Volunteer Cyber Forces to Strengthen Australia's Defence

Dan Jerker B. Svantesson
Samuli Haataja

July 2025

Volunteer Cyber Forces to Strengthen Australia's Defence

July 2025

ISBN: 978-0-6452396-8-3

Funded by the Australian Department of Defence's Strategic Policy Grants Program

The views expressed herein are those of the authors and are not necessarily those of the Australian Government, the Australian Department of Defence, or the universities or other institutions with which the authors are affiliated.

Cover image: Cavan - stock.adobe.com.

Executive Summary

- Australia should harness the capability provided by civilians and develop volunteer cyber forces as part of a whole-of-society approach to national defence and cyber resilience.

- In addition to cybersecurity functions, volunteer cyber forces may be effectively utilised in relation to Open Source Intelligence (OSINT), information and cognitive conflict, as well as espionage and proactive cyber activities.

- A number of States internationally, including key allies, already have civilian cyber reserve structures in place in order to address workforce shortages and increase cyber preparedness in society. Such volunteer cyber forces perform a range of functions ranging from education and awareness raising in society, to incident response. Having these structures in place in peacetime also provides a potential capacity that can be harnessed in times of crisis or conflict.

- Lessons from the States studied in this report, namely Estonia, Finland, Sweden, Taiwan, Ukraine, and the United States, demonstrate that there is no 'one-size-fits-all' model to developing a volunteer cyber force. Australia should develop volunteer cyber forces suited to its governance and organisational structures, taking into account its geography and local conditions.

- The volunteer cyber forces may include youth organisations either drawing upon current structures such as 'Air Force cadets', or by developing new cyber-focused youth organisations.

- Volunteer cyber forces may specifically seek to recruit senior Australians. Doing so limits the competition for talent with the private sector and other organisations.

- Steps may be taken to facilitate cooperation and coordination with Australia's friends and allies as more States develop volunteer cyber forces.

- There are a number of legal considerations under both domestic and international law that must be factored in when developing volunteer cyber forces. These considerations greatly depend on the activities undertaken by the volunteer cyber forces and the context in which they operate. Volunteer cyber force members must be informed about the relevant legal considerations and potential risks associated with their activities.

- The Report concludes with 15 recommendations.

Contents

About the authors

Professor Dan Jerker B. Svantesson is a Professor at the Faculty of Law, Bond University. He specialises in international aspects of the IT society, a field within which he is has published a range of books and articles, presenting in Australia, Asia, Africa, North America and Europe. Dan is a Senior Fellow with the Social Cyber Institute, a 2025 Fellow at the Norwegian Nobel Institute, and an Associated Researcher at the Swedish Law & Informatics Research institute, Stockholm University. Professor Svantesson held an ARC Future Fellowship (2012-2016) and was the inaugural Managing Editor for International Data Privacy Law, published by Oxford University Press. He is a Member of the Editorial Boards for several journals, including the Commonwealth Cybercrime Journal, the International Cybersecurity Law Review, the International Journal of Law and Information Technology, the Commonwealth Law Bulletin, the International Review of Law Computers and Technology, the Masaryk University Journal of Law and Technology and the Computer Law and Security Review. Professor Svantesson has contributed to a commissioned report by international organisations including the United Nations Office on Drugs and Crime, OECD, the United Nations Conference on Trade and Development, the Commonwealth Secretariat, and the Internet & Jurisdiction Policy Network.

Dr Samuli Haataja is an Associate Professor at Griffith Law School, Griffith University. His research explores international law and cyber security, with a focus on state-sponsored cyber operations under public international law. He has published widely in books and leading journals in the field.

1. Introduction

The importance of cyber, both as a distinct war-fighting domain and as support for the other war-fighting domains, is now well established. Australian defence doctrine recognises this and is continuously being adjusted accordingly. A strong characteristic of the cyber domain is its deep integration in, and partial dependence on, civilian structures including many under the control of the private sector.

Cybersecurity, and the cyber environment more broadly, are consequently whole-of-society concerns and must be defended with a whole-of-society approach. The same is true in the related, or indeed entwined, information and cognitive war-fighting domains.

Perhaps it is the awakening to this characteristic that has prompted so many States to explore options for integrating civilian capabilities in the defence of the cyber domain? Or perhaps such developments are more directly driven by personnel shortages in cyber security and defence?[1] Or maybe it is because in some areas, the private sector has the better resources and perhaps the best staff? Most likely, it is a combination of all of these factors, and perhaps others.

What is clear, however, is that there is an unprecedented level of interest in harnessing volunteer capabilities to strengthen defence in the cyber, and related, domains. The experiences from Ukraine's improvised 'IT Army' have doubtlessly helped bring attention to the potential contributions that a volunteer cyber force may make. But other States, such as Estonia and the US, already had advanced volunteer structures prior to Russia's full-scale invasion of Ukraine in 2022 that prompted the creations of the famed 'IT Army'.

In this Report, we seek to equip the Department of Defence with unique high quality research informing the development of Australia's defence policy and strategy regarding (1) what roles could volunteer cyber forces fulfil for Australia, (2) how such volunteer cyber forces might be structured, (3) what are the risks involved in Australia establishing volunteer cyber forces, (4) what are the legal constraints and considerations involved, and (5) what can Australia learn from measures taken in this context by States leading the way in the adoption of volunteer cyber forces? Specifically, the Report draws upon the valuable experiences of

[1] Personnel shortages in cyber security and defence seems to be a widespread issue. For example, as to the US situation it has been noted that: 'the U.S. military is not the only one struggling to recruit cyber talent. There is a national shortage of cyber personnel, and the federal government struggles to compete with the private sector, which offers much better pay.' Erica Lonergan and Mark Montgomery, *United States Cyber Force: A Defense Imperative* (FDD Press, March 2024) 15.

Estonia, Finland, Sweden, Taiwan, Ukraine, and the United States.

The Report is timely in the light of international developments but also given domestic developments. As we put the finishing touches to the Report, work is ongoing to implement the recommendations – including the recommendation as to the Cyber Reserve Concept – of the Strategic Review of the Australian Defence Force Reserves:[2]

> "Director Cyber Reserve Concept Support Colonel John Molnar said expressions of interest and a refinement of entry processes would be issued in the coming months to support activation of the cyber reserve capability by early 2026."[3]

The Report's structure follows the research questions outlined above, and the findings are based on a combination of extensive desk research, and informative semi-structured meetings held with key stakeholders from the mentioned jurisdictions during a period from October 2024 to March 2025. We take this opportunity to sincerely thank the many experts who gave up their time to meet with us. Their input has been invaluable and has strongly influenced our thinking. However, the views expressed here are ours alone.

We also take this opportunity to thank the Department of Defence for providing the funding making this project possible via its Strategic Policy Grants, and we thank the research assistants who have contributed to the Report: Alexis Hill, Hoda Asgarian, Ji-Wei Sun, Kuan-Wei Chen, and Marisa Agius.

1.1 The mindset of the Report

Australian activity in cyberspace is governed both by strong domestic laws and by international law. The need to adhere to law is central to upholding democracy, and to Australia playing a credible role on the international arena. Consequently, adherence to the law constitutes a main guiding principle for the Report. At the same time, domestic laws can be amended within certain limits, and much is unclear, or indeed unsettled, under international law. Consequently, it would be a mistake not to allow for a broad-ranging discussion not least as the Report aims to canvass options, not to make decisions. An illustration from outside the cyber domain may be useful.

In February 2022, just days after Russia's full-scale invasion of Ukraine, reports appeared around the world about how

[2] Department of Defence (Cth), *Strategic Review of the Australian Defence Force Reserves* (18 December 2024) https://www.defence.gov.au/about/reviews-inquiries/strategic-review-of-the-adf-reserves.

[3] 'Review to Modernise Reserve Force' (Department of Defence (Cth), 15 July 2025) https://www.defence.gov.au/news-events/news/2025-07-15/review-modernise-reserve-force.

Pravda Brewery – a craft brewery in Lviv – had transitioned from brewing beer to the production of 'Molotov cocktails'. The PR director of Pravda's holding company noted that: "This is probably the only time in history when the government is publishing the recipe of the Molotov cocktails! Because we all have one aim: we're willing to defend our country."[4]

It seems uncontroversial to assume that Pravda Brewery would have preferred to focus on brewing good beer. Equally, it is highly unlikely that the Ukrainian government would have permitted – and indeed helped facilitate – the production of highly dangerous items such as 'Molotov cocktails' under less severe circumstances. This tells us something important about defence planning and the mindset needed.

If defence planning only takes the perspective of a sunny day at a Canberra café (or the equivalent in some other safe democratic capital), the measures we are willing to discuss in the defence of our country may be very different to those that turn out to be both necessary, and acceptable, when the bombs start dropping from the sky.

In thinking about what roles volunteer cyber forces may perform, our starting point must, of course, always be respect for applicable international law, and the goal of peace. But in doing so, we need to consider both the 'Canberra café perspective', and that of Lviv in early 2022. Hoping for the best is appropriate, but planning for the worst is necessary.

1.2 Context and related organisations

The idea of some form of (civilian) volunteer cyber reserve capability for Australia is not new.[5] However, one thing that earlier Australian proposals have in common is that they are focused exclusively on cybersecurity. Further, they seek to utilise those members of society that have adequate training to engage with cybersecurity issues. This Report addresses and endorses the idea that Australia should develop such cyber reserve capabilities, and it highlights that in doing so several questions need to be confronted, such as whether it forms part of the Defence structure or not, and how to avoid unduly undermining the private sector's own cybersecurity resources at times of crisis.

---

[4] Euronews, 'Ukrainian Brewery appeals for Molotov cocktail donations' (27 February 2022) https://www.euronews.com/culture/2022/02/27/ukrainian-brewery-in-lviv-appeals-on-social-media-for-molotov-cocktail-donations.

[5] See in particular Greg Austen, 'Australia Needs to Build a Cyber Militia, Says Cyber Expert' *Insurance Business Australia* (online, 1 May 2019) https://www.insurancebusinessmag.com/au/news/breaking-news/australia-needs-to-build-a-cyber-militia-says-cyber-expert-57578.aspx; Lachlan McGrath, 'Keyboard Warriors: An Australian Volunteer Cyber Corps' (5 March 2023) *National Institute for Cybersecurity Research* https://www.nisr.org.au/article/keyboard-warriors-an-australian-volunteer-cyber-corps.

In addition – and this sets this Report apart from earlier proposals – we also seek to assign a broader set of roles to the proposed cyber volunteer capability allowing the involvement of a broader section of the Australian public. After all, the attacks directed at the Australian cyber environment are diverse and include e.g. mis- and dis-information and cognitive warfare. Thus, what is proposed here addresses a broad capacity gap.

Many Australians who lack cybersecurity training can still help strengthen our defence in the cyber environment. Thus, the proposal seeks to capture, and make use of, a broad section of the Australian public. In essence, the idea is to 'crowdsource' volunteer cyber forces where each member focuses on tasks within their specific competencies.

While Australia's population is relatively small, it is a population with a generally high level of education. To-date, this is an untapped resource and given the hardening international climate in which we find ourselves, we can no longer afford to ignore this resource.

When work commenced on this project, our focus was on what we termed a 'cyber militia' defined along the following lines:

> "A cyber militia undertakes defense-related activities (broadly defined) in or pertaining to cyberspace on behalf of a state, with that state's formal recognition, and with some degree of coordination or guidance on behalf of that state but does so outside the ambit of that state's regular armed forces or national security structure. Cyber militias can be ad-hoc, gathering only for a specific occasion, or standing – and there is nothing to prevent the participants from receiving compensation or support, either financial or in the form of training, from the state in question."[6]

This definition remains useful, and the concept of a 'cyber militia' – whether we call it that or something else like 'cyber citizen guardians' or 'cyber watch' – also remains useful. However, the research and the meetings overseas pointed to such a diversity of organisations and structures that it became clear that it no longer makes sense to focus on one proposed new body under the 'cyber militia label' outlined above as we initially had thought would be the case. As a consequence, our first proposal is that Australia investigates several different options and structures.

In this Report, we use the term 'cyber volunteer force' as an umbrella concept to refer to organisations in which cybersecurity or IT experts, as well as others, can volunteer their expertise and skills outside of their normal jobs. These organisations can have a military

[6] Dan Svantesson, 'Regulating a "Cyber Militia" – Some Lessons from Ukraine, and Thoughts about the Future' (2023) 6(1) *Scandinavian Journal of Military Studies* 86.

element to them, for example in the case of voluntary paramilitary organisations or those operating under a national guard structure, they can operate under civilian emergency services structures, or they can operate within private or other kinds of non-governmental structures. The general purpose of these organisations is to facilitate or enable involvement of volunteers in cybersecurity and/or cyber defence related activities, ranging from education and awareness raising to increase society's cyber resilience, to incident response and supporting governments in cyber operations and defence.

1.3 An entire 'ecosystem'

The solution for strengthening Australia's cyber defence is not necessarily found in one distinct development. Rather, lessons from the States studied for this report suggests that what we need to do is to create an entire 'ecosystem' of multiple component all working to strengthen Australia's defence. This, we argue, include the volunteer cyber forces discussed in the Report, but we will here also make a few brief remarks about broader insights gained from the studied States.

First, however, it should be noted that to examine issues associated with potential volunteer cyber forces, it is useful to note the broad range of current and potential organisations and structures operating in the environment in which potential volunteer cyber forces would be operating, including:

- Regular military and national security cyber forces;
- Civil society actors;
- Journalists and the media;
- Academia;
- Influencers;
- Law enforcement;
- Private sector;
- Intelligence agencies; and
- Various authorities.

Thus, volunteer cyber forces can only ever be one component in a bigger picture, and they must work with, and within, existing structures. These existing structures are found e.g., in Australia's defence force, in civilian government, and in the private sector.

Many of the States studied in this Report have a longstanding and strong governmental structure broadly aimed at defence. Outside the professional military's structure, Sweden, for example, has:

- A minister specifically for civil defence;
- Conscripted soldiers that since 2020 can be trained as 'cyber soldiers' [7] with the aim to "reinforce the cyber defence capability as well as to form the basis for long- term preparedness

[7] Försvarsmakten, 'Cybersoldat' (webpage, 17 July 2025) https://jobb.forsvarsmakten.se/sv/utbildning/befattningsguiden/gu-befattningar/cybersoldat/.

and a skilled and competent workforce."[8]

- An authority – the Swedish Civil Contingencies Agency ('Myndigheten för samhällsskydd och beredskap' or 'MSB')[9] tasked with preparing Swedish society for crisis, the consequences of war and other major incidents;
- A research institute in defence and security – Swedish Defence Research Agency ('Totalförsvarets forskningsinstitut', or 'FOI') – classed as a government agency under the Ministry of Defence;
- A National Cyber Security Center ('Nationellt cybersäkerhetscenter' or 'NCSC') serving as a national platform for private-public collaboration in the field of cybersecurity; and
- An authority – the Psychological Defence Agency ('Myndigheten för physiologist Försvars) – that leads the coordination, and develops the operations, of agencies and other actors within Sweden's psychological defence.

In addition, there are also several academic institutions such as the Swedish Defence University, [10] the Centre for psychological defence[11] and the Centre for Cyber Defence and Information Security,[12] that play a role in the broader Swedish cyber defence structure.

Importantly, Sweden also as a system of 18 volunteer defence organisations contributing to the country's military and civilian defence. [13] These organisations are regulated under Swedish law,[14] and highlight the substantial role that volunteers play in the Swedish defence structure. The most important volunteer defence organisation for the topic of this Report is Frivilliga radioorganisationen ('FRO') (the Voluntary Radio Organisation) tasked to:

- recruit and train members for contract signing for positions in the 'total defence';
- inform about 'total defence';
- conduct youth activities;

[8] Försvarsmakten, 'Cyber Defence' (webpage, 27 April 2023) https://www.forsvarsmakten.se/en/about/organisation/cyber-defence/.

[9] Myndigheten för samhällsskydd och beredskap (MSB), 'MSB – The Swedish Civil Contingencies Agency' (webpage, 17 July 2025) https://www.msb.se/en/.

[10] Försvarshögskolan, 'About Us' (webpage, 17 July 2025) https://www.fhs.se/en/swedish-defence-university/about-sedu/about-us.html.

[11] Försvarshögskolan, 'About Us' (webpage, 17 July 2025) https://www.fhs.se/en/swedish-defence-university/about-sedu/about-us.html.

[12] 'Centre for Cyber Defence and Information Security' (KTH Royal Institute of Technology, 19 March 2025) https://www.kth.se/cdis.

[13] Försvarsmakten, 'Frivilliga försvarsorganisationer' https://www.forsvarsmakten.se/sv/organisation/frivilliga-forsvarsorganisationer/ (accessed 20 July 2025).

[14] Förordning (1994:524) om frivillig försvarsverksamhet (SFS 1994:524) https://www.riksdagen.se/sv/dokument-och-lagar/dokument/svensk-forfattningssamling/forordning-1994524-om-frivillig_sfs-1994-524/ (accessed 20 July 2025).

- promote interest in FRO through association activities;
- develop the members' knowledge within the areas of communication and command systems and cyber security through technical exercises.[15]

While the focus on cyber is a relatively recent addition to the areas of work, its importance is well understood and appropriately prioritised. In 2022, the Swedish Armed Forces decided to formally allocate to FRO the mission, accompanied by financial resources, to develop its work on cyber defence and cyber security making FRO the lead on these questions amongst the volunteer defence organisations.[16] FRO is already running courses on cyber defence and security topics.[17]

Sweden has been used here as an illustration of the extent to which other States engage with the issue of defending themselves in the cyber context, and to showcase that volunteers play a natural role in that work as in the example of FRO. At the same time, it must be recognised that it is not just a matter of adding 'more', and not all initiatives will work immediately. For example, a 2023 Report by the Swedish National Audit Office, found that the creation of the National Cyber Security Center "has not led to an increased capacity for giving priority to measures based on Sweden's overall needs in the information and cyber security field, or to long-term, strategic, holistic and cohesive governance of the area."[18] It remains to be seen whether the restructuring will address this.

In addition, a landscape of multiple and partly overlapping organisations may create certain difficulties. For example, a MSB report titled 'Developing Sweden's Civil Defence: Lessons from Ukraine' observes that:

> "While Sweden is considered to have some robustness, redundancy, and resilience in information and cybersecurity, it faces challenges in sharing information. MSB and other central authorities for total defence are involved in a variety of networks and continuously share information with actors

[15] Försvarets Radioanstalt (FRO), *Grundstadgar för FRO* (PDF), para 1.3 https://www.fro.se/_project/_media/FRODOK/FRODOK Publik/Dokument/FRO Grundstadgar.pdf (accessed 20 July 2025).
[16] Försvarsmakten, 'Frivilligrörelsen får uppdrag inom cyberförsvar och cybersäkerhet' (Högkvarteret, 4 October 2022) https://www.forsvarsmakten.se/sv/aktuellt/2022/10/frivilligrorelsen-far-uppdrag-inom-cyberforsvar-och-cybersakerhetfrivilligrorelsen-far-uppdrag-inom-cyberforsvar-och-cybersakerhet/ (accessed 20 July 2025).
[17] Försvilliga Radioorganisationen (FRO), *FRO Lärplattform – campus.fro.se* https://campus.fro.se/ (accessed 20 July 2025).
[18] Riksrevisionen, *Government Control of National Information and Cyber Security – Both Urgent and Important* (Summary, 13 April 2023), 2 https://www.riksrevisionen.se/download/18.2008b69c18bd0f6ed3f26657/1686569981836/RiR_2023_8_summary.pdf (accessed 20 July 2025).

> running essential societal functions. In the event of heightened alert, however, under current legislation, these actors would be severely restricted in sharing information. At the same time, experiences in Ukraine show that effective wartime defence imposes different demands on information sharing than during peacetime. Therefore, one lesson is that restrictions around the sharing of sensitive information between Swedish authorities needs to be eased during heightened alert and war."[19]

There may be lessons in this for Australia as well.

