Security as a Wicked Problem

A word search of Australia's 2020 Cyber Security Strategy - Discussion Paper for keywords 'wicked' and 'problem' results in zero and three results respectively. It's extremely concerning that we (The Minister for Cyber Security and more broadly the Australian Federal Government) don't seem to grasp the scope of the complexity of the wider cyber security and digital space.

The following influence diagram[9] depicts reinforcing and moderating loops of the broader cyber security wicked problem. This visualization of the wicked problem space is not a fully formed DAG[5] , Bayesian network or solvable model. But this diagram provides a useful mental model for visualization of the problem space.

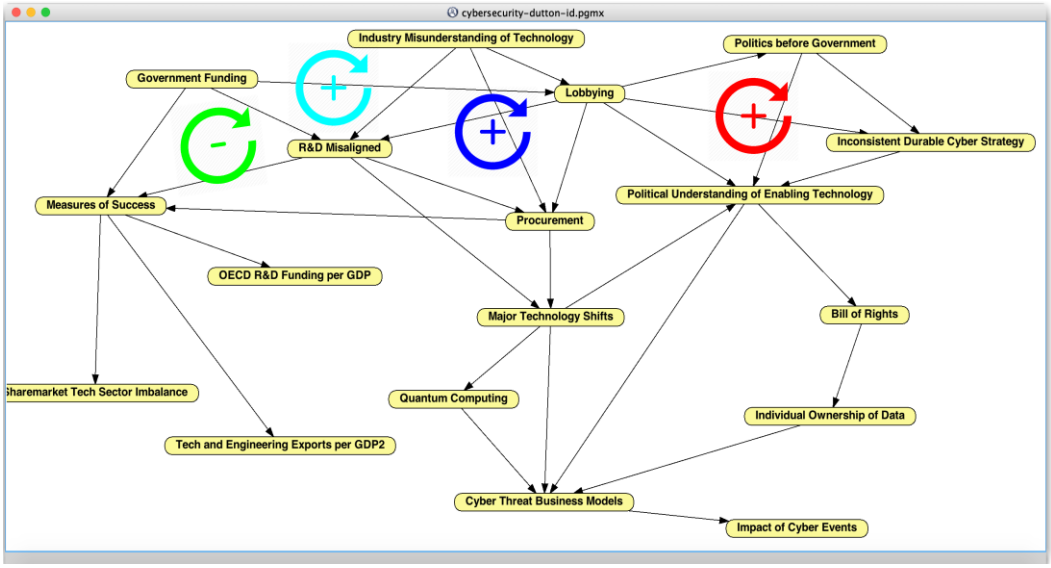

Figure 2: Cyber Security Influence Diagram

The coloured loops indicating negative and positive reinforcement loops is substantially dominated by lobbying which results in poor decision making, vendor lockin and ultimately poor outcomes. Examples including NBN, National Electrical Grid, Murray Darling Water Basin to name a few. This is a systemic problem which needs to be addressed if Government expects to create and implement a durable cyber strategy that is good for Australian and Australians.

Table 1: Key Influences

Colour	Influence	PESTEL Mapping	Comments
Green	Negative	Politics	Lack of RandD Measures of Success
Cyan	Reinforcing	Environmental	Lobbying negatively influences government decisions on RandD
Blue	Reinforcing	Economics	Lobbying directly influences procurement and creates lockin
Red	Reinforcing	Politics	Lobbying negatively influences politics and politicians

[5]Directed Acyclic Graph

PESTEL

A PESTEL[3] analysis is a method to categorize problem spaces. Issues relate to risks and opportunities that Australia can control or influence. Each issue is also labeled in terms of it's SWOT relationship.

- Strength [S]
- Weakness [W]
- Opportunity [O]
- Threat [T]

Political

Understanding of Technologies [W] Australian governments have little to no understanding of the relevant technologies and rely on outdated, biased and deceptive advice from commercially outsourced advisors.

