

Australian Seniors Cyber Volunteer Force – Combining ‘will’ and ‘skill’

Professor Dan Jerker B. Svantesson

As part of a ‘whole-of-society’ approach to cyber defence, Australia would benefit from harnessing the substantial capabilities available from Australian seniors. This concept paper provides some initial thought about what that may entail.

27 October 2025

Australian Seniors Cyber Volunteer Force – Combining ‘will’ and ‘skill’

Professor Dan Jerker B. Svantesson

Key points

- Australia is under constant attack in Cyberspace.
- Cyber defence is a ‘whole-of-society’ concern, and we cannot afford to overlook any resources at our disposal.
- In the Cyber-context, Australian seniors are often viewed, and treated, like a security concern. However, that is not telling the full story. Rather, Australian seniors can be a valuable resource in cyber defence broadly defined.
- Australian seniors could form an ‘Australian Seniors Cyber Volunteer Force’ on a local, state, or national level, and the government should support and lead such an effort.

This document draws upon: Dan Jerker B Svantesson & Samuli Haataja (2025), Volunteer Cyber Forces to Strengthen Australia’s Defence,
<https://bond.edu.au/sites/default/files/2025-07/CyberVolunteerReport2025FIN.pdf>

Background

Australia is under constant attack in Cyberspace. Cyberattacks have a huge financial and societal cost, and mis- and dis-information is undermining our democracy and our social cohesion. All this is beyond dispute, widely recognised, and a concern for the whole of our society.

Responding to this is a whole-of-society matter, and we must utilise all the tools at our disposal. Australians in general, and not least senior Australians, have a proud tradition of volunteering. Consequently, building an ‘Australian Seniors Cyber Volunteer Force’ structure is a natural step to strengthen Australia’s Cyber defence, broadly defined.

Who can help?

Senior Australians are often seen as a weakness and a security concern in the Cyber-context. But that is a dated and overly simplistic picture that no longer holds true.

Many Australian seniors now have years of computer-based work experience resulting in a set of solid basic computer skills. And some senior Australians have retired from high-level IT industry jobs including in the cybersecurity sector.

Whether you are a cybersecurity expert or an ‘average computer user’, you can play an important role in an ‘Australian Seniors Cyber Volunteer Force’.

What can an ‘Australian Seniors Cyber Volunteer Force’ do?

There are several roles that an ‘Australian Seniors Cyber Volunteer Force’ could perform, such as:

Cyber awareness training – Cyber security starts with basic computer and media literacy. If we can raise the average level of computer and media literacy, we can help minimise the impact of scams, fraud, disinformation, and cyberattacks. A cybersecurity-aware nation is a resilient nation. We can also help people build resistance to mis- and dis-information. Doing so is a matter of teaching *how* to think, not *what* to think; after all, in a democracy, there is room for different views. All this makes Australia safer and more resilient.

An Australian Seniors Cyber Volunteer Force could help train the Australian public in everything from basic computer skills to more advanced cyber security for the home environment, as well as how to identify scams and disinformation.

Illustrative example for ‘Cyber awareness’ training: Switched on Seniors
(<https://www.switchedonseniors.net.au/>)

Open-source intelligence (OSINT) – Due to the Internet, a wealth of information of national security interest may now be obtained ‘open-source’ via so-called ‘open-source intelligence’ or ‘OSINT’; that is, the collection and analysis of intelligence from publicly available sources. It has been noted that “80 to 95 per cent of classified intelligence is built upon information gathered in the realm of open-source information”¹, and volunteers – such as an ‘Australian Seniors Cyber Volunteer Force’ – can play an important role in OSINT.

Illustrative example for OSINT: Glimt (<https://glimt.nu/>)

‘Glimt’ is a ‘crowd forecasting’ platform operated by the Swedish Defence Research Agency (FOI) in collaboration with the Ukrainian government. Crowd forecasting is an established method, and on this platform, volunteer contributors are invited to make forecasts in relation to topics that may inform the Ukrainian government. This showcases one of the many ways in which volunteer OSINT efforts can be guided and harnessed.

Information conflicts – Australia is subject to constant information and cognitive campaigns initiated, or directed, by foreign actors. Thanks to technological developments, hostile actors have more options available than ever before to influence opinions and processes in foreign states.² And their appetite for doing so is not in doubt.