1.4 'Total defence', whole-of-society

A particularly important long-standing aspect of the defence structure in some of the studied States is found in the concept of 'totalförsvar' in Swedish. Totalförsvar is commonly translated in a literal way as 'total defence'. However, that term lacks a natural meaning in English, and a more informative translation may be found in the phrase 'whole-of-society defence'.[20]

Essentially the idea is that the defence of a State is a task for everyone. Thus, the 'total defence' consists of both military activities (military defence) and civilian activities (civil defence). Total defence includes authorities, organisations, private individuals and companies. This means that e.g., all of Sweden's residents are affected by total defence and are part of Sweden's defence.

If the 'total defence' thinking was (merely) a smart strategy in the past, with a cyber-dominated society, it is now an absolute necessity. As already noted, cyber is a whole-of-society issue, and the defence of cyber needs a whole-of-society approach. Consequently, we need to see a whole-of-society approach to defence in all democratic States including in Australia.

Important lessons may be learnt from States such as Sweden and Finland with a long tradition of whole-of-society defence. However, for Australia it is perhaps at least equally important to be alert to what steps others, who lack this long tradition, are taking. Here, we will consequently focus on recent developments in Taiwan.[21]

---

[19] Räddningsverket (Myndigheten för samhällsskydd och beredskap), *Handbok i krisberedskap: Struktur för myndigheters och kommuners planering* (MSB rapport RIB 2023:12, 2023) 71 https://rib.msb.se/filer/pdf/30951.pdf (accessed 20 July 2025).

[20] See also James Kenneth Wither, 'Back to the Future? Nordic Total Defence Concepts' (2020) 20(1) *Defence Studies* 61.

[21] The 'whole-of-society' thinking can also be seen in discussions in the United States. See e.g.: Craig Singleton, 'China' in Bradley Bowman (ed), *Cognitive Combat: China, Russia, and Iran's Information War Against Americans*

1.4.1 Taiwan

Due to Taiwan's unique geopolitical situation, the island nation is under near constant military threats and cyber-attack from neighbouring People's Republic of China (PRC), which views the island nation as a 'renegade province' that must be inevitably 'reunified' with the motherland. [22] According to data from the National Security Bureau, cyberattacks on Taiwan amounted to an average of 2.4 million attacks a day in 2024, mainly originating from China and targeting telecommunications, transportation and defence infrastructure.[23] As part of its response to this threat, but also to be better prepared for other types of crisis, such as natural disasters, Taiwan has started developing a whole-of-society approach and on 26 December 2024, Taiwan establishment the Whole-of-society (WoS) Defense Resilience Committee. [24]

Activities to-date have included discussions on, and tabletop exercises involving, offensive and defensive exercises centred around critical infrastructure, including the possibility of cyber-attacks against infrastructure for petroleum, water, electricity, finance, medical care, transportation, and information and communications systems. [25] Learning from this, the Committee has, for example, underlined that "good communication between the government and the people is important for maintaining social order; therefore, it is important work to ensure cybersecurity and conduct social communication". [26] Another Committee member underlined that cybersecurity also needs to incorporate discussions on how to respond to "communication disruptions", including considering

(Foundation for Defense of Democracies, June 2024) 17.

[22] 'China-Taiwan "Reunification" Is Inevitable, Says Xi' (31 December 2023) *DW* https://www.dw.com/en/china-taiwan-reunification-is-inevitable-says-xi/a-67863888 (accessed 20 July 2025).

[23] Taiwan, National Security Bureau, *Analysis on China's Cyberattack Techniques in 2024* (5 January 2025) https://www.nsb.gov.tw/en/#/%E5%85%AC%E5%91%8A%E8%B3%87%E8%A8%8A/%E6%96%B0%E8%81%9E%E7%A8%BF%E6%9A%A8%E6%96%B0%E8%81%9E%E5%8F%83%E8%80%83%E8%B3%87%E6%96%99/2025-01-05/Analysis%20on%20China's%20Cyberattack%20Techniques%20in%202024 (accessed 20 July 2025).

Yimou Lee, 'Chinese Cyberattacks on Taiwan Government Averaged 2.4 Million a Day in 2024, Report Says' (6 January 2025) Reuters https://www.reuters.com/technology/cybersecurity/chinese-cyberattacks-taiwan-government-averaged-24-mln-day-2024-report-says-2025-01-06/.

[24] Office of the President, Republic of China (Taiwan), *Minutes of the 1st Meeting of the Office of the President Whole-of-Society Defense Resilience Committee* (26 September 2024) https://english.president.gov.tw/File/Doc/9d77c4fa-2d84-49ca-8449-e590e1d1ef5c (accessed 20 July 2025).

[25] Ibid 28 (Executive Secretary, Minister without Portfolio of the Executive Yuan Chi Lien-cheng).

[26] Office of the President, Republic of China (Taiwan), *Minutes of the 2nd Meeting of the Whole-of-Society Defense Resilience Committee* (26 December 2024) 10 (Committee Member, Enoch Wu) https://english.president.gov.tw/File/Doc/2d7d0a85-9f20-4396-9fb0-3ed2e60136f5 (accessed 20 July 2025).

"methods for maintaining backup communications during power outages and base station disruptions".[27]

The WoS approach figures also prominently in Taiwan's 2025 Quadrennial Defense Review (QDR), [28] which recognises the central role that information and cyber plays in all-out defence and recognises "that Taiwan's collective will to fight is the center of gravity for the PRC's coercive tactics, something that the new whole-of society resilience effort must address".[29]

Taiwan has also conducted its first "Whole-of-society Defense Resilience Committee Field Drill" on 27 March 2025; a drill testing the coordination and communication between government agencies and civil society. [30] After observing the drill, Taiwan's President underscored that Taiwan's security rests "not just on the armed forces, but also on the forces of defense resilience throughout our society. In that way we can achieve peace through strength". [31] This highlights the importance of the will defend amongst the broader population, something that may be strengthened via volunteer cyber forces.

Debriefing the public after the drill, the National Security Council outlined several recommendations for improvement, including "expanding volunteer training programs". [32] The meetings of the WoS Defence Committee are all broadcast live, and uploaded onto YouTube for public access, "underscoring the government's commitment to transparency and continuous refinement of its emergency preparedness measures".[33]

In the debrief, several issues were also highlighted that need to be improved.[34] One is the involvement of school and

[27] Ibid 21 (Committee Member, Dai Chen-yu).
[28] Taiwan Ministry of National Defense, *Taiwan's 2025 Quadrennial Defense Review* (March 2025) https://tsm.schar.gmu.edu/wp-content/uploads/2025/03/Taiwans-2025-QDR.pdf (accessed 20 July 2025). See also Kitsch Yen-Fan Liao, 'Taiwan Focuses on Societal Resilience and U.S. Cooperation in New Defense Review' Jamestown Foundation (28 April 2025) https://jamestown.org/program/taiwan-focuses-on-societal-resilience-and-u-s-cooperation-defense-review (accessed 20 July 2025).
[29] Ibid.
[30] Kuang-Cheng Hsu and Calvin Chu, 'Taiwan Bolsters Whole-of-Society Defense Resilience' Jamestown Foundation (29 April 2025) https://jamestown.org/program/chinese-military-drill-escalates-tensions-underscoring-taiwans-commitment-to-whole-of-society-defense-resilience/ (accessed 20 July 2025).
[31] Office of the President, Republic of China (Taiwan), 'President Lai Observes 2025 Whole-of-Society Defense Resilience Committee Field Exercises' (27 March 2025) https://english.president.gov.tw/NEWS/6933 (accessed 20 July 2025).
[32] National Security Council Deputy Secretary-General Liu Te-chin, *2025 Society-wide Defense Resilience Commission Field Exercise Observation Report (2025 全社會防衛韌性委員會 實地演練觀察報告)* (2025) https://www.president.gov.tw/File/Doc/0c5cf1c5-cc5e-40cf-9d5d-48b9c75d5722 (accessed 20 July 2025).
[33] Hsu and Chu (n 30).
[34] Office of the President, Republic of China (Taiwan), *Minutes of the 3rd Meeting of the Office of the President Whole-of-Society Defense Resilience Committee* (27 March 2025) https://www.president.gov.tw/File/Doc/c1153ad7-c850-4e23-baec-98cf402c5127 (accessed 20 July 2025).

higher education institutions, and the need for the government to educate children from a young age how to react in a crisis.[35]

Further, in terms of communication to the public, it was underlined that there is a need to "confirm the accuracy of the information and avoid public confusion". [36] One member of the committee underlined the concerns of Foreign Information Manipulation and Interference (FIMI), and the need to manage communications with the public in order to concisely and in real-time manage crisis situations.[37] Further, there is a need to better identify, clarify and prepare to dispel rumours, which can sow panic among the public. It was suggested that in future drills, there be dedicated personnel to collect, record and disseminate information in real-time in order to strengthen communication with the public and avoid public panic.[38]

1.5 Potential benefits

Before we turn to examine the roles, structures, risks, and legal issues of volunteer cyber forces, it is proper to say a few words about some of the advantages that may be obtained from such a creation.

Most obviously, volunteer cyber forces may be implemented to supplement, and fill capacity-gaps, in the current structures we have that together make up Australia's cyber defence, broadly defined. The simple reality is that what we have now is not enough. We must obviously address this capacity-gap by recruitment to the defence sector, but it is a highly competitive market – skilled experts are attractive also for the private sector, and internationally. Volunteer cyber forces have the comparative advantages of being low cost, and fast to implement. Few defence measures can boast about that combination of qualities. In addition, they may attract experts who spend the majority of their time in the private sector, and they can work like a bridge to the private sector.

Indeed, done well, volunteer cyber forces may serve as a recruitment tool for defence both in relation to experts in the private sector and to students and other young people who have not yet entered the workforce. On this topic we pause and note the successful youth programme operated by the Swedish FRO (discussed above).

FRO is open to young people, but members under the age of 18 must have their guardian's consent, and members under the age of 15 may only participate in activities of a non-military nature. The youth activities include a dedicated cyber section. [39] The activities of the youth cyber section include a discussion forum run via the platform discord,

[35] Ibid, Committee member Chen Hsin-liang.
[36] Ibid, Committee member Kuo Chia-yo.
[37] Ibid, Committee member Tseng Po-yu.
[38] Ibid, Committee member Yen Po-wen.

[39] Frivilliga Radioorganisationen (FRO), 'Cyberungdom' https://www.fro.se/web/cyberungdom (accessed 20 July 2025).

interactive courses, and a 'cyber camp' run during the school holidays. Additionally, it may be noted that FRO cooperate in the production of a successful podcast on cyber security which also may attract potential members and also educates non-members.[40]

Australia already has youth organisations such as the Air Force's cadets. Such organisations could expand to also address cybersecurity, or new organisations could be set up specifically for youth activities in cybersecurity, OSINT, and information conflict. Such organisation could help raise awareness, increase the will to defend Australia, and facilitate recruitment. For example, one possibility is for the Australian Signals Directorate to set up its own cadets structure with the focus on youth activities in cybersecurity, OSINT, and information conflict.

Additionally, it can easily be imagined that volunteer cyber forces may be engaged in cooperative work with, or be used as a vehicle to harness competence in times of crisis from, various organisations such as universities and NGOs.

To this may be added that, experiences from some of the cybersecurity-focused organisations with which we have been in contact suggest that, by training together in a cybersecurity reserve, familiarity and bonds are created that mean that volunteers are able to draw help from each other in the case of incidents in relation to which time-pressure may preclude the option of starting to seek out the right expertise from unknown sources.

Finally, it may be imagined that volunteer cyber forces may be used to foster social cohesion and mitigate feelings of marginalisation among specific groups e.g., immigrants and minorities.

The above are just some of the core potential benefits that are applicable across the different types of volunteer cyber forces envisaged in the Report. Additionally specific benefits may be obtained from each of the types of volunteer cyber forces discussed.

[40] Cyber Chats & Chill (Spotify, 2025) https://open.spotify.com/show/67Vr4hudsNweY6AfxjZAe5?si=SrYCzRcDSg2qJ4GtIRuVpg&nd=1&dlsi=35d0b61b6e4f4493 (accessed 20 July 2025).

2. Potential roles

Volunteer cyber forces may be deployed in a range of different roles. However, as we will emphasise throughout the Report, we cannot imagine that one single volunteer structure will be suited for all those roles. Rather, we foresee a need for separate and specialised volunteer cyber forces for the different roles we discuss. We focus on five such roles:

- cybersecurity (systems support);
- open-source intelligence (OSINT);
- information and cognitive conflicts;
- espionage; and
- proactive cyber operations ('cyber attacks').

Some of those roles ought to be acceptable already from the 'Canberra café' point of view, while others may be unpalatable unless we adopt the perspective of 'Lviv 2022' discussed in the introduction.

Given that the different types of roles discussed will require different types of members of the relevant cyber volunteer structures tasked with those roles. However, at least for tasks within the area of OSINT and the areas of information and cognitive conflicts the tasks assigned to the members of the relevant volunteer cyber forces may usefully be guided by the following activity characteristics:

- Low risk;
- Low/no sensitivity;
- Limited complexity;
- Labour intensive;
- Under the legal threshold for 'civilians directly participating in hostilities'; and
- Where people are better than bots/tech.

Having said that, the reality is that the circumstances as a whole must set the parameters for the tasks assigned to members of cyber volunteer forces.

The exact roles carried out by volunteer cyber forces may, of course, also vary depending on whether Australia is at war or not. If Australia is at war, the roles may also depend upon whether the fighting takes place overseas or whether Australia has been invaded. However, as noted by Storm Jensen, States can principally seek to defend their societies in the cyber domain through deterrence, protection and resilience.[41] Volunteer cyber forces can contribute positively in all three through the performance of the different types of roles discussed here.

[41] Mikkel Storm Jensen, 'Sector Responsibility or Sector Task? New Cyber Strategy Occasion for Rethinking the Danish Sector Responsibility Principle' (2018) 1(1) *Scandinavian Journal of Military Studies* 1, 18.

2.1 Cybersecurity (systems support)

As already noted, discussions about cyber volunteer capabilities in Australia have so far focused on cybersecurity matters. Additionally, looking at the international landscape, it is predominantly in the area of cybersecurity that we currently find cyber volunteer forces. Below, we point to experiences from Estonia, Finland, Sweden, and the United States. As to the latter, we discuss both developments on a federal level and state-level with a focus on Ohio given the advanced structure found there.

As demonstrated below, generally volunteer cyber forces have two main functions and often analogies are made to volunteer fire fighters. The first is a preventative one, to develop cyber resilience and limit the risk of cybersecurity threats and incidents. This can involve a range of activities around education and awareness raising, to cybersecurity audits. The second relates to incident response. Like fire fighters, when a cybersecurity incident takes place, volunteer cyber forces can help organisations respond to cybersecurity incidents.

To be as useful as possible and given the sensitive environment in which they will operate, cyber volunteer forces tasked with cyber security-related roles must be: (1) tightly regulated, (2) carefully selected, and (3) properly trained.

2.1.1 Estonia

The cyber unit within Estonia's Defence League's (EDL) is a volunteer cyber force established already in 2011. The EDL is a volunteer national defence organisation originally founded in 1918 but re-established in 1990 following Estonian independence from the Soviet Union. The concept for the cyber unit was proposed in late 2007 following the events earlier that year when Estonia experienced large-scale politically motivated DDoS attacks originating from Russia.[42]

The purpose of the cyber unit is to enhance society's cybersecurity preparedness and defend Estonia's independence and constitutional order.[43] Its mission is the protection of

[42] Kadri Kaska, Anna-Maria Osula and Jan Stinissen, 'The Cyber Defence Unit of the Estonian Defence League: Legal, Policy and Organisational Analysis' (NATO Cooperative Cyber Defence Centre of Excellence, 2013) 7–9. The cyber unit was developed in the context of a history of close public-private sector collaboration in various ICT related initiatives from the late 1990s onward, such as in the development of the physical and digital infrastructure enabling electronic voting in 2005. Estonia's pre-existing cybersecurity collaboration networks positioned it mitigate the impact of the politically motivated 2007 DDoS attacks it experienced. See also Eneken Tikk, 'Civil Defence and Cyber Security: A Contemporary European Perspective' in Greg Austin (ed), *National Cyber Emergencies: The Return to Civil Defence* (Taylor & Francis, 2020) 86–7.

[43] Kaska, Osula and Stinissen (n 42) 11.

Estonia's 'high-tech way of life' through the protection of its ICT infrastructure and supporting national defence objectives.[44] It aims to do so through:

- raising society's awareness about cybersecurity threats;
- cybersecurity related information sharing among experts; and
- participation in crises management and the protection of critical infrastructure.[45]

In peacetime, its focus is on developing cybersecurity preparedness, and in crisis it provides support capabilities to the government.[46]

The EDL has a Commander under the direct control of the Commander of the Estonian Defence Forces. [47] The cyber unit is led by a commander who reports directly to the EDL commander. The cyber unit consists of sub-units (cells) responsible for the cyber unit's main operational capabilities. These include tasks relating to both passive and active cyber defence.[48]

The Estonian Emergency Act sets out the process for activating the EDL, and this is also applicable to the cyber unit. The cyber unit can be activated by an appropriate government body, such as the Estonian Information System Authority (which also houses Estonia's CERT), or the Estonian Defence Force Cyber Command.[49]

Estonian law provides requirements for membership of the EDL. Membership is only open to Estonian citizens over 18 years of age of good character. Prospective members must provide two existing members who act as referees, and these members are morally responsible for their suitability. In addition to active members of the cyber unit, the unit is also open to supporting members which includes non-Estonian citizens, and honorary members based on past achievements.[50]

Given the voluntary nature of the EDL and its cyber unit, members can decide whether or not to participate in its activities. But where a member takes up a duty of service, they are legally required to follow legitimate orders of superior staff until completion of the duty/task. Members are obliged to either wear uniform and insignia, or insignia on civilian attire when carrying out duties of service.[51]

[44] Ibid.
[45] See Estonian Defence League, 'Frequently Asked Questions' https://www.kaitseliit.ee/en/frequently-asked-questions (accessed 20 July 2025).
[46] Ibid.
[47] Kaska, Osula and Stinissen (n 42) 12.
[48] Ibid 14.
[49] Estonian Information System Authority (RIA), *Cyber Security in Estonia 2020* (November 2022) 36 https://www.ria.ee/sites/default/files/documents/2022-11/Cyber-Security-in-Estonia-2020.pdf (accessed 20 July 2025).
[50] Kaska, Osula and Stinissen (n 42) 15-16.
[51] Ibid 18-19.

2.1.2 Finland

Finland provides several interesting examples for how volunteer cyber capabilities may be structured and utilised. Here, we will focus on the Community Cyber Response Force (CCRF) which is known in Finnish as the 'Kyber VPK', and the National Defence Training Association of Finland.

The CCRF is a group of cybersecurity experts volunteering their expertise and skills to help the community. Its Finnish name translates to the 'cyber volunteer fire brigade', and the group's mission is to "extinguish[] cyber fires with community resources." [52] It was formed in March 2020 by private individuals during the COVID-19 pandemic in response to an increase in cybersecurity incidents. It was "established to help healthcare providers and providers of other critical services in resolving and preventing cyber threats." [53] Its founders, who include Finnish cyber experts working for leading IT companies, wanted to provide help to those who could not access it in the time of a cybersecurity incident or crisis.

The CCRF is not registered as any kind of organisation in Finland, and it simply operates as a group of volunteers in their individual capacities. The names and images of CCRF's members are included on its website as its founders wanted the public to see its members as real people providing assistance in the open (opposed to an anonymous group of cyber experts doing so in secret).

Where CCRF provides cybersecurity support to the community, members do so in their individual capacity. Many of its services are similar to consulting on cybersecurity, including checking an organisation's cybersecurity systems, data security, and so on. The CCRF also provides public awareness raising and training, for example in the form of public speaking engagements.