Emerging Technologies [O] Quantum computing will render most current cryptography obsolete. Government needs to think ahead. Agencies like CSIRO, DSD, etc need to be ahead of the game.

Who Controls Technology? [T] New technology disruption is now a norm. Government needs to be responsive. The days of government controlling technology and innovation are long gone.

Unleashing Innovation [WT] Innovation will not come from old thinking, old guard vendors and lobbying. Innovation is a key enabler to improve society, improve productivity and respond to threats. Fast track approvals of fintech startups, post Royal Commission is an example of government enabling innovation and allowing the market to break unnecessary monopolies like the 4 bank pillar.

Government Procurement Inertia [WT] Government needs to manage a staged and multi year strategy of legislative reform, procurement reform, awareness and technology implementation and not try to just outsource to legacy tech and consulting vendors who have poor track records

Marketing Spin versus Solving Problems [WT] Government needs to be seen as helping Australian businesses and its citizens in defending against, recovering from and obtaining legal satisfaction after the fact. The current government entities like the cyber security center only seem to comment after events. This is the proverbial shutting the gate after the horse has bolted. (Detective and responsive security is needed.) Bragging that Australia is 5th in the world in cyber security expertise while Australians are subjected to high levels of attacks is missing the point. This is not about being the best while Rome burns. Stop self congratulation and focus on fighting the war instead. (Refer to issue with management and leaders who lack competencies in this topic)

Cybersecurity as a capability [O] Government needs to include cybersecurity principles, minimum standards, etc into all government decision making, systems and organizations. (Refs MOST in China and reference SADI paper)

Economic

Projects are not Strategies [W] Invest for R&D not projects. There are claims in the 2020 Cyber Security Strategy Discussion Paper of 'establish academic centres of cyber security excellence in universities'[sic] but no mention of engaging with industry leaders. Academia is a laggard in the implementation of new technologies.[10] Cyber security best practice is evident in the the tech sector.[11] Without engagement with industry leaders Australia is at significant risk of exploitation by malicious actors.

Cybersecurity Measures of Success [OW] Measures of success? What have CREST achieved? Follow up and penalties for the health checks for ASX100 listed businesses

Budgets don't Correlate with Capabilities [W] Government driven strategy needs to be outcome focused and not just a budget line item. Legislate for outcomes broader and longer than just the political election, restructure time line. Dont fiddle while Rome burns

Social

Automation and Heuristics [O] Individuals (aka human in the loop) validation is required to ensure digital records retain their provenance. Centralized records management thinking is rendered obsolete, insecure and readily exploited. [12] (Ref Amazon heuristic and algorithmic security)

Cybersecurity Awareness [OW] Awareness of an individuals responsibilities, how to use, etc to be managed through a slip, slop, slap type campaign. All demographics need to be included. Make movies (like the secret), run hackathons and public try encryption. The public must be included in this journey. Government needs to be open and inclusive and not the current closed and devisive.

Individual Ownership of Personal Data [WO] All agencies and requests for an individuals data must be to the individuals metadata and not to agency, entity, organization 'owned' data. Zero trust transactions.

0.0.1 Technical

Failure of Technology Projects [W] If AWS can support a Mexican election digitally with 80M voters then Australia can electronically vote.

New Cyber Security Technologies [OT] Commercially available merkle tree technologies (aka blockchain style immutable records) can support citizen controlled identities.

Traditional Security Models are Broken [WT] Walled garden security model is obsolete. There are many technologies now available to support a robust, modern, digital and enduring cybersecurity environment.

Cyber Security Transactions[WO] Secrets management and sharing is fragile. Think new technologies like SQRL[13] and other trust no one authentication and authorization methods.

Deprecate Failed Technologies and Processes [OWT] Obsolete technologies which must be phased out include credit cards, walled garden security model, monolithic applications, Insecure and frequently hacked centralized data stores. Identity verification in many sectors is obsolete. Posting paper personally identifiable information (PII) data to insecure mailboxes, phone validation, etc are very insecure.

