Submission on Cyber Security Strategy 2020

The views and comments below are expressed by several academics of Cyber Security Hub at Macquarie University, namely:

A/Prof Christophe Doche, Executive Director of the Cyber Security Hub
Dr John Selby from Macquarie Business School
A/Prof Niloufer Selvadurai from Macquarie Law School
A/Prof Tiffany Jones from the Department of Educational Studies

1) What is your view of the cyber threat environment?

From Dr John Selby

What threats should Government be focusing on?

Cyber threats should be treated as an ecosystem risk for our society. Government should facilitate the private sector in its capability development and assist with threat discovery, threat awareness, education, funding research and harm mitigation, as well as resolving collective action problems and fix market failures relating to cyber security and privacy.

Governments should be particularly focusing on nation-state actors and organised crime threats to:

- Defence capabilities
- Critical infrastructure (including election systems)
- Industrial espionage and supply chain risks
- Financial fraud and interference with business operations (such as ransomware and business email compromise)
- Identity theft

An open question is whether it is more appropriate to include aspects of information warfare, such as fake news, within the national cyber security strategy or to develop a separate (but aligned) national information warfare strategy which is focused on the spread of mis-information online. Arguments can be made on both sides of this debate.

From A/Prof Tiffany Jones

There is scope for Government to support the doing of more on social media and media dominations which further Australia's vulnerabilities to propaganda memes and false narratives, spreading disinformation and division. There is scope for the Government to do more on educating and restricting politicians around using transnational election propaganda meme aid from countries who support their own interests, not the candidates'. Perhaps this is about requiring certain inductions on these matters, government funded but externally prepared.

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

From Dr John Selby

There are four major groups in Australia who are responsible for managing cyber risks: 1) government departments and agencies; 2) private sector businesses and not-for profits; 3) individuals; and 4) insurers. The extent to which particular risks should be managed by each of these four groups is a political and social choice, not just a matter of technical capabilities.

Government Capabilities

Governments at all levels in Australia need to ensure that their own capabilities are adequately in order against cyber risks, including their own supply chains. This is particularly relevant in the context of the Federal Government's Data Sharing Program and cuts to public service agencies (such as the recent $250m+ cut to the NSW health department) which may undermine investment in building cyber-maturity capabilities within heavily targeted sectors. In an environment where short-term operational capabilities are threatened by budget cuts, medium- to long-term investments in building cyber security capabilities are likely to be de-prioritised in practice.

Cyber-Attribution Challenges

The challenging issue of attribution of cyber-attacks to groups or nation-states risks creating a tension between government and private sector interests, and market failure in the cyber-insurance market. Attribution is known to be a hard problem – especially when cyber-attackers are deliberately using attack tools from other nation-states to cover their tracks (see the recent NSA advisory report of the Russian Turla group deliberately using Iranian cyber-attack tools to mis-direct its victims). Whilst the Australian government (along with several other governments) has made specific attributions for attacks like NotPetya, it is unclear whether the Australian government thought through all of the unintended consequences of such acts of attribution. In particular, it is unclear whether the risk to both the private and public sectors that the risk mitigation and transfer (via insurance) strategies they have made in the past may be undermined by later cyber-attribution was fully considered.

Australian companies typically assess their cyber-risks and decide how much of that risk they wish to tolerate or mitigate through: 1) spending on internal projects and policies and 2) buying products and services from suppliers. The residual level of risk they face is typically transferred through purchase of insurance policies (or self-insurance).

The risk of unintended harm by government acts of attribution is evidenced by the denial of insurance coverage by insurers for hundreds of millions of dollars of NotPetya-related losses suffered by companies such as Mondelez International (owners of Tasmania's Cadbury factory) and Maersk (a major global shipping and logistics company). Those insurance claims were denied on the basis of "Acts of War" and "Acts of Terrorism" exclusions within the company's insurance policies and are now the subject of major litigation in the USA.

Many of the major cyber-insurance policies (and general insurance policies) sold in Australia currently have exclusions for either or both Acts of War and Acts of Terrorism. Although some insurance companies may choose to pay claims that they could deny coverage on the basis of such exclusions, this does not provide adequate protection for Australian businesses because those businesses lack certainty as to whether their policies will actually deliver the risk transfer they expect, or whether those risks might end up unexpectedly re-appearing on their balance sheets. This is particularly a challenge for Australian businesses because although an insurance company might elect to honour a series of relatively small claims, it is in the moments of greatest risk to the survival of their businesses (i.e. when they need to recover hundreds of millions of dollars of losses from a crippling cyber-attack) that the insurance companies are more likely to deny coverage (as experienced by Mondelez International and Maersk). Faced with such uncertainty over the effectiveness of their residual risk-transfer strategies, Australian companies may be compelled to over-spend on cyber security mitigation rather than to rely upon (what could be) a more efficient cyber-insurance market.