CCRF's members are a trusted circle of cyber experts, as opposed to an open organisation that anyone can join. Most members have long careers in the field, and many have completed cyber conscript training, [54] or are involved in other Defence related cyber activities and with the National Defence Training Association of Finland (detailed below).

There are three groups of CCRF members. The first is the steering committee which considers requests for

[52] KyberVPK, 'Frequently Asked Questions' https://kybervpk.fi/en/faq/ (accessed 20 July 2025).
[53] KyberVPK, 'Team Members' https://kybervpk.fi/en/people/ (accessed 20 July 2025).
[54] Finland has conscription and conscripts can apply to complete their military service in 'cyber conscript training.' Those chosen into this program must have pre-existing IT or related skills but receive training in a broad range of cybersecurity and defence related areas. On conscription in Finland generally, see Jarkko Kosonen and Juha Mälkki, 'The Finnish Model of Conscription: A Successful Policy to Organize National Defence' in Caroline de la Porte and others (eds), *Successful Public Policy in the Nordic Countries* (Oxford University Press, 2022).

help. When it decides to help an organisation, it can then pass that request on to the second group through a channel to its primary pool of volunteers from which people can decide to join. This is not a large pool of members, but a trusted circle of volunteers with cyber experience. The third group is a larger backup pool of individuals who have expressed interest to join the CCRF.

Despite initial concerns around a new not-for-profit like the CCRF, the Finnish government's response has been positive. An early incident that demonstrated CCRF's utility and gave it positive publicity was its response to the Vastaamo data breach in October 2020. Vastaamo is a Finnish psychotherapy service provider, and patient data was stolen with demands for ransom made to the company which it refused to pay. The CCRF was quick to respond and provide assistance to victims of the data breach, and it did so prior to the government. For example, it provided a 'checklist for victims of a data breach' containing instructions on how to limit the damage, and the government subsequently used and promoted the resource to others.[55]

The National Defence Training Association of Finland (MPK) plays a central role developing Finland's cybersecurity capability and includes a large degree of volunteer involvement. The MPK is a government funded organisation that coordinates Finland's voluntary national defence activities. Founded in 1993, the MPK provides military training, including for reservists, and training to prepare citizens for survival in 'dangerous situations in everyday life and under exceptional conditions.'[56] While core MPK personnel are government employees and the MPK works closely with the Department of Defence, most of those involved with the MPK as participants and instructors are volunteers. Training is open to all Finnish citizens over 15 years of age, while military training is only available to those over 18. Individuals can also enter into agreements committing to training and assignments provided by the Finnish Defence Forces and MPK, and Finland's voluntary national defence laws contain a number of obligations and entitlements.[57]

The MPK also plays a key role in developing Finland's cybersecurity capability. It provides training in cybersecurity at all levels, from 'cyber security for every citizen' courses with partner universities, to more advanced training for experts and cyber war game exercises. For example, the MPK selects

[55] See KyberVPK, 'Checklist for Victims of a Data Breach' (8 November 2020) https://kybervpk.fi/en/releases/checklist-for-victims-of-a-data-breach/ (accessed 20 July 2025).

[56] 'Maanpuolustuskoulutus MPK' (Maanpuolustuskoulutusyhdistys MPK, accessed 24 July 2025) https://mpk.fi/en/.

[57] See The Act on Voluntary National Defence (556/2007) (Finland) chs 6-7 https://finlex.fi/en/legislation/translations/2007/eng/556 (accessed 21 July 2025).

and trains the Finnish Locked Shields team, including the team that won the competition in 2022. Looking ahead, the MPK will also provide training to Finland's local cyber defence units. [58] Overall, through its activities, it facilitates the development of relationships and connections between volunteers from the cybersecurity community. These relationships extend across the public and private sectors, and with Defence, and contribute to Finland's cybersecurity preparedness.

2.1.3 Sweden

We have already described Sweden's Frivilliga radioorganisationen ('FRO') (the Voluntary Radio Organisation) above (see sections 1.3 and 1.5). As noted FRO plays a crucial role in building Sweden's cybersecurity structure,[59] and is now the lead organisation when it comes to cyber defence and cyber security amongst the volunteer defence organisations.[60]

2.1.4 United States of America

Work on volunteer cyber forces in the cyber security context can be found both on state-level and the Federal level in the US. Here, we focus on the Ohio Cyber Reserve as well as the developments on a Federal level.

2.1.4.1 State level civilian cyber reserves and the Ohio Cyber Reserve

A number of US states have volunteer cyber forces. The state of Michigan was the first to establish such a body with its Michigan Civilian Cyber Corps in 2013, and this structure was formalised in legislation in 2017.[61] Following Michigan, states including Wisconsin, [62] Ohio, Texas,[63] and Maryland[64] followed suit. In addition, several other states – including Oklahoma, Washington, Montana, Colorado, and West Virginia – are

[58] These units, consisting of cyber conscripts and volunteers, will be trained to assist local communities in cyber defence. See 'Uuden äärellä: Paikalliskyberpuolustuksen kenttäkoe Rovaniemellä' (Finnish Defence Forces, 8 September 2023) https://maavoimat.fi/-/uuden-aarella-paikalliskyberpuolustuksen-kenttakoe-rovaniemella- (accessed 21 July 2025).
[59] Frivilliga Radioorganisationen (FRO), *Grundstadgar* (Fastställda av FRO Riksstämma 2024) para 1.3 https://www.fro.se/_project/_media/FRODOK/FRODOK Publik/Dokument/FRO Grundstadgar.pdf (accessed 20 July 2025).
[60] Försvarsmakten (n 16).
[61] Michigan Compiled Laws, *Act 132 of 2017* (enacted 24 January 2018) https://www.legislature.mi.gov/documents/mcl/pdf/mcl-Act-132-of-2017.pdf (accessed 20 July 2025).
[62] Wisconsin Emergency Management, *Wisconsin Cyber Response Team* (webpage, 25 July 2025) https://wem.wi.gov/wisconsin-cyber-response-team.
[63] Texas Department of Information Resources, *Texas Volunteer Incident Response Team* (webpage, 25 July 2025) https://dir.texas.gov/information-security/cybersecurity-incident-management-and-reporting/texas-volunteer-incident.
[64] Cybersecurity and Infrastructure Security Agency, *Maryland Defense Force* (webpage, 25 July 2025) https://www.cisa.gov/resources-tools/services/maryland-defense-force.

launching or investigating options for cyber reserves.[65]

The Ohio Cyber Reserve (OhCR) stands out among these given the broad range of activities it engages in, and that it is placed under Ohio's National Guard. It was established in 2019 in response to a lack of resources and cybersecurity expertise among small government entities. [66] It has three core areas of activity:

- assisting organisations improve their cybersecurity practices, such as through cybersecurity audits;
- educating cybersecurity personnel in organisations, and supporting cyber education and clubs in schools; and
- responding to cybersecurity incidents against eligible entities.[67]

Entities eligible for OhCR assistance include government entities and critical infrastructure providers.

The OhCR was intentionally placed under the Ohio National Guard to take advantage of existing defence structures. Ohio's legal Code has existing provisions for its state defence forces, which include an army and a navy (despite Ohio only sharing a large lake at its border with Canada). [68] These provisions were largely replicated for a 'cyber' force, meaning the structure was familiar to local lawmakers, and members of the OhCR have access to a range of legal protections including the ability to take leave from their usual employment.[69] This showcases the type of advantages that may be gained by anchoring volunteer cyber forces in existing organisational and legal structures.

The OhCR has approximately 200 members and, for incident response, it generally operates in teams of three to four members. Anyone can apply to become a member through an online application, and applicants must conduct a SANS test and have their applications considered by a panel of existing OhCR members. On joining, members enter into a range of contractual agreements relating to their membership, including around non-disclosure and acceptable use of OhCR property. Further, as they are under the

[65] Cynthia Brumfield, 'Civilian Cyber Reserves Gaining Steam at the US Federal and State Levels' (24 January 2024) *CSO Online* https://www.csoonline.com/article/1297690/civilian-cyber-reserves-gaining-steam-at-the-us-federal-and-state-levels.html (accessed 20 July 2025).

[66] National Governors Association, *Re-Envisioning State Cyber Response Capabilities: The Role of Volunteers in Strengthening Our Systems* (June 2022) 11 https://www.nga.org/publications/re-envisioning-state-cyber-response-capabilities-the-role-of-volunteers-in-strengthening-our-systems/ (accessed 20 July 2025).

[67] See Ohio Cyber Reserve, 'About' https://ohcr.ohio.gov/about (accessed 20 July 2025); Ibid 11.

[68] See Ohio Revised Code, Title 59 – Veterans-Military Affairs, https://law.justia.com/codes/ohio/title-59/ (accessed 20 July 2025).

[69] National Governors Association (n 66) 11.

National Guard, members are subject to the Ohio Code of Military Justice.[70]

Given the OhCR is under the National Guard, the standard of training that members are required to have is high, and the OhCR training is validated by the US Department of Defense. This both helps ensure quality and works as an incentive for members. The Ohio Cyber Range plays a key role in facilitating this and is the only US state cyber range which uses the DOD methodology for training and exercises.[71]

Recent examples of incidents the OhCR has been deployed to respond to include in 2024 when the city of Cleveland was subject to a ransomware attack by Russian affiliated actors,[72] and in March 2025 in response to a cyber incident affecting the Cleveland municipal court.[73] These have improved the public awareness and perception of the OhCR. Outside of incident response, the other roles of the OhCR ensure its members can remain active and provide valuable support.

2.1.4.2 US Federal 'Civilian Cybersecurity Reserve' Pilot Program

In 2020, the US National Commission on Military, National, and Public Service recommended the creation of a pilot project establishing a 'federal civilian cybersecurity reserve.'[74] The purpose of this entity would be to allow US agencies to obtain additional cybersecurity capacity from cyber experts when they need. [75] The US Cyberspace Solarium Commission (CSC) also recommended that the US assess the establishment of 'military cyber reserve'. [76] According to the US CSC, the purpose of this entity would be to play a key role in mobilising surge capacity using existing links between the private sector and the government.[77]

Under the 'Department of Defense Civilian Cybersecurity Reserve Act' (US),

[70] Ohio Revised Code § 5924.02 (2024) https://law.justia.com/codes/ohio/title-59/chapter-5924/section-5924-02/ (accessed 20 July 2025).
[71] See Ohio Cyber Range Institute, *Capability Statement* (April 2023) https://www.ohiocyberrangeinstitute.org/_files/ugd/63659b_f99c01a55c4d40558896754bfc118483.pdf (accessed 20 July 2025).
[72] Glenn Forbes, Jeff St. Clair & Abbey Marshall, 'Cleveland Will Be Dealing with Fallout from June Cyber Attack for Weeks, Experts Say' (26 July 2024) *Ideastream Public Media* https://www.ideastream.org/government-politics/2024-07-26/cleveland-will-be-dealing-with-fallout-from-june-cyber-attack-for-weeks-experts-say (accessed 20 July 2025).
[73] Olivia Mitchell, 'Nat'l Guard Assisted on Cleveland Municipal Court Cyber Attack' (5 March 2025) *GovTech* https://www.govtech.com/security/natl-guard-assisted-on-cleveland-municipal-court-cyber-attack (accessed 20 July 2025).
[74] US National Commission on Military, National, and Public Service, *The Final Report of the National Commission on Military, National, and Public Service* (March 2020) 81.
[75] Ibid.
[76] US Cyberspace Solarium Commission, *Final Report* (March 2020) 117.
[77] Ibid. In its recommendations, the CSC maintained that the assessment of a cyber military reserve should explore, among other things, different types of reserve models (including less traditional and more flexible ones) and assess how to recruit members from the private sector and retain talent.

the Secretary of the Army will carry out a pilot project establishing a Civilian Cybersecurity Reserve. The purpose of the CCR is to is to "enable the Army to provide manpower to the United States Cyber Command" so it can effectively:

> "preempt, defeat, deter, or respond to malicious cyber activity; conduct cyberspace operations; secure information and systems of the Department of Defense against malicious cyber activity; and assist in solving cyber workforce-related challenges."[78]

Under this model, up to 50 members can be appointed to the CCR, [79] and appointed members will be considered Federal civil service employees only for the duration that they are part of the CCRA. Members must have cybersecurity expertise and will be screened to determine whether they require security clearances (and Army will sponsor the cost of obtaining that clearance if it is required). The pilot must be established within 2 years (i.e. between 2025-2026) and will be followed by a report with recommendations about:

> "(A) whether the pilot project should be modified, extended in duration, or established as a permanent program, and if so, an appropriate scope for the program; (B) how to attract participants, ensure a diversity of participants, and address any barriers to recruitment or retention of members of the Civilian Cybersecurity Reserve; (C) the ethical requirements of the pilot project and the effectiveness of mitigation efforts to address any conflict of interest concerns; and (D) an evaluation of the eligibility requirements for the pilot project."[80]

2.1.5 'Cybersecurity citizen guardians'

In addition to the highly organised cybersecurity-focused volunteer forces discussed so far – what we may call 'the cybersecurity reserve' – one may also picture structures for harnessing a broader range of volunteers in times of serious crisis. Planning for such a measure ought to be carried out already prior to such a crisis arising. One may, for example, picture a structure under which people who are not ready, or willing, to take the step of signing up to the cybersecurity reserve may nevertheless register on a list to form part of a unit of 'cybersecurity citizen guardians'. In doing so, they should also register their respective areas of expertise.

[78] Department of Defense Civilian Cybersecurity Reserve Act, S 903, 118th Congress, § 2 (2023) https://www.congress.gov/bill/118th-congress/senate-bill/903/text (accessed 20 July 2025).
[79] Ibid.
[80] Ibid.

While the criteria to sign up for the cybersecurity citizen guardians ought to be lower than to join the cybersecurity reserve, some vetting is nevertheless appropriate, and the members ought to receive access to periodic training. Where members are properly vetted and trained, they could then be provided with various support roles helping to keep computer systems available and running in a time of serious crisis. For example, on its most basic level, a cybersecurity citizen guardians unit could play a role in helping ensure that citizens in their local area maintain Internet access through home networks or the networks of institutions such as local libraries in a time of crisis.[81] Obviously, however, the support of sensitive systems must be kept in the hands of employed experts or at least the cybersecurity reserve.

Finally, one could imagine a structure under which the cybersecurity reserve took on a training and coordination role for the cybersecurity citizen guardians. This ties into the idea of creating a 'cyber capacity eco-system'.

The noted volunteer cyber forces may contribute both to protection and resilience. Indeed, we would argue that the type of resilience that volunteer cyber forces can provide is a form of deterrence as it lowers the likelihood that cyber-attacks are effective and thus may discourage them in the first place.

2.2 Open-source intelligence (OSINT)

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." [82] One consequence of the information explosion that has occurred over recent years, not least due to the Internet, is that much information of national security interest may now be obtained 'open-source' via so-called open-source intelligence; that is, the collection and analysis of intelligence from publicly available sources. As observed in the recent US 'IC OSINT Strategy 2024-2026':

> "OSINT is vital to the Intelligence Community's Mission. OSINT both enables other intelligence collection disciplines and delivers unique intelligence value of its own, allowing the IC to more efficiently and effectively leverage its exquisite collection capabilities. As the open source environment continues to expand and evolve at breakneck speed, the ability to extract actionable

[81] US Cyberspace Solarium Commission, *Building a Trusted ICT Supply Chain* (Report, October 2021) 16.

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

> insights from vast amounts of open source data will only increase in importance."[83]

A volunteer cyber force can be an important component in open-source intelligence work. This is also highlighted in Australia's *2024 Independent Intelligence Review* which notes the growing importance of OSINT capabilities and role of, for example, civilian OSINT investigators as 'pacesetters' in this context.[84]

Traditional online OSINT resources include, for example, image searches, satellite image maps, flight radar trackers, and social media. Insights gained from such data may be of value both in times of war, and outside war. As the amount of data posted online by both combatants and civilians continues to increase, the role of OSINT is amplified as such content may, for example, reveal enemy positions and troop movements. In war, the OSINT role of a volunteer cyber force may e.g., also facilitate the estimation of enemy casualties based on social media postings – a resource-intensive task requiring comparatively low-level OSINT skills.

A volunteer cyber force in the OSINT role could be given specific tasks such as being invited to go through certain materials, potentially with specific aims in mind. Alternatively, it could be given a broader investigative role utilising the volunteers' creativity. Both approaches are associated with advantages and disadvantages. However, the value that may be added to Australia's intelligence community should not be ignore.

Further, volunteer cyber forces may support evidence-gathering to be used in the future prosecution of war criminals. Even in the early stages of the 2022 Russian invasion of Ukraine, for example, it was reported that Ukraine's Digital Ministry created, and made public, a range of digital tools to crowdsource and corroborate evidence of alleged war crimes.[85] It is still too early to draw any extensive conclusions from the Ukrainian measures in this respect; much of the evidence collected is yet to be tested in court. But it is already obvious that this type of evidence collection also requires, or at least benefits from, training to ensure that the evidence is collected in a manner that enables the use of the evidence in legal procedures.

---

[83] Ibid.

[84] Commonwealth of Australia, Department of the Prime Minister and Cabinet, *2024 Independent Intelligence Review* (Report, 2024) 87 https://www.pmc.gov.au/sites/default/files/resource/download/2024-independent-intelligence-review.pdf.

[85] Vera Bergengruen, 'How Ukraine Is Crowdsourcing Digital Evidence of War Crimes' (*Time*, 18 April 2022) https://time.com/6166781/ukraine-crowdsourcing-war-crimes/.

A cyber volunteer force operating in the OSINT role may both be a deterrent (hostile activities are more likely to be discovered and recorded, for example) and may facilitate greater protection and resilience. Thus, we recommend Australia should take steps to develop a cyber volunteer capability operating in the OSINT role.

The possible structures for such a force are discussed below (see section 3). However, one specific initiative from the examined States addressed in this study may be highlighted; namely the Swedish Defence Research Agency's collective intelligence initiative 'Glimt' (glimt.nu).

2.2.1 The Swedish Defence Research Agency's crowd forecasting 'Glimt'

Launched in January 2025, 'Glimt'[86] is a crowd forecasting platform operated by the Swedish Defence Research Agency (FOI) in collaboration with the Ukrainian government. On this platform, volunteer contributors are invited to make forecasts in relation to topics that may inform the Ukrainian government.

Some questions are binary yes or no, such as "Will the US use its armed forces in an attack against Iran before June 1, 2025?". Others are more complex with multiple options, such as "How many missile attacks will Russia launch against Ukraine in May, 2025" with the possible answers being <50, 50-100, 100-150, 150-200 or 200-300.

Regardless of the type of question, the forecaster is required to attribute a percentage estimate for their forecast adding up to a total of 100 percent. In addition, text boxes are provided in which the forecaster can indicate why they think they are right, what would make them change their mind, and any relevant URLs they have relied upon in making their forecast.

Crowd forecasting is an established method. Calls for implementing crowd forecasting in intelligence work can be found also in some other States,[87] and Australia ought to consider harnessing crowd forecasting in its intelligence structures.

Beyond the obvious intelligence benefits, adopting a crowd forecasting platform may have additional benefits. For example, engagement with a crowd forecasting platform focused on matters of defence may increase the Australian public's general consciousness of the issues involved and ultimately raise the will to defend Australia. Additionally, such a platform may identify particularly

[86] Totalförsvarets forskningsinstitut (FOI), *Glimt – vå Our new weapon* (Glimt digital platform, launched January 2025) https://glimt.nu/ (accessed 20 July 2025).
[87] See e.g.: Federation of American Scientists, *Collaborative Intelligence: Harnessing Crowd Forecasting for National Security* (Policy Memo, 27 November 2024) https://fas.org/publication/collaborative-intelligence-harnessing-crowd-forecasting-for-national-security/ (accessed 20 July 2025).

gifted individuals and may serve as a recruitment tool.

