School of Engineering

GPO Box 2476
Melbourne VIC 3001
Australia

City Campus
Tel. +61 3 9925 1872
www.rmit.edu.au

RMIT University

Department of Home Affairs
Australian Government

8 November 2019

To Whom It May Concern

Submission in response to the Discussion Paper Australia's 2020 Cyber Security Strategy

The opportunity to contribute to the development of the nation's next Cyber Security Strategy is welcomed. This submission responds to the questions in the Department of Home Affairs Discussion Paper Australia's 2020 Cyber Security Strategy.

Sincerely,

Mark A Gregory

BEng(Elec), MEng, PhD, FIEAust, SMIEEE

School of Engineering

GPO Box 2476
Melbourne VIC 3001
Australia

City Campus
Tel. +61 3 9925 1872
www.rmit.edu.au

RMIT University

Introduction

The response to the questions posed in the Discussion Paper Australia's 2020 Cyber Security Strategy [1] is focused on the underlying issues of trust, transparency, verification and credibility.

Australia's Cyber Security Strategy [2] provides the basis upon which the partnership between governments, the private sector and the community exists. The strategy states that:

> "The Australian Government will take a lead role and in partnership with others, promote action to protect our online security. Much of our digital infrastructure is owned by the private sector, so securing Australia's cyberspace must also be a shared responsibility. It will be important that businesses and the research community work with governments and other stakeholders to improve our cyber defences and create solutions to shared problems."

For the Australian Government to effectively "take a lead role" it is vital that the Government acts in concert with stakeholders, including State and Local governments, business, community groups and the research community, to improve cyber security, take action defensively and offensively and to implement solutions to cyber security related problems.

Over the past decade the Internet has evolved rapidly and, as anticipated [3], the threat environment has similarly evolved to the point where the Internet has become an electronic battlefield.

To manage the cybersecurity threat environment there is a need for governments to balance cybersecurity with privacy [4], defence with offence [3], and for a passive approach to cybersecurity to become active [5].

For Australians to become fully aware and participate willingly in cyber threat detection, prevention and response, there is a need for governments to engage openly, be transparent and to build trust and credibility.

Response to Call for views

Question 1. What is your view of the cyber threat environment? What threats should Government be focusing on?

I fully agree with the Government's assessment of the cyber threat environment.

Cyber criminals should be actively pursued through international agreements and brought to justice, even if this is limited to the confiscation of assets.

Nation states involved with illegal cyber threat activities should be identified openly and transparently. It is only when there is open and transparent release of information that stakeholders will be better informed and fully understand the threat posed by other nation states and their proxies.

The Government should take a wholistic view of threats, differentiate the threats and implement cooperation with governments, business, community groups and individuals to mitigate the threats.

School of Engineering

GPO Box 2476
Melbourne VIC 3001
Australia

City Campus
Tel. +61 3 9925 1872
www.rmit.edu.au

RMIT University

Question 4. What role should Government play in addressing the most serious threats to institutions and businesses located in Australia?

The efficacy of the Government's actions and role related to cyber threats should not be undermined, yet it is reasonable to argue that the actions by the Government related to telecommunications policy is duplicitous. This undermines trust and credibility.
The Government states that "much of our digital infrastructure is owned by the private sector, so securing Australia's cyberspace must also be a shared responsibility."

Offers by Huawei Australia to fund a telecommunications security assurance centre have been ignored [6].

This lack of openness, transparency and evidence related to telecommunications related cyber threat undermines trust that the Government is acting on behalf of Australians and not a foreign power.

Question 5. How can Government maintain trust from the Australian community when using its cyber security capabilities?

Trust, transparency, verification and credibility must be the fundamentals of the Government's approach to the mitigation of cyber threats and the deployment of cyber security capabilities.

Claims by the Australian Government related to cyber threats should be open, transparent and verified.

The Government faces a loss of trust and credibility when claims are not supported by evidence and verification.

The case of the Australian Government's effective ban on Huawei Australia from participation in the NBN and 5G (telecommunications) is worthy of comment on how this has affected the Government's credibility and trust by stakeholders in what the Government's use of cyber security capabilities.

On the one hand, the Australian Government has made a number of claims over the past seven years, a substantial period of time, that utilising Huawei Australia's telecommunications equipment and systems poses an unacceptable risk, based on evidence, yet evidence of a relatable transgression by Huawei has not been produced in Australia nor elsewhere.