From A/Prof Tiffany Jones

There is a lack of recognition of the harm that can come from the allowing the privileging of the interests of multi-national media corporations, over local accurate news disseminations; and allowing the privileging of the interests of dominating social media bodies, over the citizens they 'sell' as advertising viewers to foreign entities.

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

From Dr John Selby

Cyber-security risks are a mixture of supply-side challenges and demand-side challenges. Effective and efficient allocation of rights and liabilities on both the supply-side and demand-side is essential to reducing the volume of risks posed to Australians.

Supply-Side Challenges and Possible Solutions:

The current ability of businesses to exclude or limit liability for cyber risks through contracts has resulted in them having reduced incentives to reduce "pollution" into the cyber ecosystem. Infant industry arguments are no longer valid bases to permit excluding liability for harm in the context of the world's most valuable companies now being technology companies.

Many of the efforts of government and business to clean up the mess in our cyber ecosystem are squandered if suppliers of risks are not sufficiently incentivised to reduce the number of vulnerabilities in their products *before* releasing those products into the Australian market.

We can learn from the solutions used to reduce exposure of Australians to other types of risk. By excluding them from the marketplace and by placing liability on manufacturers, importers and retailers, consumer-protection and product safety laws have worked effectively to reduce the risks of electrocution, burns and poisoning from unsafe products.

Even the United States of America is moving down this path. The state of California has passed an IoT Security Law which comes into effect on 1 January 2020. It requires that all connected devices sold in the state of California – no matter where they are made – to incorporate "reasonable security features" that appropriately protect the user of the product and the user's data from unauthorised access, modification or disclosure and bans hard-coded passwords. The US federal parliament is debating an Internet of Things Cybersecurity Improvement Act which (if passed) would require the NIST to create IoT security regulations that would be mandatory for all IoT devices used by government agencies.

The Australian government could explore introducing similar laws and using its buying power to encourage the private sector to reduce the cyber-vulnerability of IoT devices sold and used in Australia. It would be wiser to introduce such laws sooner rather than later – especially as IoT devices are expected to become more widespread after the 5G network rollout which is currently underway.

Demand-Side Challenges and Possible Solutions:

If no one ever wants to exploit a vulnerability to harm an Australian individual, a business or government agency, then the existence of that vulnerability doesn't really matter.

Whilst improving the security quality of hardware devices, software code and networks (supply-side challenges) is essential, understanding who wants to attack us and why they want to attack us is even more important than knowing how they are (or could be) attacking us. These demand-side issues are not areas where IT departments (and IT researchers) typically have skills. Attackers' identities and motivations relate to global politics, global events, cultural differences, historical vendettas, crime, corruption, overcoming technology deficits, poverty, institutional weaknesses, etc.

To better understand and respond to these demand-side challenges, there is a pressing need to bring the insights of the humanities, social sciences, human sciences, and business schools into debates around cyber security policy, strategy and tactics.

From A/Prof Tiffany Jones

There needs to be restrictions on media and social media dominations. Market diversification, not renaming of X company as Y. Separate owners. Again, arms-length hands-off funding of ABC is going to be crucial in handling disinformation attacks – it already is.

4) **What role should government play in addressing the most serious threats to institutions and businesses located in Australia?**

From Dr John Selby

The Australian government should help build capability and awareness in institutions and businesses and hold them liable if they are underprepared – raise the bar of what is considered acceptable in the ecosystem. Whilst governments have been known to hide some of their knowledge of cutting-edge exploits to build a stockpile of cyber-attack capabilities, governments have to balance the extent to which they build their arsenal versus helping to share knowledge of potential attack vectors with Australian institutions and businesses.

Helping Australian institutions and businesses to more rapidly respond to cyber-attacks (particularly financial losses) is critical. This will require the expansion of operational cyber-attack investigation capabilities within law enforcement agencies.

Whether the Australian government should deploy offensive cyber-capabilities to "hack back" against serious threats to Australian institutions and businesses is a question worthy of further research and policy debate.

