Submission by Professor Dan Jerker B. Svantesson to the Department of Home Affairs regarding:

The 2023-2030 Australian Cyber Security Strategy Discussion Paper

April 2023

Professor Dan Jerker B. Svantesson

Faculty of Law, Bond University
Gold Coast, Queensland, 4229
Australia

[redacted]

Summary of major points

- Australia ought to actively plan and strategize for the potential creation of a volunteer-based 'cyber emergency service' possibly as part of a 'cyber militia'.
- Improved capacity for attribution must be a key component in Australia's strategy to become the most cyber secure nation in the world by 2030.
- The Government should develop criteria for what may be termed 'Cyber Resilience Impact Assessments'.
- Australia ought to work on a Cyber Security Act but that should not detract from recognising that we are dealing with an entire system of interconnected legal and regulatory instruments.
- Australia must coordinate with likeminded States as often as is practical and is particularly well placed to continue taking on a mutually beneficial leadership role in the Indo-Pacific region.
- Australia ought to be present, and make its voice heard, at as many different international forums as possible.
- Further reform is needed in relation to 'data minimisation'.

1. General remarks

1. I welcome the initiative taken to seek input on the 2023-2030 Australian Cyber Security Strategy Discussion Paper.

2. These submissions are intended to be made public.

3. These submissions deal only with a selection of the questions raised in the Discussion Paper. No views are expressed on any other matters.

2. Introductory observations

4. The cybersecurity climate is seemingly constantly worsening. Presently, this is partly linked to the worsening climate in international relations. Australia must therefore have a cybersecurity strategy that recognises, and addresses, a diverse range of potential threats including cyberattacks carried out by state actors, and the risk that Australia may find itself targeted in hybrid warfare operations.

5. As is clear from the topics addressed, and as is emphasised further in the questions raised, the Discussion Paper has both a domestic and an international dimension. This is no doubt the correct approach, and it is also appropriate for the strategy to pay particular attention to the Indo-Pacific region.

6. Another important aspect of the strategy is to approach cybersecurity as a whole-of-nation effort. Much work lies ahead in that respect both in relation to improving public-private mechanisms for cyber threat sharing and blocking, and for matters such as supporting Australia's cyber security workforce and skills pipeline.

3. "1. What ideas would you like to see included in the Strategy to make Australia the most cyber secure nation in the world by 2030?"

7. In response to this important question, I will only focus on two particular matters. The first is that of what may be termed a volunteer-based 'cyber emergency service'. What I have in mind here may, in a way, be seen as a cyber equivalent of, for example, the volunteer firefighters. People devoting part of their time – on a voluntary basis – to an activity aimed at protecting Australia and the Australian society.

8. The 2022 Russian attack on Ukraine has highlighted the roles that a 'cyber militia' may play. In the case of Ukraine's 'IT Army', activities ranging from offensive 'hacking' and destruction ('defacing') of Russian public websites through to general IT support for Ukraine has been reported. The former role could be used as a form of deterrence, while the latter

could contribute towards societal resilience. However, there are many other roles that a cyber militia, including a volunteer-based 'cyber emergency service', could fulfil.

9. While the Ukrainian cyber militia appears to be a predominantly improvised response to the Russian aggression, Australia would do well to actively plan and strategize for the potential creation of its own cyber militia. A cyber militia could include a volunteer-based 'cyber emergency service'. The cyber strategy represents an appropriate opportunity to begin the discussion about doing so. At the minimum, Australia's cyber strategy ought to consider questions such as:

(1) How can Australia utilise a domestic cyber militia and a volunteer-based 'cyber emergency service', including;

a. Are there ways to better utilise Australia's high-level of IT expertise?

b. How can our various experts to be acting as volunteers in case of serious cyber incidents be vetted, trained, and organised?