¹ Michael Weinberg, ‘Keeping an Open Mindset: Why Military Intelligence Continues to Be Behind Open-Source Information’ (Kungl Krigsvetenskapsakademien, 2024) <https://kkrva.se/artiklar/keeping-an-open-mindset-why-military-intelligence-continues-to-be-behind-open-source-information/> at 110 (accessed 21 July 2025).

² Commonwealth of Australia, *Select Committee on Foreign Interference through Social Media – First Interim Report* (Report, December 2021) https://parlinfo.aph.gov.au/parlInfo/download/committees/reportsen/024741/toc_pdf/FirstInterimReport.pdf;fileType=application%2Fpdf.

Volunteers can play an important role in combatting mis- and dis-information. One important role – training – has already been discussed above. But volunteers – such as an ‘Australian Seniors Cyber Volunteer Force’ – may, for example, also actively work on ‘fact-checking’.

Illustrative discussion regarding disinformation: ‘How do we tackle disinformation online?’
<https://bond.edu.au/sites/default/files/2025-10/How%20Do%20We%20Tackle%20Disinformation%20Online.pdf>

Cybersecurity – Some Australian seniors will have extensive cybersecurity experience and expertise. Such individuals could usefully be invited to engaged in other roles such as resilience building and support. They may even consider joining an Australian Cyber Civilian Reserve as it develops.

Illustrative example for advanced cybersecurity volunteer structures: Estonia’s Defence League (<https://kuberkaitseliit.ee>)

The cyber unit within Estonia’s Defence League’s is a volunteer cyber force established already in 2011. The purpose of the cyber unit is to enhance society’s cybersecurity preparedness and defend Estonia’s independence and constitutional order. Its mission is the protection of Estonia’s ‘high-tech way of life’ through the protection of its ICT infrastructure and supporting national defence objectives.

In peacetime, its focus is on developing cybersecurity preparedness, and in crisis it provides support capabilities to the government.

Structure and organisation

The examples listed above highlight that an ‘Australian Seniors Cyber Volunteer Force’ could fulfil many different roles and could be organised in different ways. However, to provide maximum value for Australia, it would be best that it is organised by the government. As a national concern, it would be logical for this to be a federal initiative. However, it could also be done on a state, or even council, basis. Regardless of who takes the lead, it will be important that some aspects, such as the training, take place on a local, in-person, level.

The path forward

If you are interested in contributing to the development of an ‘Australian Seniors Cyber Volunteer Force’, please speak with your local MPs, local council, or other decisionmakers who potentially can make this a reality.

As illustrated above, an ‘Australian Seniors Cyber Volunteer Force’ can harness a valuable resource and significantly add to Australia’s Cyber defense, broadly defined. In addition, individual members may benefit from learning new skills, keeping active, and enjoying the benefits of a rich social environment as opposed to the social isolation and loneliness that is too common amongst our Australian seniors.³ An initiative such as this may also help further address the ‘digital divide’ that still plagues our society despite important work to address it.⁴

For more information

Dan Jerker B Svantesson & Samuli Haataja (2025), *Volunteer Cyber Forces to Strengthen Australia’s Defence*, <https://bond.edu.au/sites/default/files/2025-07/CyberVolunteerReport2025FIN.pdf>

³ See e.g.: <https://documents.parliament.qld.gov.au/com/CSSC-0A12/IQ-DD31/submissions/00000033.pdf> & <https://www.who.int/activities/reducing-social-isolation-and-loneliness-among-older-people>.

⁴ See e.g.: <https://goodthingsaustralia.org>.

About the Centre for Space, Cyberspace & Data Law

The Centre for Space, Cyberspace & Data Law is established at the Faculty of Law, Bond University (Australia). The Centre brings together researchers and experts in all aspects of space, cyberspace, and data-flows law to engage in research aimed at creating a better understanding of, and a better direction for, the relationship between space, Cyberspace, and data.

About the author: Professor Dan Jerker B. Svantesson

The author of this document – Dan Jerker B. Svantesson – is a Professor at the Faculty of Law and Co-director of the Centre for Space, Cyberspace & Data Law, Bond University Australia. Professor Svantesson has written extensively on Internet law matters and has won several research prizes and awards including the 2016 Vice-Chancellor's Research Excellence Award. The views expressed herein are those of the author alone and are not necessarily those of the Centre for Space, Cyberspace & Data Law, or any other organisation with which Professor Svantesson is associated.

Suggested Citation: Dan Jerker B. Svantesson, Australian Seniors Cyber Volunteer Force – Combining ‘will’ and ‘skill’, Centre for Space, Cyberspace & Data Law 2025:2 (27 October 2025)