From A/Prof Niloufer Selvadurai

As has been widely noted [1], the present cyber security legislative framework was developed prior to the rise of the internet as a dominant trading and communications space. The design of present laws also predates the rise of transnational malicious cyber activity that crosses national jurisdictional borders [2]. These developments require Government to design new laws and reimagine existing laws to impose greater legal responsibilities on private entities that obtain a monetary benefit from cyber transactions. Specifically, this include the development of a regulatory framework for the sharing of data and a certificate system for online services. Additionally, to increase the effectiveness of transnational cyber security initiatives, it is important that cyber crime laws be harmonised across the Asia-Pacific region in a similar way to that which has been achieved in the Europe Union [3].

The *2016 Australian Cyber Security Strategy* proposed the creation of a new cyber data sharing network to support partnerships and collaborations between business, government and the academic community to strengthen cyber security [5]. As noted in the Discussion Paper, Data61 has implemented a cyber security strategy that has included supporting secure data sharing [6]. While this initiative is highly valuable, it is suggested that it would be of greater effect if it formed a legislated model for cyber security information sharing, similar to that which was introduced in the USA through the *Cybersecurity Information Act*, 2015 (CISA). The CISA does not compel but rather incentivises data sharing by private entities by extending a variety of liability protections to private entities who share threat and risk information with other private entities or government. Such a legislated framework for data sharing would facilitate cyber security collaboration between Government and private entities in Australia and also support more transparent and accountable information sharing. Such a legislated model would also have the benefit of enabling legal sanctions to be imposed for non-compliance with the regulatory sharing framework, such as where personal information has been shared without complying with de-identification requirements or where there has been inappropriate disclosure to third parties.

Further, it is submitted that the Australian Government should consider the adoption of a certification system for online services. In 2018, the powers of the European Network and Information Security Agency (ENASA) was substantially extended to include oversight of a new cybersecurity labelling system for the certification of online services and consumer devices. Such a system has the potential to both incentivise private entities to invest in effective data security measures and also enhance user understanding of the cyber risks and promote responsible online behaviour.

To support such domestic initiatives, it would also be valuable to further harmonise cyber crime laws and enforcement procedures across the Asia-Pacific region as present inconsistencies in laws substantially hinder cross-border legal enforcement [7]. In this regard, one useful initiative is the creation of transnational academic working parties to identify inconsistencies in laws and move beyond broad-brush policy statements to designing concrete and specific legal reforms that can be enacted to fulfil obligations in the Council of Europe Convention on Cybercrime [8] and harmonise laws in the region. Such working parties have been effectively used in the European harmonisation process [9].

From A/Prof Tiffany Jones

Its focus should not be entirely there; the obsession with business and financial losses misses obvious threats which are geopolitical/ on political process sovereignty… – first and foremost Government must look to protect democracy and its processes, with restrictions on parties and politicians using external aid in cyber campaigns. Having inherent interests in powers, the Government needs to recognise the need for arms-length parties to take the helm on this issue but with their financial (hands-off) support.

5) How can government maintain trust from the Australian community when using its cyber security capabilities?

From Dr John Selby

Coordination and consistency in policy and practice, plus setting expectations appropriately are critical for maintaining trust.

Infringing on Australians' privacy is destructive of trust – e.g. the e-Health opt-out process and the Telecommunications Assistance and Access Act reducing foreign businesses' trust in Australian cyber-security export-oriented businesses. The data sharing agenda arguably increases the risk profile and may be destructive of trust if there is insufficient coordination between that strategy and the national cyber security strategy.

Government needs to protect its own systems better – its breaches severely damage trust in its judgment and competence. The recent breaches of Victorian hospitals and universities (such as ANU) indicate an under-investment by public sector agencies in their cyber-maturity and privacy-maturity in practice.

If government agencies infiltrate privacy sector or individuals systems without adequate permissions and safeguards, this is also destructive of trust.

As mentioned earlier, current consumer and privacy laws are inadequate to deal with the cyber security threats facing the nation. The government should look at the extent to which insurers can exclude or limit liability for cyber risks and be careful before engaging in cyber-attribution as that is being used by insurers to deny coverage in some situations.

Improving cyber hygiene in the ecosystem is critical. We don't permit the sale of devices to plug into the wall in Australia unless they are certified as being safe. Yet we permit the sale of IoT devices in Australia which lack even baseline cyber security capabilities. This is a consumer protection issue which needs to be addressed in the same way that we took steps to add a regulatory burden to reduce the rate at which houses burned down due to electrical fires. At the 2019 iappANZ Privacy Conference in Sydney, the NZ Privacy Commissioner, John Edwards, recently questioned whether software and IoT suppliers should owe a "duty of care" to their customers.

Different arms of government may be working at cross-purposes. There is a need for greater coordination across the Cyber Security Strategy with the ACCC's Digital Platforms Inquiry policy development process, with the government's Data Sharing Policy, and with other government policies under development.