(2) How should Australia approach foreign volunteers seeking to join its cyber militia once created;

(3) How does Australia address situations where Australians seek to volunteer for a foreign cyber militia; and

(4) Are there ways to formalize, and harmonize, the response to questions above – in particular, two and three – with likeminded States in a mutually beneficial manner?

10. I have written on these matters in some detail elsewhere and refer interested readers to those publications rather than seeking to reproduce them here.[1] However, I note that, perhaps the most interesting lesson from Ukraine is that a cyber militia can be a highly potent tool that, at least in its simplest form, can be created very quickly and at almost no cost. Speed and low cost are indeed uncommon characteristics when it comes to defence measures.

11. While the discussion above was advanced in response to the first question raised in the Discussion Paper, it may also be seen to feed into question 12; i.e., "What more can Government do to support Australia's cyber security workforce through education, […] and accreditation?"

[1] Svantesson, Dan, Regulating a 'Cyber Militia' – Lessons from Ukraine, and Thoughts About the Future. Available at SSRN: https://ssrn.com/abstract=4296849 or http://dx.doi.org/10.2139/ssrn.4296849; and Svantesson, Dan Jerker B.: *Legal Safeguards for the Volunteers of Ukraine's Cyber Militia, VerfBlog,* 2022/3/23, https://verfassungsblog.de/legal-safeguards-for-the-volunteers-of-ukraines-cyber-militia/, DOI: 10.17176/20220323-121142-0.

12. The second idea I want to mention that I would you like to see included in the Strategy to make Australia the most cyber secure nation in the world by 2030 is that of 'attribution'. A term curiously missing from the Discussion Paper, and that also was missing in Australia's 2020 Cyber Security Strategy.

13. The ability to ensure attribution is a key to successful deterrence in peacetime, especially in relation to attacks conducted directly or indirectly by state actors. And even though ensuring attribution is, of course, easier said than done, I still think this is an important observation because it points to a key issue to work on further and build expertise on.

14. Put differently, improved capacity for attribution must be a key component in Australia's strategy to become the most cyber secure nation in the world by 2030.

4. "2. What legislative or regulatory reforms should Government pursue to: enhance cyber resilience across the digital economy?"

15. Cyber resilience is central not just for the digital economy, but also for the operation of a modern society in other regards. Consequently, cyber resilience must constantly be kept in mind, and the Government should develop criteria for what may be termed 'Cyber Resilience Impact Assessments' to be performed prior to any development that may seriously undermine Australia's cyber resilience.

16. It may also be noted that cyber resilience goes hand in hand with deterrence. In a sense cyber resilience is a form of deterrence, and deterrence facilitates cyber resilience.

17. Not least in the context of State actors, deterrence needs to be approached as a system, and all aspects of this system needs to be sharpened. Thus, via the link of deterrence, there is a connection between cyber resilience and a wide range of possible legislative or regulatory reforms that the Government usefully could pursue to enhance cyber resilience across the digital economy.

18. Imagine, for example, that a significant cyberattack on Australian interests is properly attributed to a specific foreign state actor. Making public who is responsible may then e.g., make consumers wish to avoid products from that country. But as it is now, Australia's laws regarding country-of-origin marking are too weak making it too hard for consumers to avoid products from a specific country.

19. Thus, improving Australia's laws regarding country-of-origin marking may facilitate consumer boycotts that can work as a deterrence against cyberattack by foreign state actors, thus helping to build cyber resilience.

20. Admittedly there are many steps involved in the example above, but it illustrates how we need to approach all these matters a system.

21. This brings us to the answer to the sub-question "Should Australia consider a Cyber Security Act […]?" included in the Discussion Paper. My answer is yes, Australia ought to work on a Cyber Security Act and some inspiration may e.g., be drawn for the EU's approach. The main concern with pursuing a Cyber Security Act is, however, that it may become the focus at the expense of a recognition that cybersecurity is a complex and multifaceted topic that needs to be addressed on a broader whole-of-society level and a Cyber Security Act can thus only be one piece of the puzzle.