2.3 Information and cognitive conflict

The recently released United Nations Global Risk Report describes how stakeholders from around the world perceive global risks and assess the multilateral system's readiness to address them. Drawing on data from 2024, it notes that:

> "One vulnerability clearly stands out: mis- and disinformation. It is perceived as an extremely important risk for which the international community is not prepared, with the potential to exacerbate geopolitical tensions, societal discord and crisis response challenges."[88]

While information and cognitive warfare is a concern for Australia's military defence, it is not exclusively a military concern. Rather, defending against, and responding to, information and cognitive warfare is a whole-of-society concern.

Australia, like most States, is subject to constant information and cognitive campaigns initiated, or directed, by foreign actors. It has also been noted that, thanks to technological developments, hostile actors have more options available than ever before to influence opinions and processes in foreign states.[89] And their appetite for doing so is not in doubt.

Russia, for example, has a long history of propaganda and disinformation operations, and it has been noted that the Russian leadership sees "the information domain as vital to modern warfare".[90] In this context, a June 2024 report by the Foundation for Defense of Democracies (FDD) notes that: "Washington is also struggling in the battle for hearts and minds in the "Global South," where Russian propaganda outlets are often more popular than Western media."[91] In the light of several actions taken by the current US administration, this concern has no doubt been exacerbated. Australia's thinking in the information and cognitive domain must consequently not only consider the Australian environment, but must take account of our entire region, and beyond.

---

[88] United Nations Executive Office of the Secretary-General, *UN Global Risk Report* (Report, February 2024) 16 https://unglobalriskreport.org/UNHQ-GlobalRiskReport-WEB-FIN.pdf (accessed 20 July 2025).

[89] 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.

[90] Ivana Stradner and John Hardie, 'Russia', in Bradley Bowman (ed), *Cognitive Combat: China, Russia, and Iran's Information War Against Americans* (Foundation for Defense of Democracies, 2024) 21.

[91] Ibid 24.

In December, the US Department of Defense released the 2024 edition of its annual report on Military and Security Developments Involving the People's Republic of China. One of the many important observations made in the Report, relates to how the People's Liberation Army (PLA) concept of "cognitive domain operations" (CDO) combines psychological warfare with cyber operations to shape the behaviour and decision-making of China's adversaries:

> "The PLA has recognized the importance of incorporating emerging technologies, such as AI, big data, brain science, and neuroscience into CDO as the PLA perceives that these technologies will lead to profound changes in the ability to subvert human cognition. The goal of CDO is to achieve what the PLA refers to as "mind dominance," which the PLA defines as the use of information to influence public opinion to affect change in a nation's social system, likely to create an environment favorable to the PRC and reduce civilian and military resistance to PLA actions. The PLA probably intends to use CDO as an asymmetric capability to deter U.S. or third-party entry into a potential conflict, or as an offensive capability to shape perceptions or polarize a society. Authoritative PLA documents describe one aspect of deterrence as the ability to bring about psychological pressure and fear on an opponent and force them to surrender. PLA articles on CDO state that seizing mind dominance in the cognitive domain and subduing the enemy without fighting is the highest realm of warfare."[92]

To this may be added that:

> "China also maintains a 20 million-strong army of Chinese netizens, known as "network civilization volunteers," to support its digital disinformation efforts. These individuals wage the CCP's "online ideological struggle" [...] by amplifying online voices complimentary of China and suppressing those deemed "negative.""[93]

At a time when States such as China and Russia are increasing their efforts to influence our societies, we must ask whether we in the democratic countries in the world are doing enough to protect ourselves. In this context, we note the debates about Australia's abandoned Communications Legislation

[92] U.S. Department of Defense, *Military and Security Developments Involving the People's Republic of China* (Report, 18 December 2024) 38 https://media.defense.gov/2024/Dec/18/2003615520/-1/-1/0/MILITARY-AND-SECURITY-DEVELOPMENTS-INVOLVING-THE-PEOPLES-REPUBLIC-OF-CHINA-2024.PDF (accessed 20 July 2025).

[93] Singleton (n 21) 16.

Amendment (Combatting Misinformation and Disinformation) Bill 2024 as well as the fact that the US closed down its Global Engagement Center on 23 December 2024. Up until then, the Global Engagement Center worked to:

> "direct, lead, synchronize, integrate, and coordinate U.S. Federal Government efforts to recognize, understand, expose, and counter foreign state and non-state propaganda and disinformation efforts aimed at undermining or influencing the policies, security, or stability of the United States, its allies, and partner nations."[94]

An important task indeed. And one that is unlikely to become irrelevant any time soon.

A volunteer cyber force may be a potent tool – although admittedly not the 'silver bullet' and only amounting to one of the steps that ought to be taken – in addressing these issues.[95] Indeed, they may be a valuable tool both for defensive and proactive information warfare.

An Australian cyber volunteer capability could be equipped to counter foreign information warfare by providing both Australians and the outside world with a continuous flow of up-to-date, factual, and verified information. While this is significant in times of peace and hybrid warfare, it is even more critical in the case of armed conflict.

Finally, it may be noted that a properly structured volunteer cyber force in the information conflict arena may create a certain distance between the government and the audience to which the volunteer cyber force communicates, thereby helping create credibility and avoid a perception that a government with a specific political agenda interferes with free speech.

2.3.1 Ukraine

Looking at the role of information warfare, the Russian war against Ukraine is highly illustrative. Without in any sense downplaying or undermining the importance of the Ukrainian military, it may be argued that the current war may be won or lost in the arena of public opinion of the (mainly Western) states supplying weapons and other forms of support to Ukraine.

A volunteer cyber force can be used to steer the narrative, to fact-check, and to point out inaccuracies in, and counter, enemy propaganda. Already in 2023, Russia, for example, tried to use its announced (but not upheld) unilateral 36-hour ceasefire in observance of Orthodox Christmas celebrations as a propaganda tool to tarnish the Ukrainian

[94] 'About Us – Global Engagement Center' (United States Department of State, accessed 24 July 2025) https://2021-2025.state.gov/about-us-global-engagement-center-2/.

[95] See e.g. initiatives such as Debunk, 'The Elves' https://www.debunk.org/about-elves (accessed 20 July 2025).

reputation on the international stage.[96] A volunteer cyber force can play a central role in directing the narrative to counter such propaganda, especially in the influential arena of social media.

States organising a volunteer cyber force for such purposes ought to train the members on the propaganda methods of potential adversaries. Relatedly, as highlighted by the debate associated with the highly controversial Amnesty International report published on August 4, 2022,[97] a volunteer cyber force ought to be equipped to monitor the publications of key international bodies and be prepared to present a counter-narrative where it is justified to do so. This requires specialised training.

Discussing information warfare in the Ukraine context, it would be remiss not to mention the so-called North Atlantic Fella Organization. NAFO:

> "is an organic online group of pro-Ukraine supporters that have gained the attention of policymakers and global leaders for their creative use of digital media to take on key sources of Russian disinformation and raise support for the war effort in Ukraine".[98]

The work of NAFO is illustrative of some roles that a volunteer cyber force could play even though NAFO, as currently utilised, may not necessarily fit the definition of a volunteer cyber force.

Effective information warfare capabilities, to which a volunteer cyber force clearly may contribute, may arguably serve all three of the ways noted above that a state can protect society in the cyber domain.

In the context of the Russian war against Ukraine, examples may also be found of potential proactive roles for a volunteer cyber force in information warfare. For example, in the early stages of the full-scale Russian attack – at a time the world still assumed that the general Russian public was unaware of what was being done in their name in Ukraine – there was a campaign to post information about the invasion on various hotel and restaurant review websites in Russia. This is a simple yet clear illustration of the types of proactive measures a volunteer cyber force can undertake in information warfare.

---

[96] Karolina Hird et al, 'Russian Offensive Campaign Assessment, 5 January 2023' (Institute for the Study of War, 5 January 2023) https://www.understandingwar.org/backgrounder/russian-offensive-campaign-assessment-january-5-2023.

[97] Amnesty International, 'Ukraine: Ukrainian Fighting Tactics Endanger Civilians' (4 August 2022) https://www.amnesty.org/en/latest/news/2022/08/ukraine-ukrainian-fighting-tactics-endanger-civilians/.

[98] Kathleen McInnis, Seth G Jones and Emily Harding, 'NAFO and Winning the Information War: Lessons Learned from Ukraine' (Center for Strategic and International Studies, 5 October 2022) https://www.csis.org/analysis/nafo-and-winning-information-war-lessons-learned-ukraine.

2.3.2 Taiwan

Taiwan has extensive experience of dealing with information campaigns conducted primarily by the PRC. However, instead of any outright ban or heavy censorship of media outlets or platforms known to spread mis- and dis-information[99] (for instance, TikTok, which affiliated to its Chinese parent company ByteDance), [100] Taiwan resorts to "an arsenal of defenses, including a deep network of independent fact-checking organizations" [101] as well as legislative measures that tackle various forms of threats online that apply across all social media platforms. Thus, rather than letting internet service providers regulate harmful content, or take a more draconian approach to government regulation of online content, Taiwan's experience offers a third possibility to combat mis- and dis-information, which in essence is the government allowing "civil society to take the lead" and then "supplemented and strengthened citizens' actions to confront fake news instead of trying to replace them".[102] This approach to combating mis- and dis-information has been termed "an embodiment of civic constitutionalism", which involves interaction between the state, market and cooperating with "empowered citizen, instead of either entirely trusting or restraining industry".[103]

In 2018, the government issued a "Report on Preventing the Hazards of Fake News", which highlights four strategies to combat mis- and dis-information, namely:

> "(1) enhancing citizens' media literacy and judgment, (2) creating mechanisms for clarification and third-party fact-checking, (3) collaborating with media platforms, and (4) holding individuals accountable for fake news through fair and independent judicial review".[104]

[99] Foundation for Defense of Democracies, '5 Things to Know About ByteDance, TikTok's Parent Company' (12 March 2024) https://www.fdd.org/analysis/2024/03/12/5-things-to-know-about-bytedance-tiktoks-parent-company/.

[100] 'EU Bans Distribution of Four Russian Media Outlets', *Reuters* (18 May 2024) https://www.reuters.com/world/europe/eu-bans-distribution-four-russian-news-outlets-2024-05-17/.

[101] Meaghan Tobin and Amy Chang Chien, 'Taiwan, on China's Doorstep, Is Dealing with TikTok Its Own Way', *The New York Times* (16 May 2024) https://www.nytimes.com/2024/05/16/business/tiktok-taiwan.html.

[102] Wen-Chen Chang and Yu-Teng Ling, 'A Civil Society-Based Approach to Online Misinformation: The Experience of Taiwan' (*US-Asia Law Institute*, 19 February 2024) https://usali.org/usali-perspectives-blog/a-civil-society-based-approach-to-online-misinformation.

[103] Ibid.

[104] Taiwan Executive Yuan, 'Measures to Prevent the Harm of Misinformation' (防制假訊息危害因應作為) (in Chinese) (Executive Yuan, accessed 24 July 2025) https://www.ey.gov.tw/Page/448DE008087A1971/c38a3843-aaf7-45dd-aa4a-91f913c91559.

Taiwan harnesses the synergy of public-private collaboration in countering mis- and dis-information.[105] The involvement of civil society institutions and NGOs helps allay fears of government censorship or overreach and can help dispel concerns about partisan bias. Further, such public-private synergy can "enhance speed and innovation in combating disinformation".[106] During the 2024 presidential elections, for example, various government agencies collaborated with tech media platforms and independent fact-checking organisations to flag, verify and, when necessary, take down mis- and dis-information that may jeopardise election integrity.[107]

Increased government transparency is yet another approach to fighting mis- and dis-information. For instance, the group g0v,[108] which has its roots in the 2014 student demonstrations against government attempts to bypass parliament, aims to foster greater government transparency and citizen participation in governance. Collaboration between volunteer hackers and the government through g0v enables digital technology to quickly respond to mis- and dis-information, as well as foster social trust and cohesion.[109]

Grassroots civil society initiatives are demonstrating their ability to fight against mis- and dis-information. [110] Such organisations have appeared to engage in outreach and education campaigns to help citizens identify and distinguish between fact and rumours.[111] For instance, Cofacts[112] is a civic-tech project under the g0v (gov-

[105] Yang Kuang-shun, 'What Lessons Can Taiwan Share with the World on Election Interference?' (*Brookings Institution*, 11 June 2024) https://www.brookings.edu/articles/what-lessons-can-taiwan-share-with-the-world-on-election-interference/.

[106] Ibid.

[107] See 'Defending Election Integrity in Taiwan' (August 2020) https://www.tca.org.tw/files/Facebook%20Taiwan%20Election%20Report%20ENG.pdf.

[108] g0v Taiwan, 'About g0v' (accessed 24 July 2025) https://g0v.tw/intl/en/.

[109] Dan Holmes, 'Taiwan is Building a Government AI Hivemind', *The Mandarin* (21 August 2024) https://www.themandarin.com.au/253059-taiwan-is-building-a-government-ai-hivemind/.

[110] Jude Blanchette *et al*, *Protecting Democracy in an Age of Disinformation: Lessons from Taiwan* (Center for Strategic and International Studies, 2021) 19
'Just as the freedoms inherent in a democratic society make it uniquely vulnerable to disinformation, so too does a healthy and robust democratic civil society empower volunteer citizens, companies, and organizations to unite and respond to disinformation attacks.'
See also Chiaoning Su and Wei-Ping Li, 'Three Musketeers Against Mis/Disinformation: Assessing Citizen-Led Fact-Checking Practices in Taiwan' (31 March 2023) https://taiwaninsight.org/2023/03/31/three-musketeers-against-mis-disinformation-assessing-citizen-led-fact-checking-practices-in-taiwan/.

[111] Even former US Secretary of State Blinken cited Taiwan's success in teaching. See Antony Blinken, 'Summit for Democracy Speech on Building a More Resilient Information Environment' (Speech, 2024 Summit for Democracy, 2024) https://www.americanrhetoric.com/speeches/antonyblinkensummitfordemocracy2024.htm (accessed 24 July 2025).

[112] Cofacts, 'Homepage' (accessed 24 July 2025) https://cofacts.tw/.

zero) initiative. The platform is fully open-source and decentralised, with all data and code publicly accessible. The transparency help improve accuracy, and the 'gamification' included helps keep volunteers engaged.

Another example is found in Taiwan FactCheck Center.[113] It is a non-profit NGO established in 2018 which aims to combat disinformation, "improve public information literacy, and safeguard the trust principles essential for democratic operations".[114] It has organised workshops to educate journalists and equip them with the tools and knowhow to identify, for instance, AI-generated mis- and dis-information.[115] MyGoPen[116] (Taiwanese for "Don't lie anymore") was established by someone who was concerned about rumours spread by relatives and elders.[117]

The app Auntie Meiyu[118] can be integrated in chat messages on the popular application called LINE, which can scan and verify whether there is misleading content.[119]

In addition, the government is credited with using innovative new tools, such as using "engaging and memetic content" to push back on mis- and dis-information.[120] The approach has been described as "2-2-2 humour over rumour", pioneered by former Taiwan Digital Minister Audrey Tang. The premise is to respond to mis- and dis-information within 20 minutes, in 200 words or less using two fun images.[121]

---

[113] Taiwan FactCheck Center, *Taiwan FactCheck Foundation (English Website)* (webpage, 25 July 2025) https://en.tfc-taiwan.org.tw/.
[114] Taiwan FactCheck Center, *Who We Are* (webpage, 25 July 2025) https://en.tfc-taiwan.org.tw/en_tfc_298/.
[115] Taiwan FactCheck Center, *2024 Presidential Election: Combating Disinformation with Fact-Checks, Media Collaboration, and Public Empowerment* (webpage, 25 December 2023) https://en.tfc-taiwan.org.tw/en_tfc_288/.
[116] MyGoPen, *MyGoPen ／麥擱騙* (webpage, 25 July 2025) https://www.mygopen.com/.
[117] PBS, *How Taiwan Preserved Election Integrity by Fighting Back Against Disinformation* (27 January 2024) https://www.pbs.org/newshour/world/how-taiwan-preserved-election-integrity-by-fighting-back-against-disinformation ('Taiwan adopted a multifaceted approach, what Thibaut called a "whole of society response" that relied on government, independent fact-check groups and even private citizens to call out disinformation and propaganda').
[118] CheckCheck .me, *Auntie Meiyu, your trusted fact-checking confidant* (webpage, 25 July 2025) https://www.checkcheck.me/en/.
[119] Eric Cheung, *Taiwan faces a flood of disinformation from China ahead of crucial election. Here's how it's fighting back* (CNN, 15 December 2023) https://edition.cnn.com/2023/12/15/asia/taiwan-election-disinformation-china-technology-intl-hnk/index.html ('Taiwan's most popular messaging app, a chatbot replied that the claim was not supported by science, with a link to an article that fact-checked this erroneous information').
[120] Blanchette et al (n 110) 16.
[121] Arwa Mahdawi, 'Humour over Rumour? The World Can Learn a Lot from Taiwan's Approach to Fake News' (17 February 2021) *The Guardian* https://www.theguardian.com/commentisfree/2021/feb/17/humour-over-rumour-taiwan-fake-news. See also 'Is Humour the Key to Better AI Governance? Audrey Tang Thinks So', *Apolitical* (25 February 2025) https://apolitical.co/solution-articles/en/is-humour-the-key-to-better-ai-governance-audrey-tang-thinks-so.

Such a "proactive stance in narrative building" does more than react to or refute mis- and dis-information; working with fact-checking institutions, the government can take a collaborative approach in constructing and disseminating counternarratives and more accurate information (instead of top-down, government-imposed censorship).[122]

Furthermore, in addition to civil society initiatives, the government has attempted to strengthen legal prohibitions which can be used to debunk mis- and dis-information and accompanied with more stringent penalties or prison sentences. [123] However, underlining the fine balancing act between the constant concern of the government's wish to crack down on mis- and dis-information, and the freedoms of information and expression, which are the cornerstones of a free and democratic society remains important.[124]

2.3.3 Estonia

Estonia's 'Propastop' is a volunteer run online blog aimed at countering anti-Estonian propaganda. It provides fact-checking and analysis of material from various sources, including traditional and social media. The editors and those contributing to the blog are not named for security reasons, but many of those involved are members of the Estonian Defence League and its cyber unit.[125]

2.3.4 Defensive and proactive measures in information conflicts

From the above, it is clear that several States have adopted defensive structures aimed at addressing information conflicts. Importantly, however, it is also clear that several States have adopted proactive structures for such situations. Indeed, the overall picture that emerges seems to be that defensive structures are not enough and that also proactive structures are needed.

The noted June 2024 report by the FDD makes the important observation that the primary information warfare focus of the leadership in China, Russia, and Iran is placed on its own population.[126] In this context, the same report also notes the potential for democratic States to adopt coordinated offensive information warfare operations in these dictatorships so as to:

[122] Kritvi Gupta, 'Beyond Censorship: Taiwan's Model for Combating Disinformation' (14 March 2024) *Foreign Affairs Review* https://www.foreignaffairsreview.com/home/beyond-censorship-taiwans-model-for-combating-disinformation.
[123] Blanchette et al (n 110) 17.
[124] Gupta (n 122).
[125] Propastop, 'What is Propastop' (webpage, 21 July 2025) https://www.propastop.org/en/en-about.
[126] Bradley Bowman (ed), *Cognitive Combat: China, Russia, and Iran's Information War Against Americans* (Foundation for Defense of Democracies, 2024) 32.