From A/Prof Tiffany Jones

Providing one-off funding allocations and supports to arms-length, hands off bodies of other experts.

6) What customer protections should apply to the security of cyber goods and services?

From Dr John Selby

Improve the ecosystem by setting baselines: no ability to exclude liability; don't allow the import or sale of IoT products into Australia without adequate basic cyber hygiene capabilities built in. Impose liability for manufacturers, importers and retailers for harms if these requirements are ignored or violated.

7) What role can Government and industry play in supporting the cyber security of consumers?

From Dr John Selby

Education about best practices – an endless task, but critically important.

Give recommendations of options for best-of-breed Australian cybersecurity products and services for small and medium businesses to lower their information asymmetry and transaction costs which undermine their ability to rapidly improve their (often woeful) cyber-maturity. This would improve the efficiency of cyber security purchasing decision-making, stimulate domestic demand for cyber security goods and services, generate economies of scale for Australian cyber-security suppliers, and improve the maturity and health of the Australian cyber-ecosystem.

From A/Prof Niloufer Selvadurai

It is useful to consider issues 6 and 7 together.

Australia has comprehensive and effective consumer laws to protect consumers from misleading or deceptive representations [10] and ensure that services supplied to consumers are fit for purpose [11]. These provisions could potentially be relied upon by the Australian Competition and Consumer Commission to prosecute businesses for cyber security incidents that lead to the suffering of harm by consumers. Section 18 of the Australian Consumer Law could, for example, be used where a business makes a misleading representation as to the security of a particular online trading site and a consumer suffers economic loss as a consequence of relying on that representation. To date, these consumer laws have not been used for the purpose of supporting cyber security in the online space. However, it is conceivable that these laws could effectively be applied for this purpose. The broad technology-neutral drafting of the above provisions makes them particularly well-suited to governing fluid technologies. Hence, the issue is not one of the absence of relevant consumer laws but rather one of appropriate enforcement of existing laws to the new and evolving field of cyber goods and services.

8) How can government and industry sensibly increase the security, quality and effectiveness of cyber security and digital offerings?

From A/Prof Christophe Doche

As noted by Bruce Schneier in an article published by the NY Times in 2018, a fundamental shift is taking place because of the emergence of connected devices, which have the ability to interact with the physical world. So far, the consequences of a cyberattack, as devastating as they may be are mostly about losing data. In a very near future people will lose their life as a result of a cyberattack. That is going to force Government and regulators around the world to act a lot more forcefully on the matter.

At the moment, something as simple as a fluff toy or hairdryer must go through a series of tests to make sure they meet minimal standards of safety before they can enter the market.

There is no safety standard, no testing procedure regarding the hardware or the software of a smart fridge or of a car. Yet, we have seen some examples of hacking the firmware or the WIFI network a car with potentially deadly consequences.

There is a place for Government to create regulations and incentives to develop a completely new testing industry of IoT devices. Australia could even play a leading role worldwide both in the regulatory and technical space, as no other nation seems to have made much progress on this issue.

From Dr John Selby

Set minimum cyber requirements for products / services being sold into the Australian market. Prohibit businesses from denying liability for the cyber harms and real-world that they cause.

9) Are there functions the Government currently performs that could be safely devolved to the private sector? What would the effects be?

From Dr John Selby

The incentives of the private sector do not align with the public sector. The private sector will do what is profitable, but much of the work required to improve the hygiene of the cyber ecosystem is likely to be more expensive than profitable. There are significant coordination and collective action problems to be overcome which necessitate government involvement.

There are also dangers that private sector entities do not necessarily remain loyal to national interests in any particular country, particularly after buyouts. The Takeovers Review Panel and Foreign Ownership Panel need to include cyber risks in their assessments of takeovers and foreign ownership.

10) Is the regulatory environment for cyber security appropriate? Why or why not?

From Dr John Selby

No… quite a few examples:

Takeovers, foreign ownership, product liability, data sharing, privacy, corporations law, etc all need updating to deal with cyber security issues.

From A/Prof Tiffany Jones

Inadequate restriction on media and social media giants.

11) What specific market incentives or regulatory changes should Government consider?

From A/Prof Christophe Doche

Government didn't lift safety on our roads by tackling the entire problem all by themselves. Government mandated that every driver should have at least compulsory third-party insurance and let insurance companies implement policies that would enhance the safety of the cars and the skills of the drivers. Cyber security issues are vastly different from what we encounter regarding road safety, however mandating some form of cyber insurance for businesses could be a way forward to raise cyber security standards in each company individually and increase trust between them. Such a bold move would also contribute to strengthen a promising new sector in Australia with very real prospects to expand globally.