22. In other words, Australia ought to work on a Cyber Security Act but that should not detract from recognising that we are dealing with an entire system of interconnected legal and regulatory instruments.

5. "3. How can Australia, working with our neighbours, build our regional cyber resilience and better respond to cyber incidents?"

23. The goal of a more secure Australian cyber environment can best be achieved via a more secure online world internationally. Australia must coordinate with likeminded States as often as is practical and is particularly well placed to continue taking on a leadership role in the Indo-Pacific region.

24. In doing so, Australia can provide useful training and law reform advice both directly and via targeted projects run by international organisations such as UNCTAD. But this leadership role can also directly benefit Australia.

25. The example of cyber security in Internet of Things ('IoT') devices is illustrative. Australia has encountered the security concerns associated with IoT for a longer period than most of its neighbours in the Indo-Pacific region. Thus, Australia has more advanced expertise on the topic, and in this we find opportunities to assist our neighbours with relevant training and law reform proposals. At the same time, Australia's possibility of influencing the manufacturers of IoT devices obviously increases if security standards are adopted widely in the Indo-Pacific region as opposed to only in Australia.

26. This is a practical illustration of a mutually beneficial manner in which Australia can work with our neighbours, build our regional cyber resilience and better respond to cyber incidents.

6. "5. How should Australia better contribute to international standards-setting processes in relation to cyber security, and shape laws, norms and standards that uphold responsible state behaviour in cyber space?"

27. The topic of international standards-setting was already addressed in part above.

28. In addition, it is important that Australia is present, and makes its voice heard, at as many different international forums as possible. The difficulty is, of course, that it is impossible to have a voice everywhere.

29. In choosing which forums to focus on, the selection must keep in mind that key developments often take shape in (informal) workgroups lacking decision-making powers, even though those developments are then formally adopted in the obvious main forums.

30. As part of the work undertaken in these forums, Australia should contribute to agreement about how international law applies in cyber context. Topics such as sovereignty, jurisdiction, due diligence, and the attribution of responsibility for non-State cyber actors require further attention. Indeed, that work could usefully extend to clarifying what constitutes responsible state behaviour in relation to the type of cyber militia discussed above.

31. As noted in the submission by Haataja *et al*: "Australia's leadership […] will be enhanced if it further develop its national position on how it considers international law to apply in the cyber context."[2] I fully endorse this claim.

7. "19. How should the Strategy evolve to address the cyber security of emerging technologies and promote security by design in new technologies?"

32. There is clearly a multitude of matters that usefully could be raised in response to this important question. I will focus on one only; that is, so-called 'data minimisation'.

33. Catastrophic data leaks like the September/October 2022 events affecting millions of customer records highlight the harms that may be caused in the absence of sufficient data minimisation measures. Further reform is needed in this respect to address the cyber security of emerging technologies and promote security by design in new technologies.

[2] Karim, Md Saiful, Haataja, Samuli, McKenzie, Simon, & Guihot, Michael (2023) Maritime Cybersecurity and the Australian Cyber Security Strategy. This file was downloaded from: https://eprints.qut.edu.au/238768/.

Professor Dan Jerker B. Svantesson

Professor Svantesson is based at the Faculty of Law at Bond University. He is also a Researcher at the Swedish Law & Informatics Research Institute, Stockholm University (Sweden), a Visiting Professor, Faculty of Law, Masaryk University (Czech Republic) and serves on the editorial board on a range of journals relating to information technology law, cyber security, cybercrime, data privacy law and law generally.

He held an ARC Future Fellowship 2012-2016, has written extensively on Internet jurisdiction matters and has won several research prizes and awards including the 2016 Vice-Chancellor's Research Excellence Award. Professor Svantesson has been identified as the field leader in 'Technology Law' in The Australian RESEARCH magazine four years in a row (2021, 2020, 2019 and 2018).

The views expressed herein are those of the author and are not necessarily those of any organisation with which Professor Svantesson is associated.