atse.org.au

Submission to the Department of Home Affairs

Australia's 2020 Cyber Security Strategy - A call for views

1 November 2019

ATSE
Australian Academy of Technology & Engineering

GPO Box 4055
Melbourne, 3001
VIC, Australia
T + 61 3 9864 0900
F + 61 3 9864 0930
E info@atse.org.au

AUSTRALIA'S 2020 CYBER SECURITY STRATEGY - A CALL FOR VIEWS

The Australian Academy of Technology and Engineering[1] welcomes the invitation from the Australian Government Department of Home Affairs to respond to *Australia's 2020 Cyber Security Strategy – A call for views.*

Australians are increasingly moving towards living part of their lives in the digital world, including socialising, learning, conducting financial transactions and storing and sharing personal data. There is a growing national and global dependence on cyber space for economic wealth and societal well-being, the control and monitoring of critical infrastructure, and the storage, processing and management of sensitive information.

Devices with embedded controllers are on the increase and we are at the dawn of the Internet of Things (IoT), with an estimated 20 billion devices expected to be connected by 2020. Smart cities with the vision of remotely monitoring and managing critical infrastructure, public buildings, transport, businesses and homes is gathering pace. Already there are smart energy meters in homes, home security systems linked to mobile phones, the promise of driverless cars, and the appearance of smart city plans.

The increased dependence on connected systems puts Australia at higher risk of cyber threats. Australia must develop strong cyber security systems and measures by playing a leading role in the development of cyber technology and its application in business, industry, government and society. Cyber security must be positioned as an enabler for our digital future.

As a trusted global cyber nation Australia will need to maintain the highest of cyber security standards including the development of a top class professional cyber security workforce and a comprehensive education program for its citizens. Emphasis on cyber security will be on proactive, rather than reactive, approaches, and will include: techniques for predicting likely threats and vulnerabilities; tools and techniques for achieving real-time comprehensive cyber situational awareness; and methods for ensuring business continuity in the face of cyber attack. New technologies such as big data and autonomous and cognitive systems based on Artificial Intelligence will play a central part in this.

---

1. We are a Learned Academy operating as an independent, non-political and expert think tank that helps Australians understand and use technology to solve complex problems. We bring together almost 900 Fellows elected by their peers. As Australia's leading experts in applied science, technology and engineering, Fellows provide impartial, practical and evidence-based advice on how to achieve sustainable solutions and advance prosperity. www.atse.org.au

Academy Principles

The Academy has a long standing interest in Australia's digital future and cyber security, and recently produced several reports on Australia's Digital Future with recommendations towards the integration of emerging digital technologies and appropriate action towards improving Australia's cyber security:

- Embracing Australia's Digital Futures (ATSE, 2017)
- Positioning Australia as a Leading Digital Nation (ATSE, 2018)
- Implications for an Australian Society of Digital Futures Development (ATSE, TBC)

The Academy believes that digital transformation has the potential to greatly enhance Australia's economic, health and societal well-being. However, this comes with significant challenges. Our dependence on cyberspace makes us increasingly vulnerable to cyber attack which can compromise our monitoring and control of critical infrastructure; disrupt and degrade our goods and services; compromise our privacy and degrade our societal well-being.

The Academy believes that resources should be allocated to developing a robust regulatory framework for ensuring cyber resilience, developing a skilled and professional work force and strengthening our cyber resilience R&D.

Submission Summary

The Academy believes that:

- Complete cyber security cannot be achieved, and Australia must focus on achieving cyber resilience, which is the ability to continue operating in the face of a cyber attack
- Understanding critical dependencies and system vulnerabilities are key to achieving cyber resilience
- Providers of cyber goods and services must adhere to mandatory cyber security standards and be held liable when failing to do so
- The *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* poses a significant barrier to expanding Australia's cyber-security sector, as it will reduce investment in Australian cyber products and services which may be considered to be less secure
- The 2020 Cyber Security Strategy must acknowledge and address vulnerabilities and unknown threats likely to emerge from new and emerging technologies including IoT technology

The Academy recommends that:

- The Federal Government seeks to establish national cyber security standards which are developed by knowledgeable bodies and technical experts
- The Federal Government establish regulations regarding the liability of providers of cyber goods and services for data security and privacy
- The 2020 Cybersecurity strategy have a more proactive rather than reactive approach, with a view for managing future and emerging vulnerabilities and threats associated with emerging technologies such as IoT

- Priority action is taken by Government and education bodies to increase the number of high quality cyber professionals in Australia and to ensure that cyber security is a common thread through all science and technology courses

Response to 'Australia's 2020 Cyber Security Strategy – A call for Views' Discussion Paper

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

The Academy believes that:

- The cyber threat environment is highly variable, diverse and rapidly evolving. It is likely that there are a large number of threats whose existence, nature and specific characteristics will be unknown until they are exercised, known as zero day threats.
- Hardware trojans are entering the landscape with IoT providing a rich attack surface. Threats are trending away from being code based to data, systemic and business process attacks. A focus on hardware trojans is important, as there is currently no control over hardware supply chains and the presence of cyber physical systems are increasing dramatically.
- Future cyber threats will be increasingly difficult to detect, more persistent and more difficult to counter. We can expect threats to be real-time adaptable and able to detect and overcome our countermeasures.
- Australia is a data dependent and data driven society, consequently threats to data availability, integrity and confidentiality should have a high priority. Whilst a focus on countering specific threats is useful, there should be an increased emphasis on achieving cyber resilience.
- The 2016 Cybersecurity Strategy has a strong focus on enterprise IT and web services but did not address critical infrastructure or IoT technology, which the Academy considers to be critical areas for inclusion in the 2020 Cybersecurity Strategy.