From Dr John Selby

ACCC consumer protection laws – remove the ability to exclude liability (both in B2B and B2C) for harms caused by inadequate cyber security.

Be careful of attribution by government because of the consequences for cyber insurance.

12) What needs to be done so that cyber security is 'built in' to digital goods and services?

From Dr John Selby

The cyber-equivalent of the 'tick' that an electronic good requires before it can be sold in Australia. Prohibition on the exclusion by suppliers of liability for inadequate cyber security.

13) How can we approach instilling better trust in ICT supply chains?

From Dr John Selby

Cascading maturity models, standard contracting & tender requirements for local to federal governments; requirements for cybersecurity by design and privacy by design

14) How can Australian governments and private entities build a market of high quality cyber security professionals in Australia?

From A/Prof Christophe Doche

In the following, we focus on one small segment but often forgotten and essential to the development of a strong and innovative ecosystem in cyber security, i.e. applied research. Innovation tends to blossom at the intersection of academia and Industry, when applied researchers collaborate with practitioners on interesting problems. Secondments (both ways) are an option to facilitate exchanges between academia and Industry but that is not always an easy solution to scale.

Another option, that is far easier to scale and that has shown success in other countries is to embed research students, essentially PhD students, in an organisation, working on an industry topic, under the joint supervision of an academic and an industry expert. Let us call this an ***Industry PhD***. The funding model is usually to split the investment between Academia, Industry and Government (usually through tax cuts). The number of benefits of Industry PhDs are multiple.

a) Through this scheme, companies get access to deep expertise in a given field, for a relatively modest investment and have the ability to train and develop someone who most likely will remain employed after the end of the project. They also get indirect access to even deeper expertise materialised by the academic supervisor.
b) Students and academic supervisors are fed with interesting real-life issues and can use from the data generated by the project to support more theoretical research.
c) The multiple sources of funding allow for a higher stipend, which now becomes attractive to our most talented students.

For the record, the current and normal stipend for a PhD student is about $26,000 per year. No wonder that our best and brightest students, who just graduated are not too keen to pursue a career in research, especially when they studied in a field like cyber security where companies are dying to attract talents.

Note that this idea, even in Australia is not new. The APR scheme is essentially a cut-down version of an Industry PhD. There are also other schemes providing placements at different stages during a PhD. What is suggested is a national framework providing a beefed-up version of the existing schemes, where the research project is jointly crafted from the start by an academic and an industry expert, and where a student with the suitable skills and knowledge is recruited for three years to work at the company on that given project.

From Dr John Selby

Increase funding for universities / tafe courses and courses relating to cyber-security (not just in the Science faculties), reduce the HECS fees for Cyber courses (particularly for female students to increase their participation in this area); increase funding for interdisciplinary cybersecurity research projects; coordinate the areas of specialisation between particular tafes and universities to address the cyber-skills gap.

From Assoc/Prof Tiffany Jones

Invest in university researchers in the field so they can research and teach to key problems.

15) Are there any barriers currently preventing the growth of the cyber insurance market in Australia? If so, how can they be addressed?

From Dr John Selby

Unintended Consequences of Cyber-Attribution:

The challenging issue of attribution of cyber-attacks to groups or nation-states risks creating a tension between government and private sector interests, and market failure in the cyber-insurance market. Whilst the Australian government (along with a number of other governments) has made specific attributions for attacks like NotPetya, it is unclear whether the Australian government thought through all of the unintended consequences of such acts of attribution. In particular, it is unclear whether the risk to both the private and public sectors that the risk mitigation and transfer (via insurance) strategies they have made in the past may be undermined by later cyber-attribution was fully considered.

Australian companies typically assess their cyber-risks and decide how much of that risk they wish to tolerate or mitigate through: 1) spending on internal projects and policies and 2) buying products and services from suppliers. The residual level of risk they face is typically transferred through purchase of insurance policies (or self-insurance).

The risk of unintended harm by government acts of attribution is evidenced by the denial of insurance coverage by insurers for hundreds of millions of dollars of NotPetya-related losses suffered by companies such as Mondelez International (owners of Tasmania’s Cadbury factory) and Maersk (a major global shipping and logistics company). Those insurance claims were denied on the basis of “Acts of War” and “Acts of Terrorism” exclusions within the company’s insurance policies and are now the subject of major litigation in the USA.

