Strengthening Australia's Cyber Security Regulations and Incentives

Samuel Murison, *DPhil Candidate,*
Institute for Science, Innovation and Society,
University of Oxford

Michelle Howie, *Curator, Global Shapers Adelaide Hub,*
Graduate of Electronics and Communications Engineering (Honors)
from University of South Australia

Public submission

August 27, 2021

Jeff Bleich Centre
for the US Alliance
in Digital Technology,
Security & Governance

Flinders
UNIVERSITY

CONTENTS

BACKGROUND

We provide this submission as winners of The Alliance: Next Generation policy pitch competition, hosted by the Jeff Bleich Centre for the US Alliance in Digital Technology, Security and Governance at Flinders University, South Australia in February 2021.

As young leaders in our respective fields of engineering, government, law, international relations, and accounting we were asked to design a policy that would strengthen the digital resilience of Australia and our international allies. Being digital natives, we share growing concerns that the shrinking cost and increasing availability of consumer Internet of Things devices was unknowingly adding exponential vulnerability points to Australia's cyber ecosystem.

With the US being a world leader in big-tech and one of our strongest allies, a weak link in our IoT chain could be a threat to their security. From this realisation, our multidisciplinary team independently devised a policy for empowering consumers to make informed decisions when purchasing Internet of Things devices by introducing a 5-star rating system for cyber vulnerability.

We thank the Department of Home Affairs for the opportunity to participate in South Australia's public consultation event on the 18th of August 2021 and for consideration of our submission. We are grateful to the Jeff Bleich Centre at Flinders University for their generous assistance in preparing this submission, and to our team including Adi Rai, Sophie Kerr, Nicholas Davis, and Ashley Ramachandran for their thoughtful suggestions and comments on this submission.

KEY POINTS

There is a strategic imperative to re-orientate cyber security policies towards greater understanding of human experiences of the cyber domain and of the social implications of emerging smart device technologies.

Regulations and incentives should aim to have the ability to adapt to a rapidly evolving technological and social landscape without stifling innovation and economic prosperity.

Cyber security policies should be fully integrated and coordinated with broader strategic objectives at both local and global levels.

APPROACH

Strengthening Australia's cyber security regulations and incentives is a commendable and timely strategic initiative of Australia's Cyber Security Strategy 2020. The vision outlined in Australia's Cyber Security Strategy 2020 is positive and encouraging, particularly the acknowledgement that a range of system-wide actions are required across governments, businesses and community.

This submission, whilst wholly supportive of the motivation that underpins these initiatives, aims to provide some suggestions for gently reframing some of the focus to ensure that cyber security policies are aligned in the most effective way with Australia's strategic interests, directly from the next generation of leaders who will be living the benefits, and the risks, for the coming decades.

In particular, this submission highlights that regulations and incentives a) can be improved through more thorough consideration of social implications of emerging technologies; and b) should be complemented with a suite of policies that aim to build stronger societies that are more resilient to the cyber ecosystem.

The backdrop of a deteriorating global cyber security threat environment on the one hand, and an increasingly complex cyber ecosystem on the other, where it is becoming more difficult to determine what is secure and what is not, present unique challenges for Australian policymakers. Global trends warn us that the emerging paradigm of virtually ubiquitous connectivity, through for example the Internet of Things, brings with it a new set of quite fundamental vulnerabilities and severe, even catastrophic risks to democratic societies.[1]

Policies to improve cyber security should also be fully integrated with broader efforts to improve resilience by building and mobilizing a range of local and global strategies, as opposed to isolated, disjointed initiatives. Significantly, there is an opportunity for these policies to contribute to building a cyber resilient society over the longer term.

In the Australian context, it is worth remembering that part of the objective of these policies is to change the way in which Australians think about and interact with technology. To that end, another question that is important to fully consider in the design of these policies is that of the kind of society that we are aiming to produce.

This submission therefore advocates for a more holistic, human-centred approach to cyber security policy design, implementation and feedback.

---

1 U.S. National Intelligence Council 2021, 'Global Trends 2040: A More Contested World'.

RESPONSE to Paper Questions

CHAPTER 6: Standards for smart devices

Question 11:

What is the best approach to strengthening the cyber security of smart devices in Australia? Why?

Australia should take a holistic approach to strengthening the cyber security of smart devices. The Internet of Things is a connected web, where a vulnerability in one link of the chain exposes the entire network. Although our generation is more environmentally conscious than ever, people still generally prioritise convenience and cost over other factors, especially cyber-security which in most cases for consumers seems to be low risk and high effort to consider.