> "systematically expose each regime's corruption and oppression and help the Chinese, Russian, and Iranian people advocate for their own rights, including more representative governance."[127]

This same sentiment is also found in a May 2025 report published by the Swedish Psychological Defence Agency:

> "The Kremlin is also desperate to avoid fighting an information war in the information environment of the Russian Federation. If we take the information war to Russian Federation information environment, resources will have to be displaced from the "foreign front" to protect the homeland."[128]

It is important to note that the Swedish Psychological Defence Agency does not necessarily endorse this proposal. However, it highlights that there is an ongoing discussion of the extent to which proactive measures are necessary in the information conflict arena, and it is clear that such measures may bring at least two important advantages. Proactive information warfare operations may:

- Force hostile States to redirect their efforts in the information and cognitive warfare space at defensive measures in their own information environment which after all is their key focus; and
- Convince hostile States that offensive information warfare operations aimed at democratic States will be met with responses that are too costly for the hostile States.

At the same time, it must be acknowledged that proactive measures may give rise to different types of legal issues both under domestic law and under international law. We discuss those issues below (see section 5). Here it suffices to note that proactive information warfare operations aimed at exposing corruption and oppression in dictatorships such as Russia and China need only engage in providing information, *not* disinformation. Having the ability to keep to communicating truthful messages have powerful legitimating effects.

It has also been noted that opponents to proactive measures in the information warfare domain point to the risk of escalation. However, as Bowman points out, the authoritarian States clearly are unconcerned about their operations causing escalation. Furthermore, the escalation concerns:

[127] Ibid 33–35. In this context, one may envisage synergies between investigative journalism focused on exposing corruption, oppression, and human rights abuses on the one hand, and volunteer cyber forces helping to spread the findings on the other hand. This illustrates our earlier point about viewing volunteer cyber forces as parts of an ecosystem.

[128] Pamment and Tsurtsumia, *Beyond Operation Doppelgänger: A Capability Assessment of the Social Design Agency* (12 May 2025) 194.

> "must be weighed against the dangers associated with accepting the status quo in which China, Russia, and Iran are targeting with increasing ferocity and AI-empowered effectiveness the socio-political foundations upon which American [and other State's] unity, stability, liberty, and security stands."[129]

2.4 Espionage

Beyond the OSINT roles discussed above, there is some potential for a volunteer cyber force to engage in the active production of new intelligence through what may potentially amount to espionage. The means for such tasks may range from unlawful access to computer systems to the use of private drones.

Examples from overseas include instances of people gaining access to security cameras allowing the planning of kinetic attacks as well as tracking of troop movement. With an increase in the uptake of Internet of Things (IoT), this type of activity will potentially increase in potency. With millions of poorly protected IoT devices in use, the 'hacking' skills required are at the lower end of the scale. Quantity may then matter more than quality which favours a volunteer cyber force.

While it is clear that volunteer cyber forces are capable of carrying out tasks in the field of espionage, great care must be taken in respect of the risks to which the volunteers may be exposed. Espionage is a complex legal area as we discuss further below (see section 5).

2.5 Proactive cyber operations ("Cyber attacks")

An Australian cyber volunteer capability could potentially be trained to be used to carry out what broadly may be termed 'proactive cyber operations', including 'cyber-attacks' against designated targets and 'hack back' in response to attacks. Such attacks may range from relatively simple denial-of-service attacks to more sophisticated attacks that qualify as 'attacks' under international humanitarian law.

A State's ability to deploy a volunteer cyber force undertaking targeted cyber-attacks may be a significant deterrent for a potential attacker. However, at the same time, solid training, clear limits, and careful oversight is a necessity.

2.5.1 Ukraine

As illustrated by the Ukrainian IT Army, a volunteer cyber force may be utilised for the purpose of carrying out cyber-attacks, such as distributed denial-of-service (DDoS) attacks, for example,

[129] Bowman (n 126) 33.

against designated targets.[130] In the case of Ukraine, already in May of 2022 the Ministry of Digital Transformation claimed that since the Russian 2022 invasion of Ukraine, the Ukrainian IT Army had attacked some 2,000 Russian resources.[131]

Interestingly, it has been reported that cyber criminals that might ordinarily have avoided Russian targets have now directed their efforts at Russia – not for any geopolitical reasons, but, rather, due to the fact that Russian defenses are occupied with war-related cyber attacks and are therefore less able to defend against conventional cybercrime.[132] This is not to condone cybercrime; it is to simply highlight the undeniable potential synergies between war-related attacks and conventional cybercrime: each may benefit from the other's impact on the target's capacity to defend itself.

In the context of the Russian war against Ukraine,[133] the activity of the "Belarusian Cyber Partisans" is also illustrative. It has been reported that this Belarus-based hacktivist group managed to encrypt certain servers, databases, and workstations of the train company Belarusian Railway to interfere with Russian troop movements in Belarus.[134] Without entering any debate about whether the Belarusian Cyber Partisans fit within any definition of a volunteer cyber force, this highlights the diversity of types of cyber attacks in which a volunteer cyber force may engage.

2.5.2 Sweden's free war approach ('Det fria kriget')

'Det fria kriget' – or 'the free war' – is a Swedish military doctrine providing instructions for how military personnel is to act in a situation where Sweden has been invaded by a superior force with the result that conventional war fighting is no longer possible. Smaller units are to carry on fighting predominantly using guerrilla warfare tactics.

While this doctrine was developed only for military personnel, and even though it pre-dates cyber conflicts, one may wonder whether a similar thinking may be applied in the cyber context, and

[130] Stefan Soesanto, *The IT Army of Ukraine: Structure, Tasking, and Ecosystem* (Report, Centre for Security Studies, 2022) 4 https://css.ethz.ch/en/publications/risk-and-resilience-reports/details.html?id=/t/h/e/i/the_it_army_of_ukraine.

[131] Ibid 7.

[132] Joseph Menn, 'Hacking Russia Was Off-Limits. The Ukraine War Made It a Free-for-All' *Washington Post* (online, 1 May 2022) https://www.washingtonpost.com/technology/2022/05/01/russia-cyber-attacks-hacking/.

[133] For an overview of the cyber warfare aimed at Ukraine, see: *Cyber Forum Kyiv*, *A Decade in the Trenches of Cyberwarfare: An Overview of Cyber Operations Targeting Ukraine* (Report, Cyber Forum Kyiv) https://cyberforumkyiv.org/A_Decade_in_the_Trenches_of_Cyberwarfare.pdf

[134] Ann Väljataga, 'Cyber Vigilantism in Support of Ukraine: A Legal Analysis' (Report, NATO Cooperative Cyber Defence Centre of Excellence, March 2022) 1 https://ccdcoe.org/uploads/2022/04/Cyber-vigilantism-in-support-of-Ukraine-a-legal-analysis.pdf (accessed 21 July 2025).

more broadly, also to non-military personnel like members of a volunteer cyber force. After all, the reality is that in a crisis situation, and especially during war, communications may be interrupted, and conventional structures may break down. Perhaps it would be prudent to have a ‘cyber free war doctrine’ in place for such a situation, not least for the purpose of ensuring that the principles of international humanitarian law are upheld by the units and persons who must continue the fight without close supervision.

3. Structural questions

There are many structural considerations that must be addressed if Australia is to adopt some form of volunteer cyber forces. In this section, we seek to highlight and bring attention to the key considerations. Doing so is complicated by the fact that – as has been emphasised repeatedly – we are discussing a range of potentially quite different types of volunteer cyber forces, each with their own structural considerations.

But before we address the many structural considerations of concern, it is worthwhile to first make some observations as to how Australia may motivate people to join any cyber volunteer initiatives in the first place.

3.1 Building resilience, and the will to defend, in the population

Would Australians be willing to devote time to a volunteer cyber force? Obviously, continued work on the creation of such a capability could make use of a survey to ascertain the answer to such a question, and related questions like the time-commitment volunteers may be willing to make, possible tasks volunteers are willing to engage in etc.

We can only speculate and note that Australians have a proud tradition of volunteering and that perhaps that may be the case also in relation to volunteer cyber forces. Experiences from the States examined for this Report suggests that the sense amongst volunteers of making a valuable contribution to national defence can be enhanced via an emphasis on the 'military element' of the activities. An even more important factor may be the offering of training opportunities. Obviously, it is also important to foster camaraderie amongst the volunteers. Such a focus may not only help ensure that the volunteers stay engaged but may also be of great importance in a time of crisis.

With all this in mind, there seems to be reasons to be optimistic as to the willingness of Australians to contribute to volunteer cyber forces. At the same time, Australia's history and geographical position may have contributed to a sense that conflict occurs far away and does not involve Australian civilians. In contrast, most of the States we examined have much more imminent recollections of threats to their territories. The civilian populations in Estonia, Finland, and Sweden all have had – to varying degrees – to live in a state of preparedness for a possible Russian (and before that Soviet) attack for a long time. Taiwan is constantly under threat from China, and the situation in Ukraine is well-known. All this has helped shape a sense in the population that defence is everyone's concern, and this has also translated into those States' approach to defence (see discussion of 'whole-of-society' defence above section 1.4).

So, what are then the key ingredients in building resilience and a will to defend in a population? A formal adoption of a 'whole-of-society' approach to defence is a necessary first step and, as noted, inspiration may be drawn both from those States with a relatively long history of this approach, and from Taiwan's more recent steps in that direction. It may also be important to fight polarisation in the Australian society and to continue making sure that the population is aware of the threats to which Australia is exposed. Additionally, it may be the case that the Internet and the nature of cyber hostilities – hostilities that can come from anywhere in the world, showcasing that Australia's geographical isolation is no protection in cyber – will change attitudes.

While many additional measures for building the will to defend amongst the Australian population may be imagined, here it suffices to note one more lesson from the States studied for this Report; namely the importance of a clear communication of key positions. A useful illustration is found in the brochure 'In case of crisis or war' that has been published in Sweden since 1943.[135] The latest version, published by the Swedish Civil Contingencies Agency MSB, was mailed to all five million households in Sweden and is also available electronically, and in multiple languages. [136] While it serves several purposes in the context of helping the Swedish population to prepare for war and/or other crisis, there is one message that is known beyond all other; that is, "If Sweden is attacked, we will never surrender. Any suggestion to the contrary is false." [137] Not least in an era of disinformation, cognitive warfare, and 'deepfakes', a clear message such as this is invaluable.

3.2 The two types

Looking at the States examined for this report, there are essentially two models for volunteer cyber forces: (1) closed groups, and (2) open groups. The closed group structure is more common, but examples of both models can be found among the States studied for this Report. Unsurprisingly, there is a clear connection between the tasks assigned and which model is preferred.

3.2.1 Closed group model

Under the closed group structure, members formally sign up to join the group. This may involve a strict

[135] For an overview of the background of this initiative, see: Swedish Armed Forces, 'Vykort från ett land i väntans tider' (webpage, 25 July 2025) https://www.forsvarsmakten.se/sv/information-och-fakta/var-historia/artiklar/vykort-fran-ett-land-i-vantans-tider/.

[136] Swedish Civil Contingencies Agency, *If Crisis or War Comes* (2024) https://www.msb.se/sv/publikationer/om-krisen-eller-kriget-kommer-pa-engelska/.

[137] Ibid 5.

contractual arrangement but may also be a bit more flexible.

The Ohio Cyber Reserve, for example, is open for anyone to apply to join, but applicants with adequate experience are only permitted to join following a formal application process which includes screening and selection by existing OhCR members (see section 2.1.4). Admitted members then enter into a contractual agreement with the OhCR and become subject to various legal obligations in connection with their membership.

Another example of a closed group model is found in Estonia's Defence League's cyber unit. As discussed above (see section 2.1.1), existing members of the cyber unit must provide a reference to prospective new members applying to join. This is an advantage of a small countries where everyone knows everyone.

3.2.2 Open group model

In the open group structure, members need not formally join and there is no need for active participation by those who join. Among the States studied for this Report, only the Ukrainian 'IT Army' fits this category strictly interpreted. However, also Sweden's 'Glimt' initiative may be argued to essentially be a form of open group as anyone can join (although they need to sign up) and those joining are not obligated to act. Nevertheless, it is an interesting model that has distinct advantages, as well as distinct limitations as will be discussed throughout the Report.

The open group structure may facilitate the involvement of people who would not join a more formally structured closed group. This is clearly an advantage. At the same time, in an open structure, the identity of those joining may not be known. This may cause a range of problems. For example, unless strict conditions are imposed, young people – who may be classed as 'child-soldiers' in extreme cases depending on the tasks they perform – may join and be active in the activities of the volunteer cyber force.

3.3 State or federal?

One of the most basic considerations with which we must engage is whether the volunteer cyber forces ought to sit under state governments or under the federal government, or indeed under both. Looking at the model of the US, for example, we have shown that there are volunteer cyber forces in the cybersecurity context both on a state-level and on a federal level.

While any US federal level volunteer cyber force is only at an early stage of development, the state-level structures have already operated for, in some

cases, over a decade.[138] An advantage of state-level structures is that they are controlled at that level, can be faster to be deployed and respond, and can draw on state-level experts familiar with, for example, their government systems and networks. Further, they can be housed within existing structures or organised similar to existing and familiar structures, such as local State Emergency Services. However, at the state level, there may not be a sufficient number of experts available to assist in the case of a cybersecurity incident, for example, and state-based structures generally rely on state funding.

Advantages at the federal level include having a centralised structure with experts available that can operate nationally, particularly where incident response activities, for example, can be conducted virtually. However, issues can arise when providing cybersecurity support to state-level entities due to unfamiliarity with their systems, and a range of bureaucratic hurdles which often render federal level structures slow to respond. In turn, a potential issue with having both federal and state-level cyber volunteer structures is the added competition for competent volunteers, ensuring clarity around roles and responsibilities, and access to sufficient funding.

An additional complication is found in delineating mandates; that is, in some cases it may make sense to focus more on a systems-focused delineation rather than a geography-focused delineation.

Ultimately, it is important to highlight that there is no 'one size fits all' model. A cyber volunteer force structure must be created to suit local conditions taking into account a range of factors such as governance structures, funding arrangements, and geography.[139]

3.4 Which body assumes control?

If Australia pursues the option of harnessing the power of volunteer cyber forces, a key matter will be to identify who will be in charge of such forces. Importantly, given the diversity of roles that such forces may assume, it should not be presumed that one single body ought to control all volunteers. Rather, it may well be the case that e.g., the cybersecurity-oriented volunteers are under the control of one body while the OSINT focused volunteers are under the control of another.

While such a structure has advantages, it also comes with possible coordination issues. For example, one can imagine situations where the same volunteer joins more than one volunteer cyber

[138] On the benefits and drawbacks of these models in the US context, see Mark E Schreiber et al, *Creating a Cyber Volunteer Force: Strategy and Options* (Report, McDermott Will & Emery, March 2023) 33–37 https://www.mwe.com/insights/creating-a-cyber-volunteer-force-strategy-and-options.

[139] National Governors Association (n 66) 17.

force. In such situations, it would be useful if there is a degree of coordination e.g., as to time-commitments, and perhaps in cases of misbehaviour; that is, if a volunteer misbehaves within the role in one volunteer cyber force, they should be excluded from all such forces, and this requires a degree of coordination.

3.5 Direct control vs. 'control via objectives lists'

Most of the studied volunteer cyber forces have adopted a traditional structure for how orders are communicated, and objectives are set. We can call this 'direct control'. When it comes to the Ukrainian IT Army, a different model was adopted. We can call this model 'control via objectives lists'. Put simply, the State in question exercises control over the volunteer cyber force's activities by publishing lists of specific objectives for the volunteer to carry out should they wish to do so. In such cases, only when acting in the pursuit of those objectives is a person acting as part of the volunteer cyber force.

Particularly in a crisis situation, some types of Australian volunteer cyber forces could be open groups controlled via objectives lists and thus able to operate effectively without direct persistent control and guidance beyond the objectives list. That could involve the relevant body within the Australian government posting a list of objectives on an appropriate communications medium (such as an official webpage, a social media channel, or perhaps more appropriately a specifically developed app), and cyber volunteers then seeking to achieve those objectives to the best of their abilities within the predetermined parameters of their operations.

While the Ukrainian IT Army is the most prominent illustration of this model, another illustration of this structure is, as noted, found in Sweden's Glimt initiative discussed above (see section 2.2.1). Members sign up, they are not committing to do anything, but they have the option to contribute to specific objectives; in this case answering certain questions on the Glimt site that benefit from some OSINT research.

Adopting the 'control via objectives lists' approach comes with both several strong advantages and some serious limitation. These are discussed further throughout the Report. However, in any structure dependent on the 'control by objectives lists' model, the formulation of the objectives is a key challenge.

Formulating some of these objectives will be easier in times of war, or other open conflict, than it is during other times. For example, the political sensitivity characteristic of situations outside open conflict means that specific target States can perhaps not be specifically mentioned.

3.6 Technical structure for secure communication

Establishing a technical structure for secure communication between members of a volunteer cyber force and those in command would be costly and would take time. The question is whether it is needed.

Volunteer cyber forces within a 'cybersecurity reserve' could potentially be integrated within current communications structures. In contrast, other volunteers that are not vetted and trained to the same degree should not get such access.

Some new structures, such as web portals and/or apps for volunteers focused on OSINT and information conflicts may be necessary.

3.7 Filter for OSINT

A volunteer cyber force performing the OSINT function may potentially generate a large volume of information. There is a need to vet, or at least a strong advantage in vetting, that information before the professional intelligence community (e.g., an agency such as ASD) needs to deal with it. The question is then who can perform that role and how?

The answer to that questions will no doubt depend on the structure adopted. One may, for example, imagine civil society organisations or academic institutions operating OSINT facilities to which volunteer cyber forces contribute and where the relevant civil society organisation or academic institution performs a first vetting before the intelligence is communicated to the relevant agency (which may well be the agency with overall control of the volunteers' OSINT role).

3.8 'There is an app for that'

In times of crisis, effective communication with the population is crucial, yet also challenging. Two approaches found among the studied States, aimed to address this issue, may be noted.

The first involves attempts to ensure a high level of communication prior to a crisis so as to minimise the need for communication during a crisis. As noted above (see 3.1) Sweden, for example, publishes its information brochure 'In case of crisis or war' which is communicated both in hard copy and soft copy.

The second approach – found in Estonia[140] and in Ukraine[141] – is the use of a dedicated app or apps. An app has the clear advantages of making possible

[140] Ole Valmis, *Ole Valmis* (webpage, 25 July 2025) https://www.olevalmis.ee/en.

[141] Den Prystai, 'From Ukrainians to Ukrainians. 5 Digital Tools and Products Created to Help in Wartime' (War Ukraine, 5 October 2022) https://war.ukraine.ua/articles/digital-tools-created-to-help-in-wartime/.

continuous updates both as to content and functionality. Further, at least some core functions, such as important generic information, may be accessible via an app even where Internet connectivity is unstable or lacking.

Australia should consider developing a national 'war and crisis' app to be promoted to the entire population. Lessons from the past have illustrated that undertaking that type of task under time-pressure may have a negative impact on the quality of the app. Consequently, work should commence now, rather than wait for a time of crisis or war.

Such an initiative may usefully be combined with a hard copy distributed to Australian households. The hard copy has advantages such as being accessible to the small segment of the population that is not comfortable with technology, and the hard copy may be accessible also where interruptions to the electricity supply results in people not being able to access their phones to the degree they ordinarily would.

3.9 Libraries and other potential hubs in crisis

A report focused on the roles that libraries may fulfil in the Swedish civil defence highlights that planning is needed for the roles libraries can fulfil both in crisis and in war.[142] Libraries are natural hubs in society and a place to which people turn for information. Properly resourced and structured, libraries may play a central role in civil defence and volunteer cyber forces, not least cybersecurity volunteers may usefully be integrated into this.

3.10 Seniors: Harnessing an overlooked resource

In the context of the cyber-environment, older Australians (65 years +) are commonly approached as a vulnerable risk group. However, older Australians can also be an important resource within a whole-of-society approach to the benefit of Australian.

First, there is now a large, and increasing, number of retirees who have worked in an IT environment for most (or even all) of their work life. Indeed, some are e.g., cybersecurity experts of the highest calibre.

Second, even beyond IT experts, many Australian seniors today are highly competent users of computer resources and with the time available when finishing working life, they may play a significant role e.g., in OSINT and information warfare.