Many of the major cyber-insurance policies (and general insurance policies) sold in Australia currently have exclusions for either or both Acts of War and Acts of Terrorism. Although some insurance companies may choose to pay claims that they could deny coverage on the basis of such exclusions, this does not provide adequate protection for Australian businesses because those businesses lack certainty as to whether their policies will actually deliver the risk transfer they expect, or whether those risks might end up unexpectedly re-appearing on their balance sheets. This is particularly a challenge for Australian businesses because although an insurance company might elect to honour a series of relatively small claims, it is in the moments of greatest risk to the survival of their businesses (i.e. when they need to recover hundreds of millions of dollars of losses from a crippling cyber-attack) that the insurance companies are more likely to deny coverage (as experienced by Mondelez International and Maersk). Faced with such uncertainty over the effectiveness of their residual risk-transfer strategies, Australian companies may be compelled to over-spend on cyb er security mitigation rather than to rely upon (what could be) a more efficient cyber-insurance market.

Access to evidence-base for actuaries and actuary academics:

Efficient pricing of cyber-insurance policies is currently very difficult. This results in higher than necessary cyber-insurance premiums for Australian businesses, lower than optimal claim limits, wider than necessary exclusions and limited carve-backs in policy wordings.

One of the major contributing factors to this inefficiency in cyber-insurance policies is the immaturity of the actuarial models which are used to price such insurance. In comparison to other insurance sectors, cyber-insurance models suffer from a lack of access to rich historical datasets of losses, and to information about the cyber-maturity capabilities of the individuals / businesses / government agencies prior to them suffering those losses. Collection of such information by government and making it available for study by both actuarial academics and practicing actuaries would improve the efficiency of the Australian cyber-insurance market, potentially lowering premiums for Australians. Providing funding for scholarly research to improve those actuarial models of cyber-risks would also deliver benefits to Australians.

Engaging with the Cyber-Re-Insurance industry:

Insurance companies selling cyber-insurance policies into the Australian market are constrained in their decision-making by the choices made in the re-insurance market. Inconsistency in the language in policies between insurers, the use of legacy language in insurance policies which is unsuited to cyber-risks, and a lack of sufficient training for insurance brokers all undermine the efficiency of the cyber-insurance market in Australia.

The re-insurance industry is already working to address some of these issues. To the extent possible, the Australian government should consider working with domestic insurance companies to engage with the re-insurance industry at the international level so that the efficiency of the cyber-insurance market in Australia is maximised.

Encouraging cyber-insurers to offer discounts to policy holders who demonstrate improved cyber-maturity and privacy-maturity

Whilst insurance policies are a post-hoc solution to cyber-attacks (i.e. they only pay-out after a breach which causes loss has occurred), encouraging insurers to offer discounts on cyber-insurance policy premiums to Australian policy holders who have demonstrated improvements in their cyber-maturity and privacy-maturity could deliver a number of benefits.

First, it would improve the Australian cyber-ecosystem by encouraging individuals, businesses and government agencies to make efficient up-front investments that reduce their exposure to cyber-attacks. Second, it could encourage spending by policy holders on Australian cyber security goods and services. This could stimulate macro-level demand for those Australian businesses, enabling them to invest further into research-and-development, lower the costs of their products, hire more employees, and potentially become market leaders in the region.

16) How can high-volume, low-sophistication malicious activity targeting Australia be reduced?

From Dr John Selby

Only by improving the maturity of the entire Australian cyber-ecosystem. This would make Australia a less-desirable target for such attacks.

17) What changes can Government make to create a hostile environment for malicious cyber actors?

From Dr John Selby

Work to improve the maturity of the entire Australian cyber-ecosystem.

From A/Prof Tiffany Jones

The most effective tools the Australian Government has in combatting transnational cyberwar and election interference via propaganda meme attacks is 1) internally requiring politicians take oaths not to support or work in coalition with these attacks/ attackers so this is not an ‘unstated’ problem and then outlining and following through on clear measures against those who do; 2) moving towards sanctions on interfering nations in coalition with a large collection of allies (not alone – it needs to be systematic; key countries to work with include France given the recent Paris Call [11] and others in the EU, Brazil, New Zealand etc); 3) working directly with social media on which the most Australians are located such as Facebook (60%) and Instagram, and Twitter, to restrict harms. On the latter there needs to be Ministerial Advisory Committees as this will be complex work requiring research, legal and social media experts.

20) What funding models should Government explore for any additional protections provided to the community?