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

Not addressed as this is outside the technical focus of the Academy.

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

Not addressed as this is outside the technical focus of the Academy.

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

The Academy believes that shared situational awareness and collaborative approaches are necessary to achieve national cyber resilience, and that governments should take the lead in creating the environment necessary to encourage this.

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

The Academy believes that in order for the Government to maintain the trust of the Australian community it must make a commitment to taking individual citizen's data privacy seriously, and demonstrate accountability by taking strong, open and transparent action in response to data leaks.

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

The Academy believes that security must be a priority feature of cyber products and services, and that security must become an issue of product liability. The Academy recommends that cyber products and services should abide by cyber security standards that have been developed by knowledgeable bodies and technical experts, with significant contributions from the R&D community.

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

The Academy believes that the role that Government can play to support consumer security is to establish regulations ensuring the liability of providers of cyber goods and services for data security and privacy. Industry should work collaboratively with Government in ensuring these regulations are complied with and regularly reviewed, and strengthen regulations as necessary.

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

The Academy believes that Government and industry must consider cyber security to be a first-class safety issue, in order to increase the security, quality and effectiveness of cyber security and digital tools.

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

Please see the Academy's response to Question 18.

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

The Academy considers that the regulatory environment for cyber security is not strong enough in its current state, based on the knowledge that providers of cyber goods and services are not being held liable for data and privacy breaches.

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

The Academy recommends that the Government establish regulations ensuring the liability of providers of cyber goods and services for data security and privacy, and use liability as an incentive for providers to do better.

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

The Academy believes that cyber technology needs to be designed with security as a key performance parameter, rather than as a 'bolt-on' afterthought, and recommends the creation of a regulatory framework that encourages this.

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

The Academy recommends the establishment of a "trusted partner" status for suppliers who adhere to defined standards, and the establishment of regulations ensuring the liability of providers of cyber goods and services for data security and privacy.

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

The Academy believes that cyber security must be a common thread through various science and technology programs, and that a strategic focus on digital business, data management and cyber security vocational training and University education would support the development of a highly skilled workforce of cyber security professionals.

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

The Academy believes that in order to ensure growth of the cyber insurance market, the Government must establish clear liability of providers of cyber goods and services for data security and privacy, and create a transparent regulatory environment.

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

The Academy considers that the following two mechanisms may be used to reduce high-volume, low-sophistication malicious activity targeting Australia:

- Improvement in automated/autonomous processes to counter threats would be beneficial as reduced efficacy of cyber-attacks will act as a deterrent to perpetrators.
- A population-wide approach to education about data security and cyber attacks, and what individuals can do to better protect themselves from cyber threats.

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

The term "hostile environment" could suggest the use of active cyber security countermeasures. The Academy advises extreme caution in this regard as the technical challenges associated with attribution and validation of such countermeasures make this a very expensive and risky approach.

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

The Academy considers that the following two mechanisms may improve the ability of governments and private entities to identify and remediate cyber risks on essential private networks:

- Shared situational awareness, whereby organisations share real-time data on cyber threats or attacks and collaborate to counter cyber attacks and address cyber vulnerabilities within the network.
- The use of AI to design cognitive systems which have the potential to provide rapid decision support capabilities through autonomously recognising cyber threats and attacks, and provide course of action suggestions.

19. What private networks should be considered critical systems that need stronger cyber defences?

The Academy believes that many control systems, including electricity, water and road traffic, should be considered critical systems that need stronger cyber security defences, and that the movement of these systems towards open systems technology, as well as their reliance on dated technology, dramatically increases their vulnerability. The Academy also believes that as Australian industries increasingly adopt Industry 4.0, consideration of cyber security and identification of vulnerabilities in these systems will be increasingly important.

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

Not addressed as this is outside the technical focus of the Academy.

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

The Academy considers that the main constraints to information sharing between Government and industry on cyber threats and vulnerabilities are commercial sensitivity, security, privacy and a lack of infrastructure for real time shared situational awareness, including tools to ingest data and provide actionable intelligence at a level that can be comfortably shared.

22. To what extent do you agree that a lack of cyber awareness drives poor consumer choices and/or market offerings?

The Academy acknowledges that a lack of cyber awareness drives poor consumer choices and market offerings, but believes that the implementation of national cyber security standards and regulations to ensure liability of providers of cyber goods and services for data security and privacy are the key drivers of improvement of market growth and consumer safety.

23. How can an increased consumer focus on cyber security benefit Australian businesses who create cyber secure products?

The Academy believes that by ensuring liability, this will create pressure on businesses to produce more secure cyber products.

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

The Academy believes that a "mass campaign" targeting the Australian public as a whole is necessary, and acknowledges past research and evidence that demonstrates changing human behaviour is difficult. The Academy advises engaging with social scientists and psychologists to understand the efficacy of other campaigns, such as anti-smoking, drink driving, and the AIDS awareness campaign of the 1990's.

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

The Academy strongly believes that cyber security features should be prioritised in products and services.

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

The Academy believes that the growth in Australia's cyber capabilities will increasingly yield new vulnerabilities, particularly with respect to critical infrastructure and IoT technology, and that Australia's focus should be shifting towards ensuring cyber resilience.

Australia has the opportunity to become a global role model for achieving strong cyber security systems and capabilities. To ensure Australia meets its domestic and international cyber security responsibilities, it must focus on developing policies necessary to support the growing complexity of Australia's digital and data driven society.

ATSE would be pleased to further assist with this inquiry as appropriate. The contact at the Australian Academy of Technology and Engineering is Matt Wenham, Executive Director, Policy (Ph: +61 3 9864 0900 or matt.wenham@atse.org.au).

Professor Hugh Bradlow

ATSE President