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

The regulatory environment does not place sufficient burden on business to improve cybersecurity practices nor to participate in cyber threat mitigation activities.

For the past decade, I have advocated for a telecommunications security assurance and supply chain assurance capabilities [7][8][12]. The weakness in the cyber regulatory environment is the use of "self-regulation" and reporting as a mechanism to mitigate risk. There is no evidence that "self-regulation" related to cyber threat mitigation in the telecommunications industry will be anything other than a failure.

The Government's telecommunications sector security reforms that commenced on 18 September 2018 state [9]:

School of Engineering

GPO Box 2476
Melbourne VIC 3001
Australia

City Campus
Tel. +61 3 9925 1872
www.rmit.edu.au

RMIT University

> "All carriers, carriage service providers and carriage service intermediaries will be required to do their best to protect networks and facilities from unauthorised access and interference – including a requirement to maintain 'competent supervision' and 'effective control' over telecommunications networks and facilities owned or operated by them."

It is inconceivable that Government regulations related to national security rely on a "do their best" approach for industry involvement in the security of telecommunication networks. This is tantamount to absolving the telecommunications industry from any meaningful effort to implementing and improving cyber threat mitigation.

As mentioned earlier, Huawei Australia has offered to fund a telecommunications security assurance centre [6] for testing of Huawei equipment and systems, however, there is a need to test the equipment and systems supplied by all vendors to the Australian telecommunications carriers.

It is vital that a trust no-one and test, audit and verify everything approach be adopted for the Australian telecommunications industry.

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

For telecommunications, there is a need for a significant step forward in thinking about cyber security risk mitigation. Telecommunications carriers and service providers need to be encouraged through regulation and other incentives to setup a telecommunications security assurance centre. This will be a good first step towards securing current and future telecommunications networks and bring Australia into line with international efforts [10][11].

The telecommunications industry needs to do more to facilitate cyber risk mitigation, to meet consumer expectations and to match the Government's rhetoric on cyber threat risk mitigation.

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

You don't know what you don't know.

The Australian Government's approach to cyber threat mitigation must be to learn more about how technology is affecting our lives and how technology can be improved to reduce cyber threats.

If the Australian Government relies upon self-regulation as a mechanism for cyber threat risk mitigation and does not take the important step to take up the practice of security assurance then Australia will never gain the knowledge necessary to effectively combat cyber threats.

There is a cost associated with implementing cyber threat risk mitigation, and initially this cost will be high but we should expect it to reduce over time as more is learnt about cyber threat risk mitigation and goods and services are enhanced to have cyber security 'built in'.

Question 13. How could we approach instilling better trust in ICT supply chains?

Trust in supply chains is gained through testing, auditing and verification. As we become increasingly dependent on technology, security of the supply chain becomes more important.

School of Engineering

GPO Box 2476
Melbourne VIC 3001
Australia

City Campus
Tel. +61 3 9925 1872
www.rmit.edu.au

The Australian Signals Directorate's Australian Cyber Security Centre (ACSC) guide titled *Cyber Supply Chain Risk Management Practitioners guide* [13] fails to provide adequate guidance on how organisations should carry out testing, auditing and verification for goods, services and the supply chain.

The ACSC guide falls back on vague statements and requirements that match the current Government's approach to risk mitigation. For example:

> "**Know what makes a vendor high risk.** A high risk vendor is any vendor that by nature of the product or service they offer, has a significant influence over the security of your system. That vendor can be subject to adverse extrajudicial direction, or the vendor's poor cyber security posture means they are subject to adverse external interference. In both cases if not managed, the vendor can transfer unreasonable risk to your system."

Most countries, including Australia, have legislation that, in one way or another, requires companies operating in that country to assist in national security related matters. Australia has proposed and introduced laws that compel companies to decrypt messages, and other information and to make it an offence to make public a request to assist in national security matters and this apparently applies to journalists and whistleblowers [14].

Australia relies on trade, yet to most other countries and business originating outside Australia, would appear to now be a "high-risk" nation, and this may lead to a loss of trade opportunities.

From a supply chain perspective, Australian vendors providing goods and services globally may be considered "high risk" by the very nature of the national security legislation.

What this means is that the Government has implemented a duplicitous scenario, where every foreign based company should be considered "high risk" and other countries should consider Australian companies to be "high risk."