From A/Prof Tiffany Jones

Where this pertains to combatting transnational propaganda memes, expert actions should be taken and funding needs to be supplied upfront, hands-off and at arms-length (to ensure trust in Government, as propaganda tends to be political) – as argued by Nimmo and Laity [12]. Some funding needs to be marked for interdisciplinary, educational, sociological and psychological interventions when it comes to social media attacks. Traditional cyber security work is business focused and hacking focused; research should involve other disciplines too.

21) What are the constraints to information sharing between Government and industry on cyber threats and vulnerabilities?

From A/Prof Tiffany Jones

A similarly important question is: to what extent will information sharing between Government and researchers aid progress? Researchers need more access to transnational propaganda memes uncovered by government sources for their analyses to be effective; particularly publicly viewed material. The discussion paper stated the Department of Defence established an Information Warfare Division – are there ways various types of researchers can apply for access to banks of identified propaganda artefacts to analyse? This would be key to providing feedback and expertise on their features, strategies and so forth with reference to a wide range of literature and lenses.

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

From A/Prof Tiffany Jones

A useful example of how sharing of raw data from propaganda meme attacks in the US was done well is the House of Representatives' hosted database [13]: https://intelligence.house.gov/social-media-content/social-media-advertisements.htm

This has everything researchers need to perform analyses effectively.

As to other practices, I'll get back to you if I get funding on this, it's a research question I share, on propaganda memes.

26) Is there anything else that Government should consider in developing Australia's 2020 Cyber Security Strategy?

From A/Prof Tiffany Jones

Australia's Cyber Security Strategy [14] discusses the problem of online propaganda in only a very limited way. 'Propaganda' is used in relation to terrorism and radicalisation of terrorists – which may be one application, but is not by any means its limit. Since the release of the strategy it is clearer than ever before that the internet – including media and especially social media – is being used by foreign government agencies to spread propaganda memes and narratives in highly systematic ways, whose effects are not immediately apparent or detectable to the groups of citizen viewers targeted. We posit these attacks, which are subtle, geopolitical in nature and sometimes very well-funded, are of urgent threat to democracies and need to at least be a ‘topic for further investigation and attention’, as well as ‘further research support and collaborative strategising’.

A case in point includes, famously, the Russian Internet Research Agency’s use of Facebook, Instagram and Twitter propaganda memes in as a tool for influence in the 2016 US election – part of broader campaigns of influence across Europe and other regions [15,16]. Research by OPTUS Macquarie University Cyber Security Hub member Associate Professor Tiffany Jones highlighted that the Russian IRA campaign used such strategies as double-use of (both ‘pro’ and ‘anti’) lesbian, gay, bisexual, transgender (LGBT) education; immigration and ethnic grouping messaging in propaganda memes towards impacting division, real-world group confrontations, elections, democratic processes, and the US’s geopolitical positioning [17].

Part of what makes the US attacks hard to guard against is the false belief by certain politicians that election interferences ‘aids their side’; and not ‘the other side’ – playing into the idea that one is more aligned to foreign influencers than one’s nation and its plurality of citizens. This is the core trick of such propaganda meme attacks; they actually seem to aid ‘both sides’ of a debate; ‘both sides’ feel supported and helped… where in reality such memes serve to inflame them both against each-other (inciting progressive vs. conservative divisions) and moreover, incite both groups against the targeted governments and the nations democratic systems.

There is evidence of similar systematic intervention in other contexts including Australia and New Zealand warranting investigations [18-20]. Sometimes there can be a mistaken sense that this problem is too widespread, complex, political and difficult to deal with. But there are many options of response without resorting to extremes of overkill (shutting social media down altogether) or neglect (not acting). In turning humans - and most especially marginal social groups – from the weakest link in the cyber security equation to the first line of defence, there needs to be efforts at:

- Researching divisive and tribalizing social propaganda meme campaigns;

- Researching direct and indirect election interference;

- Educating politicians who are vulnerable to working in coalition with transnational agencies seeking to interfere (and imaging they can ‘use’ such ‘help’) that such agencies are not ‘on their side’ but acting against our national interests and ‘for’ foreign parties’ interests;

- Educating the media on this threat and understanding the way media domination by a few key entities enhances the quick spread of external propaganda memes and disinformation narratives once penetrating, through cross-publication circularity and a lack of news fact-checking and diversification;

- Educating the public with consideration of European efforts at citizen education models in the area of disinformation – perhaps most famously the Swedish pamphlet distributions [21] but there may be more contextually appropriate options here;

- Thinking deeply and responsibly about how political and media efforts at demonising marginal groups (perhaps for clickbait or to attract certain voter groups) plays into and increases the likelihood of this particular type of socially driven cyberwar attack. Demonisation of minorities – particularly LGBTs, ethnic minorities, immigrants, Indigenous people and also religious conservatives – creates an already most fertile ground upon which the seeds of propaganda memes and false media narratives can further feign false divisions, dismays, despairs and distractions as suits external and malicious interests.