Of the greatest importance, by recruiting from the segment of the population who have already retired, volunteer cyber

[142] Anna McWilliams, *Bibliotekens roll i det civila försvaret* (Report, Totalförsvarets forskningsinstitut, November 2024) https://www.foi.se/rest-api/report/FOI Memo 8635.

forces avoid competing for talent with the private sector and the existing cyber defence capabilities.

To facilitate senior Australian's joining volunteer cyber forces, one could for example imagine targeted recruitment campaigns and even some cooperation with the major employers in the cybersecurity field so that those about to retire are informed of the possibility to join a volunteer cyber force.

Beyond the advantages already noted, involving senior Australians in volunteer cyber forces may facilitate digital inclusion and digital innovation, help seniors stay mentally active, and have a favourable impact on our societal cohesion.

3.11 Cooperation with friends and allies

A further matter to consider relates to whether there are ways to formalise, and harmonise, cyber volunteer structures with likeminded states in a mutually beneficial manner, including in situations where the citizens of one state serve in the volunteer cyber force of another; after all, there are clear synergies that could be exploited for mutual benefit especially amongst States that already cooperate in a defence setting.

In the context of international law, there are frequent calls for cooperation, and that the type of cooperation hinted at above may – not least where it decreases state reliance on vigilantes and non-state actors – be viewed as a measure:

> "to increase stability and security in the use of ICTs and to prevent ICT practices that are acknowledged to be harmful or that may pose threats to international peace and security".[143]

In Appendix 1, we outline a previously published proposal for a legal structure accommodating cooperation with friends and allies in the context of volunteer cyber forces.

3.12 The importance of training

The training provided to members of cyber volunteer forces is particularly important. For example, training provided by a government funded organisation provides volunteers with the opportunity to develop new cybersecurity skills and/or obtain relevant certifications for free, and this can act as a strong motivator for volunteers to participate. This also benefits the employers of those volunteers. Further, training and exercises organised for members allows volunteers to network and develop

[143] United Nations, *Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security* (Report, A/76/135, 14 July 2021) 8.

relationships with other volunteers in the cybersecurity sector. As noted, this fosters the development of informal networks and communication channels among individuals from the public and private sectors, and these networks can be critical in times of crisis.

When it comes to how training is conducted, there are indications that combining younger and more senior trainers can help to bridge generation-gaps. Furthermore, the need to facilitate sufficient training capacity to ensure that losses may be replaced in a time of war puts a degree of stress on the training program that must be planned for already in times of peace.

4. Key risks, implementation challenges, and their mitigation

Creating volunteer cyber forces, as envisaged in this Report, involves risks. Some may argue that we should not create new capabilities that involve risks. However, such a perspective misses the obvious point that not developing such capabilities also involves risks. Furthermore, it may also be noted that we already have many structures in society that involve risks. Police and military are equipped with weapons and trained to use them. That is not risk-free. Intelligence services may misuse their powers and methods of access, medical staff that intentionally administer the wrong drugs, and so on.

What is important is an awareness of the risks, and that all appropriate steps are taken to mitigate those risks. In this section, we point to and discuss a range of risks associated with volunteer cyber forces. We also point to potential mechanisms to mitigate those risks.

4.1 Loss of control

Any country creating a resource capable of undertaking the types of roles discussed above, must take great care to ensure that the resource created remains under its effective control. How this is achieved must depend on the structure adopted for the cyber volunteer capability in question. Volunteer cyber forces operating with a closed group model where members are subject to contractual and other legal obligations and are under the direct control of a relevant government authority, can mitigate this risk.

In relation to the discussed 'control via objectives lists' structure, it may be noted that it ensures that the body governing the cyber volunteer capability can delineate what the volunteers can, and cannot, do. Any member of the volunteer cyber force that undertakes activities not conforming to the objectives list, is simply not acting in the capacity of a member and would not enjoy any of the safeguards afforded to members.

4.2 Escalation risk

A key risk with the current use of non-state actors in cyberspace is that lacking discipline amongst such actors may lead to unwanted escalations. Formally recognised volunteer cyber forces ensure a higher level of transparency and accountability – and thereby a lower risk of unintended escalation – than what we are currently seeing in relation the cyber activities of non-state actors.

Furthermore, the 'control via objectives lists' structure ensures that the governing body can set limits for the cyber volunteers' activities in a manner that avoid such escalation.

4.3 Infiltration

The risk of infiltration must always be borne in mind but may differ depending on the structure in place. Closed groups built on personal relationships may be associated with lower risks of infiltration, while for open groups operating based on the 'control via objectives lists' structure infiltration is all but guaranteed. This must guide the types of tasks a volunteer cyber force is assigned, as well as how directions are worded.

Having said that, it is not necessarily difficult to formulate objectives that can be effectively pursued by a volunteer cyber force even where the enemy is aware of those objectives.

4.4 Abuse

Just as a government may be tempted to use the state's law enforcement, national security, and military for abusive purposes, it may be tempted to misuse volunteer cyber forces for such purposes. Safeguarding against such a development is crucial.

Just as Australian society has adopted structural safeguards (e.g., oversight) against such abusive use of the law enforcement, national security, and military, the risk of an abusive utilisation of an Australian volunteer cyber force may be avoided by safeguards such as proper oversight.

Furthermore, the proposed 'control via objectives lists' structure ensures complete transparency as to those volunteer cyber forces that operating under that model. This transparency is a powerful tool to address the risk of abuse.

4.5 Risk to individual members and organisations

The current legal landscape for civilians contributing to defence-related activation in cyberspace is plagued by uncertainty. However, where a State is willing to adopt, and benefit from, the work of a volunteer cyber force, it ought to provide appropriate legal safeguards – including legal indemnity in certain circumstances – for the participants of that force. Thus, a practice of States designating individuals as members of their volunteer cyber force has direct benefits for the individuals in question.

For example, it can be expected that some militia members will be exposed to harmful content, and/or attacks on their person. In such cases, they need to be provided appropriate help such as trauma help and/or legal help.

Similarly, organisations engaging in certain tasks (e.g., civil defence preparation or combating disinformation), or otherwise operating in the anticipated volunteer cyber force structure may become targeted by

hostile actors.[144] Where that occurs, the States benefiting from their work ought to provide support.

4.6 Problem of formulating the general mandate

The way in which the mandate for each volunteer cyber force is articulated is of obvious importance. Great care must be taken in delineating how these forces may act.

This task is complicated by the need to considering their operation in both peace time (characterised by grey zone conflict) and in war. This necessitates constantly reflecting on both the 'Canberra Café' and the 'Lviv 2022' perspective as observed in the introduction.

In this context it may be noted that, while the line between peace and armed conflict may be (increasingly) blurred under international law, Australia needs to develop clear guidelines for what type of circumstances trigger different types of mandates for the volunteer cyber forces. Such a classification need not be binary (peace v. armed conflict). Rather it may benefit from being more gradual in nature. At the minimum, one may imagine a three-stage distinction involving: (1) peace, (2) severe societal threat, [145] and (3) armed conflict. Any increased powers or roles for a volunteer cyber force in times of severe societal threat or armed conflict ought to be (1) necessary, (2) proportionate, and (3) temporary.

The formulation of the general mandate of a given volunteer cyber force must also take account of possible restrictions on what types of organisations are allowed to operate domestically.

4.7 Undermines capacity of private sector

With a limited pool of expertise to draw from, any increase in personnel devoted to their roles in volunteer cyber forces risk undermining the capability of other structures, such as the private sector. The reality is that, in many situations in which the need for members of volunteer cyber forces is the greatest will also involve the needs of the private sector, from which the volunteers commonly are drawn, being great.

---

[144] See further: Aneli Ahonen and James Pamment, *The Ethics of Outsourcing Information Conflict: Outlining the Responsibilities of Government Funders to their Civil Society Partners* (NATO Strategic Communications Centre of Excellence, Riga) https://stratcomcoe.org/publications/the-ethics-of-outsourcing-information-conflict-outlining-the-responsibilities-of-government-funders-to-their-civil-society-partners/292?ref=disinfodocket.com (accessed 21 July 2025).

[145] Defining what amounts to a 'severe societal threat' goes beyond the scope of this Report. However, one may usefully link such a definition to occurrences in which a substantial segment of Australian society is severely affected, and/or where fundamental values and functions are under threat.

The obvious solution to this issue is, of course, to train more people in the relevant fields and/or to broaden the pool from which expertise is drawn. However, while obvious, both these paths are associated with complications. First, training takes time and it seems reasonable to assume that the need e.g., for cybersecurity expertise will continue to outpace the Australian education system's ability to produce cybersecurity experts. Second, when it comes to the option of broadening the pool from which expertise is drawn, the reality is that competition for talent is fierce on an international level. This, combined e.g., with the need to ensure that recruitments from abroad are loyal to Australia, raises substantial obstacles.

In this context, we again emphasise the potential benefit of involving senior Australians in any volunteer cyber forces created, as well as the usefulness of establishing youth organisations providing relevant training.

Finally, when it comes to the interaction with the private sector, it may be noted that, while cybersecurity-related cooperation with the private sector is relatively uncomplicated in peacetime, such cooperation raises important additional questions and issues in a situation where Australia is involved in an international conflict. Those questions and issues stem both from the fact that different legal regimes apply, and from the practical issue that many key private sector actors are headquartered overseas.

4.8 Organisational complexity / activity overlaps

While there clearly are many advantages to be gained from harnessing the power of volunteer cyber forces, adding this capacity will add to organisational complexity, and there is an obvious risk of activity overlap. Activity overlap is not necessarily harmful, but it clearly can be. Consequently, it is important that the task assigned to volunteers do not interrupt the activities of our current capabilities.

4.9 Organisational culture

In a March 2024 report by the Foundation for Defense of Democracies, Lonergan and Montgomery highlight the strong impact a negative organisational culture may have:

> "Many officers have described how service culture denigrates cyber talent, damaging the morale of cyber personnel and eroding retention. "Retention rates of cyber personnel is abysmal" one retired Navy captan remarked. "The biggest reason the services hemorrhage talent is that cyber personnel do not feel

valued by their service's culture.""[146]

These are serious concerns, and similar issues may arise in relation to any volunteer cyber force placed in a defence structure. Consequently, it is important that volunteer cyber forces, and indeed any other 'cyber warriors' are made to feel valued. Shaping the culture of the organisation in question is crucial.

4.10 Operational complications

To conclude this section, it must also be acknowledged that volunteer cyber forces doubtlessly will encounter a range of operational complications. Not all such complications are easy to identify in advance and some will require being addressed as they arise rather than being pre-empted in advance. One person we interviewed made the comparison to 'flying a plane while, at the same time, building it'.

To provide one illustration of the type of operational challenges that must be expected, there have been situations where public bodies that could benefit from cyber security measures provided by volunteer cyber forces have been unable to accept such assistance due to their insurance policies requiring that measures taken in response to an incident are carried out by the insurance company's appointed actors.

[146] Erica Lonergan and Mark Montgomery, *United States Cyber Force: A Defense Perspective* (Foundation for Defense of Democracies) 16.

5. Legal considerations

Any creation of a volunteer cyber force comes with legal considerations. Some such considerations relate to domestic law. Others, stem from international law. Here we will briefly introduce a selection of key legal considerations. In doing so, we limit ourselves to providing a basic account of existing law. Suggestions for law reform fall outside the scope of this Report. However, one may relevantly observe that cyber conflicts put several key legal concepts under significant stress. For example:

- Under conventional current doctrine, the concept of sovereignty is unhelpfully anchored in territoriality and a focus on 'exclusiveness' incompatible with the cyber environment;

- The concept of espionage may become overly broad in the context of volunteer cyber forces; and

- In the context of cyber defence (as opposed to cyber-attacks) drawing sharp lines between military and civilian (i.e., the principle of distinction) may not be possible and is counter-intuitive given the need for whole-of-society defence in the cyber context. This requires a thinking going beyond habitual repetition of conventional dogmas.

In Appendix 2 we provide our 'Manual for Volunteer Cyber Forces: Legal Risks for Individuals' previously published within our project. It provides a more detailed overview of the domestic law issues that volunteers ought to be aware of.

5.1 Domestic law

The legal considerations and risks for individual members vary greatly depending on how the volunteer cyber force is structured and depending on the activities in which they engage. Many of the organisations examined in this Report have pre-existing legal frameworks in place for the volunteer cyber force in question, and these frameworks establish rules for membership, the law applicable to the activities of members (e.g., military law), and provisions around liability and immunities. [147] Additionally, members will generally be under contractual obligations contained in relevant membership agreements and non-disclosure agreements that they may have entered into.

In addition to these laws and obligations (and even where such laws or

[147] See for example, Ohio Code ch 5922, 'Civilian Cyber Security Reserve Forces' https://law.justia.com/codes/ohio/title-59/chapter-5922/ and The Estonian Defence League Act (consolidated version) https://www.riigiteataja.ee/en/eli/521032014005/consolide.

agreements are not in place), a number of areas of law are potentially relevant to the activities of volunteer cyber forces. For example, cybercrime laws contain offences relating to illegal access to computer systems, illegal interception of computer data, illegal interference with electronic data or computer systems, and misuse of devices and software. In addition to these core cyber-dependent offences, most legal systems also criminalise cyber-enabled offences such as computer related forgery or theft, online child sexual abuse related offences, non-consensual dissemination of intimate images, and laundering of proceeds of crime. These laws prohibit a range of 'hacking' and related offences, DDoS attacks, phishing, and certain uses of malware. Members of cyber volunteer forces are generally not exempt from these laws (unless, for example, authorised by law enforcement). Similarly, some of these activities may also result in claims against a member of a volunteer cyber force under private law such as torts law. This means that they may be held liable for damage they cause and that they may have to personally pay to compensate the victim.

Members of volunteer cyber forces may gain access to private, confidential, or otherwise sensitive information. Most States have laws regulating the handling of personal information, around the handling of commercially sensitive information as well as rules more broadly regarding breach of confidence. While it is best practice for affected organisations to enter into non-disclosure agreements with the members of volunteer cyber forces, even where these agreements are not in place, there are still legal restrictions on the use of different types of private, confidential or otherwise sensitive information.

Members of volunteer cyber forces who engage in information conflicts must take note of speech-related laws. The laws of most States regulate matters such as defamation, subversion, and hate speech. Some States also specifically regulate mis- and dis-information, and some State's laws include specific provisions against election interference. Some also prohibit insults to the king or other leaders. All these types of laws may impact what members of volunteer cyber forces legally may express. Most States also recognise some form of freedom of expression and where members of volunteer cyber forces are engaged in any attempt to restrict or otherwise limit hostile speech, account must also be taken of such laws. Importantly, the freedom expression is not absolute in any State's law and that right must often be reconciled with, or balanced against, other important interests such as the protection of the privacy or reputation of others. Members of volunteer cyber forces must have an understanding of the impact of all these laws from the point of view of the law of the State from which they operate. However, they may

also need to be informed of the law of other States with which they come into contact. The violation of foreign law may lead to lawsuits or prosecution in foreign jurisdictions, and even though such actions may have limited direct impacts due to enforcement difficulties, they may still impact the target e.g., by limiting the places to which they may safely travel.

5.2 International law

There are several international law considerations associated with the creation and utilisation of civilian volunteer cyber forces. These considerations vary greatly depending on the nature of the organisation, the types of activities it engages in, and the context and where these activities occur. This section provides an overview of key legal issues that must be taken into account by states when developing or utilising volunteer cyber forces. First, it outlines key rules of international law relevant to determining the lawfulness of cyber operations conducted against another state. This is important when considering the potential activities in which volunteer cyber forces may engage. Second, this section examines the implications of how a volunteer cyber force is organised under international law on State responsibility. Essentially those organisations operating as part of a State's government or defence structures generally ensures the state can exercise control over their activities and that there is clarity around legal responsibility. Finally, this section examines the legal implications of how a volunteer cyber force is organised or created in relation to the legal status and protections for its members in an armed conflict.

5.2.1 Cyber operations under international law

Where a volunteer cyber force engages in cyber operations or activities with effects in another country's territory or jurisdiction, there is a risk that those activities can constitute violations of international law.[148] Generally low-level cyber activities, including cyber espionage, will not constitute a violation of international law due to limited effects.[149] Cyber operations that cause physical effects or interfere with the governmental functions of another State can constitute violations of international law on sovereignty. Similarly, cyber operations that involve coercive interference with matters a State has the right to decide freely, such as its foreign

[148] See generally Samuli Haataja, 'Cyber Operations against Critical Infrastructure under Norms of Responsible State Behaviour and International Law' (2022) 30(4) *International Journal of Law and Information Technology* 423.
[149] Ibid 437-8. Notably the African Union has adopted the position that even unauthorised intrusions into a state's ICT infrastructure could constitute a violation of sovereignty. See African Union Peace and Security Council, *Common African Position on the Application of International Law to the Use of Information and Communication Technologies in Cyberspace* (Report, 29 January 2024) 9–10 https://cyberlaw.ccdcoe.org/wiki/Common_position_of_the_African_Union_(2024).

and economic policy, can result in violations of the non-intervention principle. In extreme cases, destructive or seriously disruptive cyber operations against, for example, critical infrastructure in another state, can constitute an unlawful use of force.[150] However, activities such as collection of OSINT or online activities designed to counter, or fact-check propaganda would generally not violate these rules of international law due to their effects. Similarly, in an armed conflict, cyber operations that constitute 'attacks' under international humanitarian law must be consistent with principles of distinction and proportionality, and the state has obligations to ensure its armed forces respect the law.[151]

5.2.2 State responsibility for unlawful activities of a volunteer cyber force

The structure and organisation of a volunteer cyber force is important in determining whether the State is responsible for any unlawful activities, such as cyber operations in violation of international law as outlined above. While it is generally recommended that the volunteer cyber force is under the command of the State, particularly in times of crisis, the following outlines the legal implications of volunteer cyber forces organised in different ways.

5.2.2.1 Volunteer cyber force operated by the State

Under international law, a volunteer cyber force can be considered an organ of the State, such as where it is part of its armed forces or operated by any State of federal level government.[152] This means that where the volunteer cyber force engages in cyber activities in systems or networks outside that State's territory or jurisdiction, the State can be responsible under international law where those activities violate international law obligations owed to other States. Much will depend on the activities the volunteer cyber force engages in, and the types of effects they cause. Where the cyber activity in question does constitute a violation of international law, this has legal consequences for the State operating the volunteer force and increases the risk of the State being subject to countermeasures. Similarly in the context of an armed conflict, if a volunteer cyber force engages in conduct that violates international humanitarian law, that conduct can be attributed to the State so that it is responsible under international law.

---

[150] Haataja (n 148) 433-9.

[151] See generally Eve Massingham and Annabel McConnachie (eds), *Ensuring Respect for International Humanitarian Law* (Routledge 2020).

[152] On international law on state responsibility in this context, see James Crawford, *The International Law Commission's Articles on State Responsibility: Introduction, Text and Commentaries* (Cambridge University Press, 2002) 94–99. See also Michael Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Warfare* (Cambridge University Press, 2017) 87–88.

5.2.2.2 Volunteer cyber force operating under the instructions, directions or control of the State

Where the volunteer cyber force is established as a private entity, such as a private company, and not part of an organ of the State, the State can only be held responsible for its unlawful activities where it provides instructions, directions or exercises effective control of over the volunteer cyber force's activities. [153] Generally this requires specific instructions or determining the objectives of the volunteer cyber force. However, where the State only provides funding or training, then any internationally wrongful conduct of the volunteer cyber force would generally not be attributed to the State under international law.[154] Instead the wrongful conduct of the volunteer cyber force would be treated as a criminal matter and individual members could be criminally responsible. Prosecution of these individuals could occur either their home State or in the foreign State where their online activities caused harmful effects.