It is not a stretch to imagine some buying habits (e.g. of cheap international knock-off Ray Ban glasses) becoming a cyber risk when smart watches, coffee machines and other smart devices enter Aussie homes. Consider Australia's migrant and aging populations, who may not have the means to purchase US or Korean made premium consumer smart devices or have the knowledge to consider the implications of their personal purchase on the vulnerability of our connected web of devices.

Consumer devices and enterprise devices are no longer distinct, with even CEOs and publics servants working from home amongst connected water meters and light bulbs. As digital natives, we bring our cyber literacy (or lack of) into our various work and professional lives. Empowering the consumer to protect their digital world has never been so important.

Australia should not undertake this in isolation. We would like to see the silos of regional policies mentioned in this paper[2] lead to the establishment of a more coordinated range of global standards, agreements and norms in the cyber domain.

The best place to expand this coordination effort is with our alliances and partners. The Joint Cybersecurity Advisory between the US, UK and Australia is a worthwhile step in the right direction, however there appears to be an opportunity for further collaboration and coordinated policymaking in the cyber domain across all Five Eyes partners.

Further, it might be worth considering leaning-in to our ANZUS alliance by expanding "Article II cooperation to strengthen our democracies, build resilience, improve technological competitiveness and provide guardrails to improve certainty during rapid change in the environment."[3] We could also consider updating the 2007 Defence Trade Cooperation Treaty with respect to what could be construed as strategic goods and defence articles.

---

[2] The discussion paper makes it clear that in the last year alone, we have seen, for example, a range of cyber security policies and regulations in the U.K, an Executive Order on Improving the Nation's Cybersecurity in the U.S., and voluntary labelling schemes for smart devices in Singapore and Finland based on the international standard ETSI EN 303 645.

[3] Seebeck, L 2021, 'Cyberspace and ANZUS', in Walters, P (ed.), ANZUS at 70: The past, present and future of the alliance, Australian Strategic Policy Institute, pp. 143-145.

Question 15:

Is a standard for smart devices likely to have unintended consequences on the Australian market? Are they different from the international data presented in this paper?

We can foresee several unintended social and entrepreneurial risks.

RISK 1: Widening the digital divide and exposing those who are less well off or who have not had the same opportunities to develop awareness of cyber risks. We can assume that more expensive consumer IoT device manufacturers can afford to comply with labelling and standards, but cheaper devices might retain vulnerabilities. Complying to the standards should not be cost-prohibitive or time-prohibitive for manufacturers, retailers and wholesalers. This cost should not flow on to the consumer, at the risk of widening the digital divide and giving safety only to those who can afford it.

RISK 2: Stifling local innovation. If complying to standards are mandatory, this would reduce the agility and speed of bringing new innovations to market. However, considering the potential for societal damage from a "move fast and break things" mantra, slowing down may be the sacrifice we should take. Policymakers should provide signposts for responsible behaviour whilst being careful to avoid disincentivising innovation for companies that might enter the market.

RISK 3: Limited device imports. The paper recognises the risk to limiting device availability of international manufacturers that cannot comply with our standards, however we think it is a much greater risk than stated in the discussion paper.[4] If Australia attempts to enforce these standards in isolation, our international suppliers have little incentive to comply, and we miss out on the newest, more efficient and cost-effective options.

RISK 4: Misleading cyber-safety-washing marketing. We caution the misinformation that marketing efforts could employ in order to make their smart devices seem more cyber-safe than they actually are, taking advantage of any labelling scheme.

Consider a similar approach to the 'green marketing' guidance issued by the ACCC in response to product environmental claims and the introduction of the energy and water efficiency labelling scheme to protect consumers from this risk.[5] Similar issues have been found in the health star rating scheme, or the use of "no added sugar" leading consumers to believe that some carbonated drinks are as healthy as water when they might not be.

True cyber safety requires constant vigilance and a balanced ecosystem that doesn't rely on any quick fix. It is much more holistic than a star rating. We must factor in human error, social engineering, and over-reliance on any one vendor. For example, if the Australian Defence Force allowed only 5/5 rated devices for smart watches and phones, which resulted in everyone ending up with iPhones and Garmin watches, this could create a systemic vulnerability to any cyber breaches of those two vendors.

---

[4] As stated on page 36 of the discission paper, "A mandatory standard may result in reduced product availability...for consumers…Industry feedback and analysis by the UK indicated that reductions in product choice from a basic standard or increases in costs for consumers are likely to be low."

[5] Australian Competition and Consumer Commission 2011, 'Green Marketing and the Australian Consumer Law'.