- Holding social media and media leadership to greater account to provide editing and protections against transnational interference and restricting their monopolisation of key information and social markets in Australia.

References

1. Gillespie, A. Cybercrime: Key issues and debates. (2019). Routledge, at pp. 15-16.

2. Menthe, D.C, "Jurisdiction in cyberspace: A theory of international spaces" (1998) 4(1) Michigan Telecommunications and Technology Law Review 69. Available at https://repository.law.umich.edu/mttlr/vol4 /iss1/3; and Svantesson, D.J.B, "Geo-location Technologies and Other Means of Placing Borders on the 'Borderless' Internet," (2004) 23(1) John Marshall Journal of Computer & Information Law 101-139. Available at http://repository.jmls.edu/jitpl/vol23/iss1/3

3. Verbruggen, P and Wolters, P, Hildebrandt, M, Sieburgh, C and Jansen, C, "Towards harmonised duties of care and diligence in cybersecurity," 11 May 2016, Cyber Security Council, pp. 78-107. Available at http://dx.doi.org/10.2139/ssrn.2814101

4. Australian Government, Australia's Cyber Security Strategy - Enabling Innovation, Growth and Prosperity, 21 April 2016. Available at https://cybersecuritystrategy.homeaffairs.gov.au/AssetLibrary/dist/assets/images/PMC-Cyber-Strategy.pdf

5. Australian Government, Australia's 2020 Cyber Security Strategy - A Call for Views, 2019 at p.30.

6. Mittal, I.P.S, and Sharma, P, "A review of international legal framework to combat cybercrime," 2017 8(5) International Journal of Advanced Research in Computer Science 1372-1374. Available at http://dx.doi.org/10.2139/ssrn.2978744

7. Council of Europe Convention on Cybercrime, ETS No. 185, Signed 23 November 2001, effective 1 July 2004.

8. Lasaballett, E.S, "Conceptualizing harmonization: The case for contract law," (2019) 24 Uniform Law Review 73-120 at p. 81. Available at http://dx.doi:10.1093/ulr/unz007

9. Competition and Consumer Act 2010 (Cth), Schedule 2, (Australian Consumer Law), s 18.

10. Competition and Consumer Act 2010 (Cth), Schedule 2, s 61.

11. France Diplomatie. Paris Call for Trust and Security in Cyberspace2018 24.11.18. Available from: https://www.diplomatie.gouv.fr/IMG/pdf/paris_call_text_-_en_cle06f918.pdf.

12. Jackson L. The Three Warfares - China's New Way of War. In: Pomerantsev P, editor. Information at War: From China’s Three Warfares to NATO’s Narratives. London: Legatum Institute; 2015. p. 5-15.

13. US House of Representatives Democrats Permanent Selection Committee on Intelligence. Social Media Advertisements. 12.5.18 ed. Washington: US House of Representatives Democrats Permanent Selection Committee on Intelligence; 2018.

14. Australian Government. Cyber Security Strategy. Canberra: Commonwealth of Australia; 2016.

15. Mueller RS. Report on the Investigation into Russian Interference in the 2016 Presidential Election. Washington: US Department of Justice, 2019.

16. Mueller RS. Internet Research Agency Indictment in the US District Court for the District of Columbia [Case 1:18-cr-00032-DLF]2018 1.1.19. Available from: https://www.justice.gov/file/1035477/download.

17. Jones T. Double-use of LGBT youth in propaganda. LGBT Youth,. 2019:1-24. Epub 4.10.19. doi: 10.1080/19361653.2019.1670121.

18. Tomazin F, Zhuang Y. Safe Schools scare campaign targets Chinese-Australian voters. Sydney Morning Herald, [Internet]. 2019 27.4.19. Available from: https://www.smh.com.au/federal-election-2019/safe-schools-scare-campaign-targets-chinese-australian-voters-20190427-p51hrk.html

19. Cannane S, Hui E. Federal election 2019: Anti-Labor scare campaign targets Chinese-Australians. ABC Investigations. 2019. Epub 3.5.19.

20. Brady A-M. Magic Weapons: China's political influence activities under Xi Jinping. Washington: Wilson Centre; 2017.

21. Swedish Civil Contingencies Agency. If crisis or war comes: Important information for the population of Sweden. Karlstad: Swedish Civil Contingencies Agency; 2018.