The only mechanism that reduces the escalation of nonsense legislation is for testing, auditing and verification in the supply chain. For the telecommunications industry this means that all vendor equipment should be subjected to testing and certification.

Question 18. How can governments and private entities better proactively identify and remediate cyber risks on essential private networks?

The best mechanism is for regulation that requires independent security assurance.

Infrastructure, goods and services in the supply chain and monitoring and reporting for operating networks.

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

Open, transparent and cooperative interaction between government and industry is necessary if cyber risk mitigation is to be successful. Certified practitioners that have an appropriate level of security clearance should be able to facilitate the information sharing between Government and industry.

Question 25. Would you like to see cyber security features prioritised in products and services?

School of Engineering

GPO Box 2476
Melbourne VIC 3001
Australia

City Campus
Tel. +61 3 9925 1872
www.rmit.edu.au

RMIT University

It is vital that the nation have a proactive and reasonable approach to cyber security prioritisation in products and services.

First, however, it is important to ensure that the underlying infrastructure, products and services are secure and there is a balance between security and privacy.

It is lazy and destructive if the Government, the security forces and the police adopt an approach to cyber security risk mitigation that goes too far and fundamentally alters the nature of our society. It is arguable that this has already occurred.

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

Honesty. Whilst this is a difficult concept for governments to grasp, there is a need to understand the effect that honesty has on trust and credibility.

The UK Science and Technology Select Committee published a letter to the Secretary of State for Digital, Culture, Media and Sport about Huawei's involvement in the UK's 5G network on 15 July 2019 [15]. In the letter the Rt Hon Norman Lamb MP, Chair of the Science and Technology Committee, said:

> "Following my Committee's recent evidence session, we have concluded that there are no technical grounds for excluding Huawei entirely from the UK's 5G or other telecommunications networks.
>
> "The benefits of 5G are clear and the removal of Huawei from the current or future networks could cause significant delays.
>
> "However, as outlined in the letter to the Secretary of State for Digital, Culture, Media and Sport, we feel there may well be geopolitical or ethical considerations that the Government need to take into account when deciding whether they should use Huawei's equipment.
>
> "The Government also needs to consider whether the use of Huawei's technology would jeopardise this country's ongoing co-operation with our major allies.
>
> "Moreover, Huawei has been accused of supplying equipment in Western China that could be enabling serious human rights abuses. The evidence we heard during our evidence session did little to assure us that this is not the case.
>
> "I hope the evidence we have gathered helps the Government as it completes its Telecoms Supply Chain Review, which must be published by the end of August 2019."

The head of Germany's foreign intelligence service Bruno Kahl recently told legislators [16] "that Huawei should not be allowed to play a significant role in building the country's 5G network, warning that the Chinese group could not be trusted."

However, the German government has opted to implement cyber security risk mitigation rules that would affect all vendors, including Huawei.

The weakness with the new German security criteria guidelines is a clause that allows vendors to self-certify products and services. This is similar to the Australian TSSR approach for carrier network certification and it is worthy of condemnation.

School of Engineering

GPO Box 2476
Melbourne VIC 3001
Australia

City Campus
Tel. +61 3 9925 1872
www.rmit.edu.au

RMIT University

The potential weakness in the German Government's approach is mitigated by the correct approach that is being taken. In future, it is possible that the German Government will implement independent verification similar to what is happening in the UK and Brussels through the new assurance centre in Bonn.

If the rationale for the Australian ban on Huawei is not technically related and was implemented for trade (in support of the U.S.) or other reasons then it is vital that the Australian Government be honest and provide the reasons.

Government ministers and senior members of the security establishments appear to have made false statements about 5G and why Huawei should be banned because there would be no edge or a "blurring of the edge" in 5G, which became, after the claims were challenged, "future 5G". To clarify the status of 5G standards related to the 5G edge a paper published in the Journal of Telecommunications and the Digital Economy provides clarity [17].

The lack of honesty, openness and transparency have damaged the Government's credibility and more importantly has damaged the credibility of the Australian security agencies. Whilst it is understood generally that Government's may opt for no credibility when political expediency is necessary, it is unacceptable for any reason that the Australian security agencies may be dragged into a political game.

A debate related to whether or not a foreign company should be banned is quite a separate issue that does not reflect on the need for honesty, trust and credibility related to cyber security.

The Minister for Home Affairs Peter Dutton states in the discussion paper that "Cyber security incidents have been estimated to cost Australian businesses up to $29 billion per year and cybercrime affected almost one in three Australian adults in 2018" [1].