Digital Identity [OWT] Australian cannot expect to be secure in a digital world without having an ability to manage idempotent and trusted identities for individuals, entities and decisions. Australia card and std metadata model are two options.

Environmental

Risk Ignorance [W] Risk avoidance culture endemic across Australian federal, state and local governments and across most business sectors results in poor decision making

Research AND Development [SWOT] Australia invests in research but falls short in development.[14]

Unintelligent Processes and Thinking [WT] Simplistic and monopolistic procurement, recruitment avoidance of new thinking and and knowledge hoarding processes mean that new ideas, learning from others and innovation is stifled. Government and business need to clean out middle level management and senior management who lack competencies in digital things, security and usage. Its not just about training people (ref D2D CRC)

Many resisters to the status quo use new technologies as causes for existing problems. Law enforcement, the judiciary and many decision makers will need to change their thinking. Government can and should enable change by replacing the Luddites.

Legal

Individual Rights [OT] Bill of rights for individuals which enshrines personal ownership of data is needed

Penalties for the Weakest Links [OW] US President Obama's weakest link to suffer most penalties, censorship and pain when breaches occur is needed. Full provenance of transactions against an individual's merkle tree.

Exploitation of an Individuals' Data [O] Those who benefit financially from any transaction against an individual's metadata (a supposedly trusted entity) must be able to prove their innocence. This requires a shift from enforcement having to prove guilt. This is unobtainable in the digital age. Penalties and restitution can then be automated.

Data Access Governance [S] Law enforcement must have a court issued subpoena for privacy invasion. Intel agencies need blanket surveillance approval. If intelligence or law enforcement violate an individuals right then penalties need to be severe, visible and a deterrent. Individuals under an active investigation or with criminal history or connections should be treated differently

Whistleblower Protections [OW] Whistle blower protection for exposing security vulnerabilities in a process that alerts cybersecurity center. A time limit is set for the whistleblower to go public. Official recognition of whistle blower civic responsibility but no financial incentives or motivations allowed.

Bibliography

[1] AustralianGovernment, "Australias 2020 cyber security strategy," 2019.

[2] AustralianGovernment, "Australias 2020 cyber security strategy - a call for views," 2019.

[3] wikipedia, "Pestel," 2019.

[4] wikipedia, "Wicked problem," 2019.

[5] J. Sterman, *System Dynamics Modeling*, 2001.

[6] AustralianGovernment, "Telecommunications and other legislation amendment (assistance and access) bill 2018," 2018.

[7] P. Credlin, "Podcast - sky news credlin," 24Oct2019.

[8] wikipedia, "swot analysis," 2019.

[9] wikipedia, "Influence diagram," 2019.

[10] M. Shoebridge, "Lessons from the anu cyberattack aspi," 2019.

[11] AmazonWebServices, "Aws security web portal," 2019.

[12] nuid, "Trust is risk.," 2019.

[13] S. Gibson, "Secure quick reliable login," 2019.

[14] OECD, "Oecd statistics on gdp and research," 2018.

[heading=none]

Bio

Ian Falconer[6] has more than 30 years of digital, security, engineering, big data and R&D experience. This review is based on my first hand experience working with, observing and solving problems for organizations including Amazon Web Services, Australia's Chief of Army, BAE Systems, DaimlerChrysler, NASA, US DOJ, Banks, Airlines, BHP Billiton Uranium, Twitter, Yahoo, Expedia, GE, Honeywell, Mitsubishi, MBDA to name a few.

Disclaimer

This review is solely based on the opinions of Ian Falconer[7] and do not represent and are not endorsed by my current[8] or any former employer.

[6] https://www.linkedin.com/in/leftbrainstuff/

[7] Ian Falconer BEng Mech, GradDip Military Systems Integration, MEngSc Materials Welding and Joining

[8] Ian Falconer has been employed by Amazon Web Services in the United States since 2014