

10 October 2019

**Cyber Security Policy Division
Department of Home Affairs
4 National Circuit
Barton ACT 2600**

Dear Sir/Madam

Re: Submission to Australia's 2020 Cyber Security Strategy consultation

Swinburne University of Technology welcomes the opportunity to take an active role in the development of Australia's 2020 Cyber Security Strategy through this consultation and any future input or initiative development opportunities that may evolve. Please find below our responses to a number of the questions posed in your *A Call for Views* paper where we believe we can add value:

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

In our highly inter-connected world, threats to society can come from everywhere through cyberspace. To date, there has been extensive research studying various aspects of cybersecurity incidents. Most of the work has focused on passive analysis, detection, and defence. However, there have been no comprehensive studies that use data from multiple sources and then process and interpret the aggregated data to provide verifiable measures that effectively control damage before attacks occur. Government should be focusing on protecting cyberspace through novel predictive methods based on the analysis of very large amounts of data to yield predictive countermeasures and conducting prediction. Research and innovation in the area of using data-driven methodologies to detect and prevent cyber threats should be supported and promoted.

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

To maximise benefits and minimise risk, Government should not take direct action on private networks and systems, or collect private information from individuals and businesses beyond the current national security law framework. Currently it is not yet clear if Government is protecting or facilitating the trade of personal data. Instead, Government should play a key role in growing the cyber capabilities for Australia.

The former Prime Minister hosted two industry roundtables in 2017. However, the academia and research institution involvement was limited. The necessary connections among the Government's organisations, such as ASD, ACSC, and the

Swinburne Research

John Street Hawthorn
Victoria 3122 Australia

PO Box 218 Hawthorn
Victoria 3122 Australia

Telephone +61 3 9214 5223

Facsimile +61 3 9214 5267

www.swinburne.edu.au/research

ABN 13 628 586 699

CRICOS Provider 00111D

Australian Federal Police, the industry, and Universities appears minimal. Research institutions were not involved in the co-design of joint cyber threat sharing centres in different cities. Universities and the VET sector could be involved to ensure research informed policy and practice, and aligned education and training.

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

The government has supported research to better understand the cost of malicious cyber activity to the Australian economy via different mechanisms such as the Australian Research Council grants, the AustCyber projects, Data61 projects, and the Cyber Security CRC projects. Ongoing support is required to ensure the continuity of the research activities and the translation of research outcomes into economic and social benefits. Government should not only support cyber awareness and education, but also support fundamental research by Australian researchers on the system approaches to protect both hardware and software from malicious cyber-attacks.


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

There is no independent cyber security assessment association or organisation in Australia. Such organisations can assist users to understand their risks of malicious cyber activities from an objective and fair perspective.

AusCERT provides members with proactive and reactive advice and solutions to current threats and vulnerabilities. It helps members prevent, detect, respond and mitigate cyber-based attacks (<https://www.auscert.org.au>), however an independent cyber security assessment association, could also help to raise understanding of the risks through providing thorough assessment of user networks and systems. In UK, JISC runs and protects the networks of its members by detecting and resolving issues that might affect availability, in an effort to ensure seamless access for users (<https://www.jisc.ac.uk/network/security>).

Thank you for the opportunity to shape this new and important strategy for the security of Australia. For further information in relation to this submission, please contact Professor Yang Xiang, Dean - Digital Research & Innovation Capability Platform,

Yours sincerely


Professor Aleksandar Subic
Deputy Vice-Chancellor Research & Development
Swinburne University of Technology