The cost to business and the damage to the lives of Australians must be justification for the Government to commit to developing a telecommunications security assurance and supply chain security assurance capabilities.

References

[1] Department of Home Affairs, Australia's 2020 Cyber Security Strategy - A call for views, Australian Government, August 2019, Online: https://www.homeaffairs.gov.au/reports-and-publications/submissions-and-discussion-papers/cyber-security-strategy-2020

[2] Department of Home Affairs, Australia's Cyber Security Strategy, Australian Government, 2016, Online: https://cybersecuritystrategy.homeaffairs.gov.au/

[3] Gregory, M.A., Time for industry and business to rethink the electronic battlefield, CSO Online, IDG, 2 February 2015, Online: https://www.cso.com.au/article/565269/time-industry-business-rethink-electronic-battlefield/

[4] Gregory, M.A., We're watching you: why the government should focus on cybersecurity, not surveillance, TheConversation, 16 August 2012, Online: https://theconversation.com/were-watching-you-why-the-government-should-focus-on-cybersecurity-not-surveillance-8846

[5] Gregory, M.A., Active Online Security Measures for Business, CSO Online, IDG, 27 April 2015, Online: https://www.cso.com.au/article/573517/active-online-security-measures-business/

[6] Fernyhough, J., Government rebuffed Huawei's cyber security offer, Australian Financial Review, 5 March 2019, Online: https://www.afr.com/companies/telecommunications/government-rebuffed-huaweis-cyber-security-offer-20190305-h1bztd

[7] Fernyhough, J., Huawei asks for trust with cyber security centre in EU, Australian Financial Review, 6 March 2019, Online: https://www.afr.com/companies/telecommunications/huawei-asks-for-trust-with-cyber-security-centre-in-eu-20190306-h1c2gf

[8] Sadler D., Australia 'out in the cold' on cyber, InnovationAus, 7 August 2018, Online: https://www.innovationaus.com/2018/08/Australia-out-in-the-cold-on-cyber

[9] Department of Home Affairs, Telecommunications sector security reforms, Australian Government, 18 September 2018, Online: https://www.homeaffairs.gov.au/nat-security/Pages/telecommunications-sector-security-reforms.aspx#

[10] European Commission, "Commission Recommendation – Cybersecurity of 5G Networks", March 2019. https://www.europeansources.info/record/recommendation-on-cybersecurity-of-5g-networks/

[11] European Commission, Proposal for a European Cybersecurity Competence Network and Centre, 19 September 2018, Online: https://ec.europa.eu/digital-single-market/en/proposal-european-cybersecurity-competence-network-and-centre

[12] Gregory, M.A., Will national security concerns end the globalisation of technology? East Asia Forum, 7 March 2019, Online: https://www.eastasiaforum.org/2019/03/07/will-national-security-concerns-end-the-globalisation-of-technology/

[13] Australian Signals Directorate's Australian Cyber Security Centre, Cyber Supply Chain Risk Management Practitioners guide, June 2019, Online: https://www.cyber.gov.au/sites/default/files/2019-06/Supply%20Chain%20Risk%20Management%20-%20Practitioners%20guide.pdf

[14] Karp, P., Australia's war on encryption: the sweeping new powers rushed into law, The Guardian, 8 December 2018, Online: https://www.theguardian.com/technology/2018/dec/08/australias-war-on-encryption-the-sweeping-new-powers-rushed-into-law

[15] Science and Technology Select Committee, Letter to the Secretary of State for Digital, Culture, Media and Sport about Huawei's involvement in the UK's 5G network, 15 July 2019, Online: https://www.parliament.uk/business/committees/committees-a-z/commons-select/science-and-technology-committee/news-parliament-2017/chairs-comments-huawei-5g-network-17-19/

[16] Donahue, P., German Spy Chief Says Huawei Can't Be 'Fully Trusted' in 5G, Bloomberg, 30 October 2019, Online: https://www.bloomberg.com/news/articles/2019-10-29/german-spy-chief-says-huawei-can-t-be-fully-trusted-in-5g

[17] Soldani, D., Shore, M., Mitchell, J., & Gregory, M. A. (2018). The 4G to 5G Network Architecture Evolution in Australia. Journal of Telecommunications and the Digital Economy, 6(4), 1-30. Online: https://doi.org/10.18080/jtde.v6n4.161