RISK 5: Consumer complacency. Potential for misinformation on the difference between cyber-attacks and the legal (but unsavoury) use of your personal information can lead to consumer complacency. Just because Apple products may be more resilient from cyber-attacks doesn't mean that your data will not be used for targeted ads. Just because your device is rated 5/5 stars for cyber security doesn't mean you are protected from phishing scams if you still click the links in your spam emails.

RISK 6: Over or under rating smart devices without context. The "safety" of something depends on the intended use, which should be taken into account when designing and assessing the rating. For example, a smart sports watch might be rated 5/5 stars for securing your running data but might not necessarily be recommended for payment systems.

RISK 7: Quickly becoming obsolete. This regulatory shift should aim to be agile in design, to have the ability to adapt to a rapidly evolving cyber threat landscape, and to be responsive to feedback from experts, consumers and industry.

CHAPTER 7: Labelling for smart devices

Question 16:

What is the best approach to encouraging consumers to purchase secure smart devices? Why?

Recommendation 1: Ensuring that the default option for consumers is to choose secure devices (i.e. by limiting major retailers to only sell above a certain rating, limiting the marketing scope for devices below a certain rating), to make it more difficult for consumers to purchase riskier options.

Recommendation 2: Demonstrating the benefit of secure devices, translating the risks into financial and personal loss (e.g. losing your photos, having to pay for replacement, losing your job, hurting your family).

RISK 1: Labelling could be misleading or misinterpreted by consumers. We don't want a situation for example where cyber security, safety and privacy are all conflated, implied or incorrectly interpreted from a rating that only assesses the security of the device itself. This could potentially erode trust in the policy. This risk could be met by a) aiming to ensure that the labelling is not open for misinterpretation; b) providing qualifying information or website links for additional detail; and c) determining how consumers understand the labelling over time and feeding this information back into updated labelling designs.

Although a somewhat simplistic and crude response to the complex cyber ecosystem, we believe that a smart device labelling system would indeed provide substantial benefits for governments, businesses and consumers.

Question 20:

Should a mandatory labelling scheme cover mobile phones, as well as other smart devices? Why or why not?

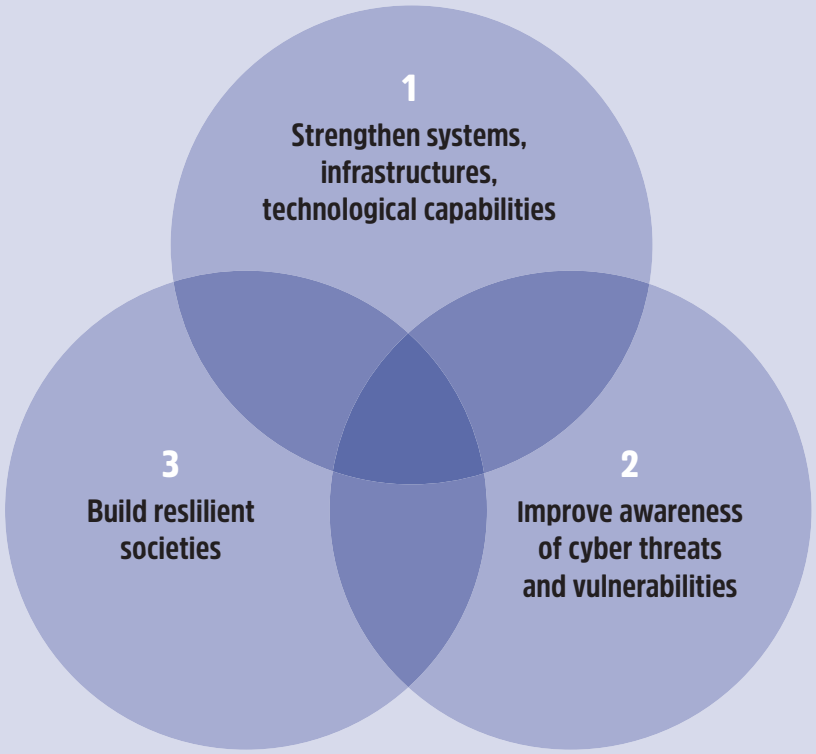
Yes, though more sophisticated standards might be required to account for the fact that mobile phones (and tablets, laptops, computers) are only as 'secure' as the apps downloaded onto them. We should be clear that the standard refers to only the hardware and operating system, but that each application that is downloaded has its own vulnerabilities to be considered. Given that all phones have different approaches to cyber security (e.g. frequency of firmware updates, requirements for screen locks and so on), and they are the most used device, leaving mobile phones out of a labelling scheme might entrench vulnerabilities and even undermine confidence in the scheme itself over time.