5.2.2.3 Private volunteer cyber force operating from the territory or jurisdiction of a State

Where the volunteer cyber force is established as a separate legal entity, such as a private company, or operates as merely a network of volunteers without a connection to the State (opposed to being connected with a government agency), the State can still potentially responsible for cyber activities it engages in which harm is caused in other States. Under the notion of due diligence, States should not knowingly allow their territory to be used to cause harm to other States.[155] While there is some debate about the status and scope of due diligence in the cyber context, this could extend to the activities of a volunteer cyber force where its members cause harmful effects in another State. For example, where members of a volunteer cyber force spread malicious software or engage in other criminal activities within systems and networks in another State, and the State in which those members are operating in has knowledge of those activities, then it should take reasonable measures to stop the harmful conduct. Failing to take such measures can render the State in violation of its international law obligations owed to the victim state, and this in turn could allow the victim State to take lawful countermeasures against them.

5.2.3 Legal status and protections for members of a volunteer cyber force in an armed conflict

As outlined above, depending on how a volunteer cyber force is organised and

[153] Schmitt (n 152) 94-96.
[154] Ibid 97.
[155] For an overview, see Samuli Haataja and Dan Svantesson, 'Cyberspace and National Security' in Danielle Ireland-Piper (ed), *National Security Law in Australia* (The Federation Press, 2024) 278–79.

structured, a State may be responsible for the unlawful or harmful activities of its members. In an armed conflict, given the involvement of civilians, an additional consideration is the legal status and protections of members of a volunteer cyber force. This is important as combatants are entitled to legal protections in the form of combatant immunity meaning they cannot be prosecuted for having engaged in lawful acts as part of the conflict, and prisoner of war status. While civilians generally cannot be targeted, where they actively participate in hostilities through cyber means, they may become lawful targets and are not entitled to the same legal protections as combatants.

5.2.3.1 Combatants

Where a State has an established a volunteer cyber force, its members can be considered 'combatants' under international humanitarian law in the event of an international armed conflict. The law defines combatants to include not only the armed forces of a State, but also militias and volunteer corps that are part of the armed forces.[156] Where a militia or volunteer corps is not part of the armed forces, its members can still be considered combatants where they constitute an organised armed group. This requires that its members are under responsible command, wear a distinctive sign, carry arms openly, and operate in accordance with the laws of armed conflict.[157] In other words, where a volunteer cyber force is integrated into the armed forces, then its members would be considered combatants and be entitled to combatant immunity and prisoner of war status. But where a volunteer cyber force is not part of the armed forces or integrated into them in times of crisis, then it would need to satisfy the above criteria for it to constitute an organised armed group meaning its members are considered combatants and entitled to combatant immunity and prisoner of war status.[158]

5.2.3.2 Levée en masse

Where a State does not have an organised volunteer cyber force but one is created spontaneously by its inhabitants when faced with an invasion, those individuals could be entitled to combatant immunity and prisoner of war status where they constitute what is known as a levée en masse.

A levée en masse refers to situations where the inhabitants of a non-occupied territory 'spontaneously take up arms to resist the invading forces'.[159] Traditionally

[156] Geneva Convention Relative to the Treatment of Prisoners of War (adopted 12 August 1949, entered into force 21 October 1950) 75 UNTS 135 (Geneva Convention III) art 4(A).
[157] Ibid.
[158] On the debate about how these criteria should apply in the cyber context, see Schmitt (n 152) 403-406.

[159] Geneva Convention III (n 156). 'Inhabitants of a non-occupied territory, who on the approach of the enemy spontaneously take up arms to resist the invading forces, without having had time to form themselves into regular armed units, provided they carry arms openly and respect the laws and customs of war.'

a levée en masse involves the general population standing up against the invasion in situations where they have not had time to organise, and it is a requirement they carry arms openly. Some comparisons between a volunteer structure such as Ukraine's IT Army and this concept can be drawn given the spontaneous way in which the IT Army was formed. However, experts are divided on whether a volunteer cyber force such as that could satisfy the above criteria to constitute a levée en masse. [160] Generally, at least a pre-existing volunteer cyber force would fall outside the scope of this concept given its level of organisation.

5.2.3.3 Direct Participation in Hostilities

Where members of a volunteer force are not considered combatants as part of or incorporated into a State's armed forces, and those members actively engage in hostilities as part of an armed conflict, there is a risk that members can lose important legal protections as civilians. The law defines civilians as those persons who are not members of the armed forces (or who have been incorporated into them) or part of a levée en masse. [161] The activities of civilian members of a volunteer cyber force could potentially constitute 'direct participation in hostilities' (DPH) which would render its members lawful targets and open to criminal prosecution. Therefore, it is important to ensure the activities of a civilian members of a volunteer cyber force remain below the threshold of what constitutes DPH so that they retain their legal protections as civilians.

The law on DPH requires that three cumulative criteria are met. First, the 'threshold of harm' element requires that the activities in question adversely affect the military operations or capacity of the adversary (or result in death, injury or destruction). Second, the 'direct causation' element requires that the activities conducted by the volunteer cyber force caused the harm. This allows for civilians to 'indirectly' participate in the general war effort and war sustaining activities, provided their acts are not integral parts of acts that cause adverse effects on the enemy's military capacity. Finally, the 'belligerent nexus' element requires a connection between the action and the hostilities, opposed to, for example, actions conducted for private or criminal purposes. [162]

[160] Russell Buchan and Nicholas Tsagourias, 'Ukrainian "IT Army": A Cyber Levée en Masse or Civilians Directly Participating in Hostilities?' (EJIL: Talk!, 9 March 2022) https://www.ejiltalk.org/ukranian-it-army-a-cyber-levee-en-masse-or-civilians-directly-participating-in-hostilities (accessed 21 July 2025); Väljataga (n 134) 4-5. See also Schmitt (n 152) 409.

[161] Schmitt (n 152) 413.

[162] See generally Nils Melzer, *Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law* (International Committee of the Red Cross, 2009); Michael Schmitt, 'Deconstructing Direct Participation in Hostilities: The Constitutive Elements' (2010) 42(3) *New York University Journal of International Law and Politics* 697; Emily Crawford, *Identifying the Enemy: Civilian*

Where, for example, a volunteer cyber force conducts offensive cyber operations against an adversary's military communication networks, that would qualify as DPH. However, activities such as sharing information about enemy movements through an online platform or app can be legally problematic. Where this information is provided to a State's own armed forces enabling an attack on these targets, then that would likely qualify as DPH. However, where the information is only of a general nature, or obtained and shared with the purpose of helping to protect civilians from incoming threats, then it would likely not qualify. [163] Similarly, countering disinformation operations through fact checking and other means would likely fall below the threshold for DPH. In relation to defensive cyber activities, most would regard these as not adversely affecting the enemy's military capacity and therefore not DPH. However, some legal experts view actions such as 'maintaining passive defences of military cyber assets' which benefit one party's military capacity (as they effectively weaken the adversary's position) as within the scope of DPH. [164] Under this approach, a broader range of potential activities conducted by a volunteer cyber force would reach the threshold of DPH. Therefore, given the different interpretations of the law about when civilian cyber activities in an armed conflict constitute DPH, having civilian members of a volunteer cyber force engage in these activities carries legal risks as it has potential to render those individuals lawful targets and open to criminal prosecution under the target State's domestic law.

Importantly, civilians directly participating in hostilities only become lawful targets 'for such time' that they actively participate. Generally this includes:

> "[m]easures preparatory to the execution of a specific act of direct participation in hostilities, as well as the deployment to and the return from the location of its execution". [165]

However, there is debate among legal experts about what constitutes preparatory acts, [166] and whether the 'revolving door' of protection that civilians participating in hostilities may

Participation in Armed Conflict (Oxford University Press, 2015).

[163] See Schmitt (n 152) 430; Mačák, Kubo. 'Will the Centre Hold? Countering the Erosion of the Principle of Distinction on the Digital Battlefield' (2023) 105(923) *International Review of the Red Cross* 965. See also Michael Schmitt and William Casey Biggerstaff, 'Ukraine Symposium – Are Civilians Reporting With Cell Phones Directly Participating in Hostilities?' (*Articles of War*, 2 November 2022) https://lieber.westpoint.edu/civilians-reporting-cell-phones-direct-participation-hostilities (accessed 21 July 2025).

[164] This was the view adopted by some (but not all) of the legal experts that authored the Tallinn Manual. See Schmitt (n 152) 429.

[165] Melzer (n 162) 65.

[166] Schmitt and Biggerstaff (n 163).

receive is practical from an operational perspective.[167] For example, consider a civilian using their computer or smartphone to launch DDoS attacks against adversary military networks. Assuming this act meets the DPH criteria, the individual would at least be targetable while using their device to launch the attack. But legal experts are divided on whether the same individual, launching multiple attacks over a longer time period, would be targetable for the entire time period or only during active acts of DPH.[168] In relation to preparatory acts, it is unclear whether an individual using a smartphone app to engage in acts of DPH must be actively preparing to use the app to do so or, for example, whether simply having the app installed qualifies as a preparatory act which falls within the scope of DPH.[169] In any case, even if an individual is considered a lawful target due to their acts constituting DPH, a number of practical difficulties arise in relation to identifying those individuals and, should those individuals be targeted, ensuring compliance with other principles of international humanitarian law such as proportionality.

Finally, it is important to note that under international law a civilian engaging in DPH becomes targetable even where they are located outside the combat zone. This generally applies to foreign individuals located in a State that is not party to the armed conflict. Though there is some debate,[170] the law in this context generally applies to "any hostilities wherever located, with a direct nexus to the conflict", [171] and whether an individual can be targeted depends on their status or their actions of participating in hostilities, not their location. [172] Further, where individuals are nationals of neutral states but their actions constitute DPH, they lose their status as neutrals and can be targeted.[173] This means that even foreign members of a volunteer cyber force located in another State, such as in the case of some members of Ukraine's IT Army, could be rendered lawful targets. However, again practical difficulties arise in relation to their identification and ensuring targeting decisions are consistent with international humanitarian law. Additionally, a number of other non-legal factors, including political and strategic, and practical and logistical, make it unlikely

[167] Schmitt (n 152) 432; William Boothby, *The Law of Targeting* (Oxford University Press, 2012) 160–61.
[168] Schmitt (n 152) 432.
[169] Schmitt and Biggerstaff (n 163).
[170] See Jelena Pejic, 'Extraterritorial Targeting by Means of Armed Drones: Some Legal Implications' (2014) 96(893) *International Review of the Red Cross* 67, 97–100.
[171] Michael Schmitt, 'Extraterritorial Lethal Targeting: Deconstructing the Logic of International Law' (2013) 52(1) *Columbia Journal of Transnational Law* 77, 97.
[172] Ibid 97-104.
[173] Hague Convention (V) respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land (adopted 18 October 1907, entered into force 26 January 1910) 205 CTS 299 art 17; Pejic (n 170) 101.

those individuals would be targeted by at least traditional kinetic means.

6. Recommendations

Based on the above, we make 15 recommendations. They are as follows:

Recommendation 1
Strengthening Australia's cyber capabilities beyond current conventional structures may take many different forms. Australia should investigate several options for volunteer cyber forces, and all such options must be understood, and evaluated, as parts of a bigger picture.

Recommendation 2
Strengthening Australia's cyber capabilities requires being willing to re-think several structures, and it requires approaching the matter as an entire 'ecosystem' with attention placed both on each component individually and on the bigger picture those components create as a whole. Lessons may be learnt e.g., from structures adopted in the studied States.

Recommendation 3
The whole of Australian society depends on Cyberspace, so strengthening Australia's cyber capabilities requires a whole-of-society approach. Lessons may be learnt e.g., from structures adopted in the studied States, both those with a long history of a whole-of-society structure and those that more recently have moved in this direction.

Recommendation 4
Australia should take steps to develop a cyber volunteer force to strengthen the country's cybersecurity – a 'cybersecurity reserve'. Inspiration may be drawn from the structures adopted e.g., in Estonia, Finland, or the United States (either on the federal level or from Ohio).

Recommendation 5
In addition to the 'cybersecurity reserve' envisaged in Recommendation 4, Australia should take steps to also adopt measures making it possible to harnesses a broader range of volunteers ('cybersecurity citizen guardians') to carry out lower-level cybersecurity tasks in a time of serious crisis.

Recommendation 6
Australia should take steps to develop a cyber volunteer force operating in the OSINT role ('OSINT volunteers'). A first step may be to offer free courses on OSINT to the public. However, a range of alternatives such as the 'collective intelligence' model adopted by the Swedish Defence Research Agency for its Glimt initiative (glimt.nu) may be considered.

Recommendation 7
Australia should take steps to develop a cyber volunteer force working to detect and report on foreign information or cognitive warfare aimed at Australians and Australian interests ('INFOWAR volunteers'). A first step may be to offer free training courses raising the public's

interest in, and awareness of, the issues involved, and that equip participants to better identify hostile information or cognitive campaigns. Such courses could then facilitate the recruitment of 'INFOWAR volunteers'.

Recommendation 8
Australia should take steps to evaluate whether the proposed 'INFOWAR volunteers' (See Recommendation 7) should also be trained for a potential role in countermeasures, such as countering false, or otherwise misleading, narratives. Further, it may be envisaged that INFOWAR volunteers are trained and guided to engage in low-level proactive information conflict operations.

Recommendation 9
Australia should take steps to evaluate whether there are any circumstances under which some cyber volunteer capability ought to be equipped to engage in conduct that may amount to espionage.

Recommendation 10
Australia should take steps to evaluate whether there are any circumstances under which some cyber volunteer capability ought to be equipped to engage in proactive cyber operations.

Recommendation 11
Where it is advantageous to do so, existing organisational and legal structures should be utilised for the creation of volunteer cyber forces. However, where doing so is not appropriate, new organisational and legal structures should be developed.

Recommendation 12
To enhance Australia's capability to communicate with the population during crisis or war, a dedicated national app should be developed. The app should be supplemented with hard copy information distributed to all Australian households.

Recommendation 13
Work should be commenced to identify how libraries and other societal hubs may most effectively contribute to Australia's civil defence. In this context, attention should be placed on how volunteer cyber forces may contribute to such hubs.

Recommendation 14
Australia already as youth organisations such as the Air Force's cadets. Such organisations should expand to also address cybersecurity, or new organisations should be set up specifically for youth activities in cybersecurity, OSINT, and information warfare.

Such organisation could help raise awareness, increase the will to defend Australia, and facilitate recruitment.

Recommendation 15
Australia should take steps to recruit senior Australians to join the volunteer cyber forces. Many senior Australians

may have suitable skills, and the necessary time, to make major contributions to such work.

Harnessing this capability, also has the advantage of not competing with the staffing requirements of the private sector and other organisations.

7. Concluding remarks and the path forward

Drawing upon the experiences from Estonia, Finland, Sweden, Taiwan, Ukraine, and the United States, this Report has sought to outline the roles that volunteer cyber forces can play, how such forces may be structured, and the risks and legal considerations involved. Australia should develop a volunteer cyber force to increase cybersecurity preparedness and resilience in peacetime. A capability such as this can also be harnessed in times of crisis or conflict and may in fact be even more important then.

In addition, Australia should consider developing volunteer cyber forces in the fields of OSINT, as well as in information and cognitive conflict. As to a potential volunteer cyber force in the domain of information and cognitive warfare, both defensive and proactive roles may be considered. Indeed, Australia should also consider the possible advantages and disadvantages of volunteer cyber forces operating in the context of espionage and proactive cyber measures.

The Report has outlined certain key risks and complications and proposed mitigating steps that may be taken. In addition, several obstacles need to be overcome if Australia is to gain the benefits of the types of volunteer cyber forces envisaged in the Report. First, there may be a lacking political will for broad reform. While everyone recognises and speaks of the need for innovation, there is seemingly still an unwillingness to accept anything new. Relatedly, so far the cyber volunteer agenda has lacked a political champion that can move the proposals forward and take on the task of guiding the proposals through the appropriate political processes. Perhaps there is also a fear of competition among some bodies. If so, it is importantly to bear in mind that what is proposed in the Report is to complement, not replace, existing structures and capabilities.

In the end, perhaps the biggest implementation obstacle is found in the misguided view that this is not urgent. There is perhaps still a ‘why buy a firehose if the house is not on fire’ type attitude preventing serious work on volunteer cyber forces. But as the reality of the world we live in catches up with us, such dilutions ought to evaporate.

Appendix 1 – Facilitating coordination with friends and allies in relation to volunteer cyber forces

In order to facilitate coordination with friends and allies, Australia could consider introducing a Bill along the lines of what is proposed below. The Bill aims to make possible the involvement of Australian volunteers in foreign volunteer cyber forces. It is consequently a supplement to the proposals above aimed at establishing Australian volunteer cyber forces, and if other friendly States also adopt a structure such as that advanced below, Australia could benefit from the surge capacity potential of including foreigners in some aspects of the work of Australian volunteer cyber forces.

Proposal for a '*Designated Volunteer Cyber Force Bill*'[174]

Article 1

The [INSERT OFFICE] can proclaim a foreign Volunteer Cyber Force as a *Designated Volunteer Cyber Force* under the following circumstances:

1. A foreign State has established the Volunteer Cyber Force;
2. That foreign State has invited foreigners to join its Volunteer Cyber Force; and
3. The foreign State is under armed attack [by another State].

Explanatory comments:

It is crucial that any proposed protection for the members of a volunteer cyber force is conditioned on State oversight and control; after all, we are here talking about volunteers carrying out activities in an organised manner based on orders issues by a State. In this proposal, Article 1 is the first mechanism to ensure such State control and oversight.

Article 1 gives the Australian government the power to, in a sense, recognise as legitimate a foreign volunteer cyber force. There is no duty to do so. Thus, if my proposal is adopted, Australia has full discretion as to when to activate the anticipated legal safeguards (Articles 3-5) for Australian citizens who join the foreign volunteer cyber force. Under this approach, the starting point is that Australians are prevented from joining a foreign volunteer cyber force to the extent that their activities fall foul of cybercrime

[174] This proposal, and the explanatory comments, was first published in: D J Svantesson, 'Legal Safeguards for the Volunteers of Ukraine's Cyber Militia' (Verfassungsblog on Matters Constitutional, 23 March 2022) https://verfassungsblog.de/legal-safeguards-for-the-volunteers-of-ukraines-cyber-militia/ (accessed 21 July 2025).Their proposal has been amended here to reflect the terminology adopted within this report.

laws, and only where the Australian government has recognised as valuable the activities of the foreign volunteer cyber force could they enjoy the relevant legal safeguards.

The alternative to this 'institutionalisation approach' would be to focus solely on the activities themselves – prosecutorial discretion could allow "good" activities to go unpunished. However, such a structure would perhaps become unworkable due to its inherent lack of predictability.

Finally, the term "foreign State" should be read broadly so as to also open for the possibility of assisting entities not fully recognised as States under international law, e.g., Taiwan.

Article 2

Unless the activities constitute a violation of international law, a genuine member of a *Designated Volunteer Cyber Force* enjoys the protection of the legal safeguards outlined in Articles 3-5 in relation to activities that are:

1. Undertaken in the capacity as a member of a *Designated Volunteer Cyber Force*;
2. Undertaken based on an order issued by the foreign State in command of the *Designated Volunteer Cyber Force*; and
3. Defensive in nature.

Explanatory comments:

Article 2 seeks to set criteria for when a member of a *Designated Volunteer Cyber Force* is entitled to the legal safeguards this Bill aims to provide. It is the most complex, and likely the most controversial, provision of the proposed Bill.

First, and most obviously, the phrase "Unless the activities constitute a violation of international law" can be attacked for its vagueness, or perhaps more specifically, for its reliance on international law that is too vague currently. This is a genuine concern. However, on balance this structure was preferred to emphasise that international law must play a role here and to acknowledge that violations of international law – where they can be established – must invalidate the legal safeguards in question.

Second, the fact that only activities undertaken based on an order issued by the foreign State in command of the *Designated Volunteer Cyber Force* adds further legal safeguards and constitutes the second mechanism to ensure adequate state control and oversight.