DISCUSSION

This submission aims to reposition policy options in the 'Strengthening Australia's cyber regulations and incentives' discussion paper as opportunities to build trust and resilience.

The objective of building a more secure digital economy has significant value in and of itself, however this framing naturally lends itself to technical answers to narrow policy problems that might unintentionally obscure more fundamental strategic opportunities to build resilient societies and to shape the way that everyday Australians think about and interact with technology.

FIGURE 1



Whilst the discussion paper and policy options tend to focus on (1) and (2), this submission aims to draw the attention of policymakers towards (3) as a third, overlapping domain of necessary policy action to build digital resilience.[6]

---

[6] A human-centred perspective of digital resilience would address a large gap in the literature, much of which is written from the perspective of technologists (see for example Boneh et al. 2020, 'Preparing for the Age of Deepfakes and Disinformation', Stanford University Institute on Human-Centred Artificial Intelligence).

We know that consumers can feel overwhelmed by the complexity and technical nature of the cyber ecosystem and will naturally question how these apparently distant and obscure cyber threats might have direct consequences for their day-to-day lives. Because it seems likely that humans will continue to be the weakest link in cyber security, it seems worthwhile to consider more thoroughly what a more human-centred cyber policy might look like.

Moreover, we should place significant value not only on whether a specific cyber policy achieves its narrow objectives but also on how these outcomes might fruitfully interact and intersect with broader strategies of building trust in our institutions and in our system of government. Trust considered in this way is a strategic resource that builds democratic resilience, which is important not only for the strength of our society but also for providing confidence for our allies and partners.[7]

Therefore, the building of trust should be prioritised, or at least given more prominent place whendeveloping cyber security policies.[8] A focus on building trust and resilience aims to make Australians a tough target in the same way that we should make Australian critical infrastructure and cyber systems a tough target.

One way to achieve this is through education. Israel's cyber education system offers a helpful exemplar to broaden and deepen Australia's cyber education for example through initiatives throughout schooling to encourage participation in cyber education and training, as well as a focus to connect teachers with the cyber industry for up-to-date training.[9] This education focus does not only provide future generations with greater cyber resilience but also fosters a pipeline for the future cyber security workforce.[10]

Considerable effort should therefore be directed towards the education of Australians in cyber literacy to ensure that Australians are more resilient to the rapidly evolving nature of the cyber ecosystem. The Cyber Security National Workforce Growth Program should be applauded however more work should be undertaken to broaden and deepen these sorts of resilience-building programs.

We should also sharpen our definition of cyber literacy. In the discussion paper, cyber literacy tends to focus on awareness campaigns and building technical capabilities. Both are important. However, we should also aim to provide Australians with the skills and abilities to approach digital interactions with care and context. Cyber security threats are part of this picture, to be sure, but misinformation, disinformation and other cognates should not be underestimated as significant and growing threats to Australian life.

---

7 Bienvenue, E, Rogers, Z & Troath, S 2018, 'Trust as a strategic resource for the defence of Australia'.

8 Rogers, Z 2020, 'The Strategic Implications of Manipulative Digital Platforms: A Trust-Driven Approach', National Security College Policy Options Paper, no. 15.

9 Stuparu, A 2020, 'Educational pathways to national cyber resilience: the Australian story', PhD Thesis, Australian National University.

10 Ibid.

Discussion *(continued)*

Dealing with these considerable challenges requires a holistic, multidisciplinary and coordinated approach across all education jurisdictions and sectors, and should be considered more thoroughly as a tool to build democratic resilience.[11] Cyber education in this sense moves beyond the technical to provide a foundation for resilience to the digital interface more generally.

Finally, further research is required to ensure robust policy design, smooth policy implementation and that value is fully realised from our cyber security policies. With reference to the option of labelling smart devices, for example, empirical research should be conducted alongside a pilot or staged rollout of the policy.

Research should feed into the policymaking process at all stages to ensure that policymakers can adapt to changing social understandings of cyber security, to sharpen understandings of the drivers of cyber safe behaviour, and to refine policies to maximise effectiveness over time.[12] Broader themes of trust and resilience should also be explored in this research into the social-cyber interface to ensure that we are building the kind of society that we want to live in, both now and into the future.

---

[11] Following Oceania Cyber Security Centre, 'Comments on the Discussion Paper: Australia's 2020 Cyber Security Strategy - A call for views', Submission 176.

[12] See for example Mazaar, M et al. 2019, 'The Emerging Risk of Virtual Societal Warfare: Social Manipulation in a Changing Information Environment', RAND Corporation.

Jeff Bleich Centre
for the US Alliance
in Digital Technology,
Security & Governance