In addition, some observations must be made as to the limitation to activities that are "Defensive in nature". Some cyber activities are inherently defensive. Others are inherently offensive. However, drawing a distinction between cyber activities that are defensive and those that are offensive is not always

going to be easy. Against that background, states considering adopting a version of this proposed Bill may wish to include a definition of what amounts to activities that are 'defensive in nature'.

Finally, the reference to the activity being undertaken in the capacity "as a member" of a *Designated Volunteer Cyber Force* must be read from the perspective of how the cyber militia in question operates. Some may require a formal membership while others are more open.

Article 3

A person classed as a genuine member of a *Designated Volunteer Cyber Force* under Article 2 is exempt from the criminal liability that otherwise would apply under the following provisions:

[INSERT LIST OF RELEVANT LEGAL PROVISIONS FROM AUSTRALIAN LAW]

Explanatory comments:

Australian law contains several provisions imposing criminal liability for computer-related offenses. Article 3 aims to provide exemption form such provisions and should the proposed law move ahead, it will be necessary to map out all such provisions.

Article 4

The Commonwealth will refuse any extradition request received where it relates to the activities of a person classed as a genuine member of a *Designated Volunteer Cyber Force* under Article 2

This does not prevent the Commonwealth cooperating in the case of allegations of war crime being brought against the person before a recognised international war crimes tribunal.

Explanatory comments:

The combination of Article 3 and the need for 'dual criminality' (that is, the activity must be a crime punishable in both the country where a suspect is being held, and in the country asking for the suspect to be extradited) may dispose of the risk of extradition in many states. Article 4 is included to specifically and expressly exclude the possibility of a person enjoying the protection of this Bill being extradited.

In addition, the second paragraph of Article 4 clarifies that the legal safeguards in question do not extend to allegations of war crime before a war crimes tribunal recognised by the state adopting the Bill.

Article 5

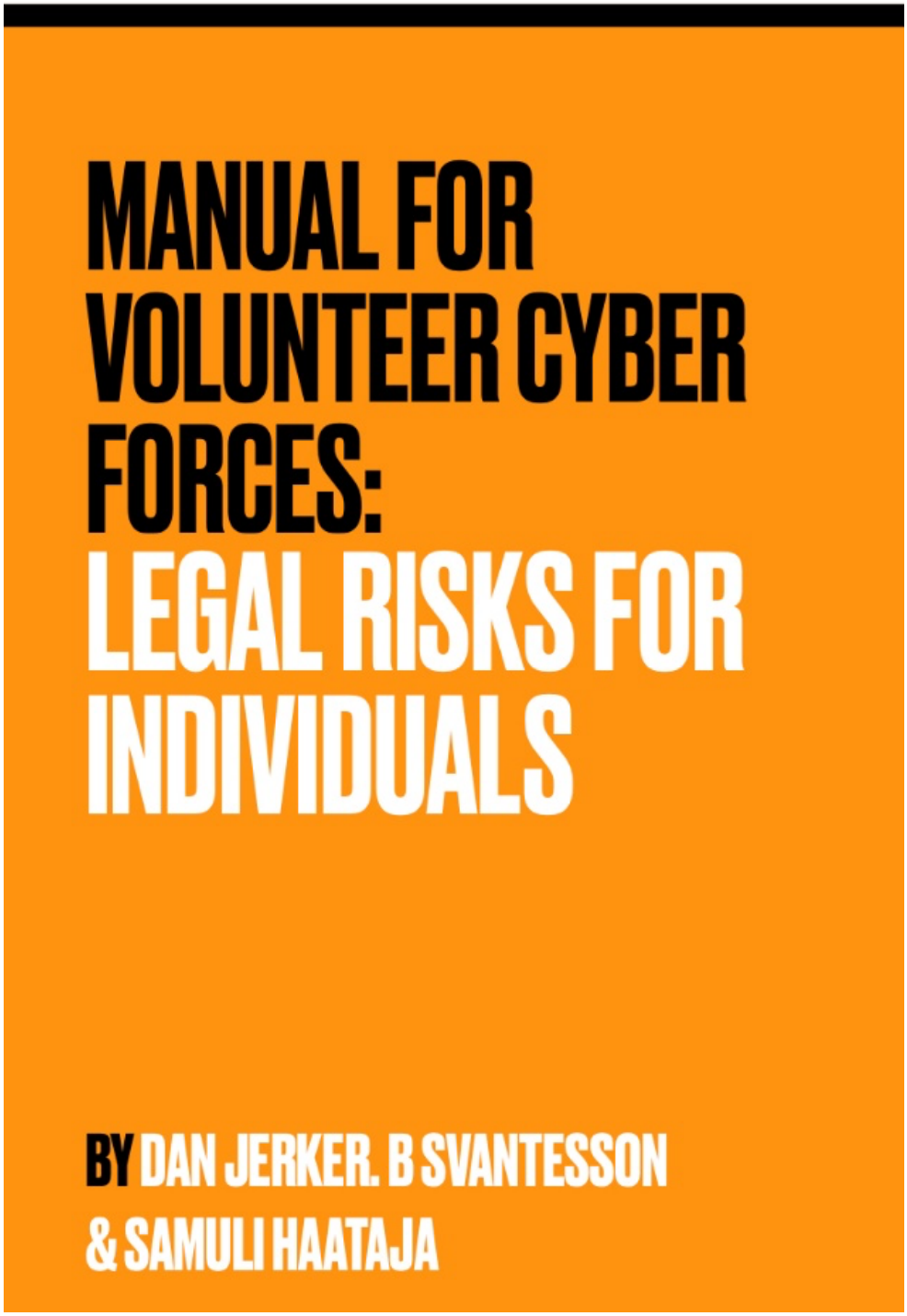
A person classed as a genuine member of a *Designated Volunteer Cyber*

Force under Article 2 is exempt from civil liability in relation to activities carried out in that capacity.

Explanatory comments:

While excluding criminal liability (Article 3) and the risk of extradition (Article 4) may be the most important legal safeguards for someone joining a foreign *Designated Volunteer Cyber Force*, the protection would clearly be incomplete if it did not extend to civil liability that may arise from the activities. This makes a provision such as that of Article 5 a necessary addition.

Appendix 2 – Manual for volunteer cyber forces: Legal risks for individuals



Funded by the Australian Department of Defence's Strategic Policy Grants Program

ABOUT THE MANUAL

This manual provides general guidance about the legal issues associated with civilian involvement in volunteer cyber forces. Volunteer cyber forces exist in many shapes and forms – some are operated purely by volunteers, others by international NGOs, and others are part of a nation-state's government agencies. The activities volunteer cyber forces engage in also vary. Common activities range from promoting public awareness and education around best practices in cybersecurity, conducting cybersecurity inspections and audits for companies and organisations, responding to cybersecurity incidents, and – in extreme cases – supporting nation-states in their national cyber defence.

Volunteer cyber forces may also engage in other activities, for example, within the fields of Open-source Intelligence (OSINT) or both defensive and proactive information warfare.

Given the variety of volunteer cyber forces and activities they can engage in, there are multiple areas of law and legal issues that can be potentially relevant for civilian members of these forces. The implications for engaging in conduct that is inconsistent with the law can be serious, including civil and criminal penalties such as fines or imprisonment. In extreme cases, such as participating in the activities of volunteer cyber forces engaging in a conflict, such participation can render an individual a lawful target of attack. This means that such individuals are exposed to the risk of being physically harmed or killed.

Against this background, it is important for members of volunteer cyber forces to be aware of the legal risks and consequences associated with their activities. This manual is intended for prospective individuals seeking to join volunteer cyber forces, and it aims to provide some brief and general guidance only about the legal risks and considerations associated with the activities of volunteer cyber forces. The

manual is neither providing legal advice, nor is it a substitute for legal advice.

As a first step, prospective members looking to join a volunteer cyber force ought to contact the organisers of that group and seek clarity of what is involved. The relationship between the organisers and the members of a volunteer cyber force ought to be regulated in a contract drafted in clear an accessible language. Clarity upfront avoids issues later on.

1.

CYBERCRIME LAWS - DO NOT ENGAGE IN CONDUCT THAT VIOLATES CYBERCRIME LAWS

The laws around cybercrime prohibit a range of 'hacking' and related activities. Most States have cybercrime offences relating to illegal access to computer systems, illegal interception of computer data, illegal interference with electronic data or computer systems, and misuse of devices and software. In addition to these core cyber-dependent offences, most legal systems also criminalise cyber-enabled offences such as computer related forgery or theft, online child sexual abuse related offences, non-consensual dissemination of intimate images, and laundering of proceeds of crime. Essentially these laws criminalise activities such as DDoS attacks, phishing, and certain uses of malware. They also generally criminalise 'hacking back' against a malicious actor in response to a cybersecurity incident.

Members of volunteer cyber forces are not exempt from these laws and should not engage in conduct that may contravene these laws unless they have been properly authorised (for example by law enforcement) or have the consent of the relevant organisation for activities on their systems. And even where they act under such authorisation

or consent, they may potentially be prosecuted in other States that may not recognise an authorisation by the State from which they acted, or on whose behalf they acted.

2.

PRIVATE LAW INCLUDING TORTS - DO NOT VIOLATE CIVIL LAWS SUCH AS TORTS LAW

Certain activities, such as those falling within the cybercrime laws discussed above may also result in claims against a member of a volunteer cyber force under private law such as torts law. This means that they may be held liable for damage they cause and that members may have to personally pay to compensate the victim.

Like discussed regarding authorisation and consent in relation to cybercrime laws, members of volunteer cyber forces must be aware that other States may not recognise an authorisation by the State from which they acted, or on whose behalf they acted.

3.

PRIVACY, SENSITIVE, AND CONFIDENTIAL INFORMATION - DO NOT HANDLE PRIVATE, CONFIDENTIAL, OR OTHERWISE SENSITIVE INFORMATION IMPROPERLY

Members of volunteer cyber forces may gain access to private, confidential, or otherwise sensitive information. Most States have laws regulating the handling of personal information and other legally protected information. These laws must be complied with.

Further, there are laws around the handling of commercially sensitive information as well as rules more broadly regarding breach of confidence. While it is best practice for affected organisations to enter into non-disclosure agreements with volunteer cyber forces, even where these agreements are not in place, there are still legal restrictions on the use of different types of private, confidential or otherwise sensitive information.

4.

RESTRICTIONS IMPOSED IN YOUR CONTRACT OF EMPLOYMENT - DO NOT ENGAGE IN CONDUCT THAT VIOLATES YOUR CONTRACT OF EMPLOYMENT

Members of volunteer cyber forces who are employed must carefully consider whether their contract(s) of employment imposes any restrictions on what tasks they are allowed to undertake in their volunteer capacity. Such restrictions may also affect the use of hardware and/or software provided by the employer whether they are used during work hours or not, and whether they are used outside the workplace or not.

5.

PARTICIPATION OR SUPPORT IN AN ARMED CONFLICT - DO NOT ACTIVELY CONTRIBUTE TO HOSTILITIES IN AN ARMED CONFLICT

An 'armed conflict' is a legal term referring to a war or related conflict between states, or non-state groups (such as revolutionary forces) and a State. International humanitarian law (IHL) is a special area of law that applies in times of armed conflict and to activities connected to an armed conflict. While the law does not prohibit civilians from actively contributing to hostilities, where individuals engage in such activities, they can lose important legal protections with potentially serious consequences. These include becoming lawful targets of attack, as well as losing 'prisoner of war' status. Under IHL and during an armed conflict, civilians generally cannot be targeted. However, an exception arises where civilians take an active part in the armed conflict and this can also occur through cyber means.

Under what is known as the law on 'direct participation in hostilities', civilians cannot engage in activities that adversely affect (or are likely to affect) another state's military operations or capacity. For example, if civilians engage in offensive cyber operations disrupting another state's military

communications or the operation of railway networks being used for military transport, then those civilians may give up their civilian immunity. As a consequence, those civilians can be lawfully targeted, or they may be prosecuted under the laws of the State against which they conducted those activities.

“WHILE THIS IS AN EVOLVING AREA OF LAW, THERE ARE A RANGE OF CYBER ACTIVITIES THAT CIVILIANS CAN CONDUCT IN SUPPORT OF THE WAR EFFORT WITHOUT LOSING THE PROTECTIONS OF THEIR CIVILIAN STATUS. ”

While this is an evolving area of law, there are a range of cyber activities that civilians can conduct in support of the war effort without losing the protections of their civilian status. These include, for example, helping organisations defend against cyber threats or improving their cybersecurity, and collecting OSINT and other information about the movement of enemy troops (except where it is done to enable specific military operations against those targets). As such, while most activities of volunteer cyber forces will not constitute ‘direct participation in hostilities’, the risks of

crossing this legal threshold are serious. These risks are exacerbated by the fact that some States may interpret the law differently and therefore adopt a broader approach to what activities result in civilian cyber volunteers losing their protections.

Additionally, States generally have their own laws around whether, for example, civilians can join foreign forces in a conflict, so there may be other legal consequences within one's own country for participating in such activities. Importantly, even though the activities occur in connection with an armed conflict, the normal cybercrime offences remain applicable meaning civilians can violate the law and be prosecuted for their actions either in their own country or in the country where their cyber activities have effects.

For those individuals that nonetheless decide to participate in cyber hostilities during an armed conflict, the International Committee of the Red Cross has provided useful additional guidance about what you should not do. These include not directing cyber attacks against civilian targets, not using malware or similar tools which spread and affect civilian and military systems indiscriminately, and not conducting cyber operations against hospitals and medical facilities (see here for more information: https://blogs.icrc.org/law-and-policy/2023/10/04/8-rules-civilian-hackers-war-4-obligations-states-restrain-them).

6.
SPEECH-RELATED LAWS - DO NOT VIOLATE LAWS REGULATING SPEECH

Members of volunteer cyber forces who engage in information conflicts must take note of speech-related laws. The laws of most States regulate matters such as defamation, subversion, and hate speech. Some States also specifically regulate mis- and dis-information, and some State's laws include specific provisions against election interference. Some also prohibit insults to the king or other leaders. All these types of laws may impact what members of volunteer cyber forces legally may express.

Most States also recognise some form of freedom of expression and where members of volunteer cyber forces are engaged in any attempt to restrict or otherwise limit hostile speech, account must also be taken of such laws. Importantly, the freedom expression is not absolute in any State's law and that right must often be balanced against other important interests such as the protection of the privacy or reputation of others.

Members of volunteer cyber forces must have an understanding of the impact of all these laws from the point of view of the law of the State from which they operate. However, they may also need to be informed of the law of other States with which they come into contact. The violation of foreign law may lead to lawsuits or prosecution in foreign jurisdictions, and even though such actions may have limited

direct impacts due to enforcement difficulties, they may still impact the target e.g., by limiting the places to which they may safely travel.

Bibliography

African Union Peace and Security Council, *Common African Position on the Application of International Law to the Use of Information and Communication Technologies in Cyberspace* (Report, 29 January 2024) https://cyberlaw.ccdcoe.org/wiki/Common_position_of_the_African_Union_(2024)

Ahonen, Aneli and James Pamment, *Beyond Operation Doppelgänger: A Capability Assessment of the Social Design Agency* (12 May 2025)

Ahonen, Aneli and James Pamment, *The Ethics of Outsourcing Information Conflict: Outlining the Responsibilities of Government Funders to their Civil Society Partners* (NATO Strategic Communications Centre of Excellence, Riga) https://stratcomcoe.org/publications/the-ethics-of-outsourcing-information-conflict-outlining-the-responsibilities-of-government-funders-to-their-civil-society-partners/292?ref=disinfodocket.com (accessed 21 July 2025)

Amnesty International, 'Ukraine: Ukrainian Fighting Tactics Endanger Civilians' (4 August 2022) https://www.amnesty.org/en/latest/news/2022/08/ukraine-ukrainian-fighting-tactics-endanger-civilians/

Austin, Greg, 'Australia Needs to Build a Cyber Militia, Says Cyber Expert' *Insurance Business Australia* (online, 1 May 2019) https://www.insurancebusinessmag.com/au/news/breaking-news/australia-needs-to-build-a-cyber-militia-says-cyber-expert-57578.aspx

Bergengruen, Vera, 'How Ukraine Is Crowdsourcing Digital Evidence of War Crimes' (18 April 2022) *Time* https://time.com/6166781/ukraine-crowdsourcing-war-crimes/

Blanchette, Jude et al, *Protecting Democracy in an Age of Disinformation: Lessons from Taiwan* (Report, Center for Strategic and International Studies, 2021)

Blinken, Antony, 'Summit for Democracy Speech on Building a More Resilient Information Environment' (Speech, 2024 Summit for Democracy, 2024) https://www.americanrhetoric.com/speeches/antonyblinkensummitfordemocracy2024.htm (accessed 24 July 2025)

Boothby, William, *The Law of Targeting* (Oxford University Press, 2012)

Bowman, Bradley (ed), *Cognitive Combat: China, Russia, and Iran's Information War Against Americans* (Foundation for Defense of Democracies, 2024)

Brumfield, Cynthia, 'Civilian Cyber Reserves Gaining Steam at the US Federal and State Levels' (24 January 2024) *CSO Online* https://www.csoonline.com/article/1297690/civilian-cyber-reserves-gaining-steam-at-the-us-federal-and-state-levels.html (accessed 20 July 2025)

Buchan, Russell and Nicholas Tsagourias, 'Ukrainian "IT Army": A Cyber Levée en Masse or Civilians Directly Participating in Hostilities?'

(*EJIL: Talk*!, 9 March 2022) https://www.ejiltalk.org/ukranian-it-army-a-cyber-levee-en-masse-or-civilians-directly-participating-in-hostilities

Chang, Wen-Chen and Yu-Teng Ling, 'A Civil Society-Based Approach to Online Misinformation: The Experience of Taiwan' (US-Asia Law Institute, 19 February 2024) https://usali.org/usali-perspectives-blog/a-civil-society-based-approach-to-online-misinformation

CheckCheck.me, 'Auntie Meiyu, your trusted fact checking confidant' (webpage, 25 July 2025) https://www.checkcheck.me/en/

Cheung, Eric, 'Taiwan Faces a Flood of Disinformation from China Ahead of Crucial Election. Here's How It's 'China-Taiwan "Reunification" Is Inevitable, Says Xi' (31 December 2023) *DW* https://www.dw.com/en/china-taiwan-reunification-is-inevitable-says-xi/a-67863888 (accessed 20 July 2025)

Cofacts, 'Homepage' (webpage, 24 July 2025) https://cofacts.tw/

Commonwealth of Australia, Department of the Prime Minister and Cabinet, 2024 Independent Intelligence Review (Report, 2024) https://www.pmc.gov.au/sites/default/files/resource/download/2024-independent-intelligence-review.pdf (accessed 25 July 2025)

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

Crawford, Emily, *Identifying the Enemy: Civilian Participation in Armed Conflict* (Oxford University Press, 2015)

Crawford, James, *The International Law Commission's Articles on State Responsibility: Introduction, Text and Commentaries* (Cambridge University Press, 2002)

Cyber Chats & Chill (Spotify, 2025) https://open.spotify.com/show/67Vr4hudsNweY6AfxjZAe5?si=SrYCzRcDSg2qJ4GtIRuVpg&nd=1&dlsi=35d0b61b6e4f4493

Cyber Forum Kyiv, *A Decade in the Trenches of Cyberwarfare: An Overview of Cyber Operations Targeting Ukraine* (Report, Cyber Forum Kyiv) https://cyberforumkyiv.org/A_Decade_in_the_Trenches_of_Cyberwarfare.pdf

Cybersecurity and Infrastructure Security Agency, *Maryland Defense Force* (webpage, 25 July 2025) https://www.cisa.gov/resources-tools/services/maryland-defense-force

Debunk, 'The Elves' (webpage, accessed 20 July 2025) https://www.debunk.org/about-elves

'Defending Election Integrity in Taiwan' (August 2020) https://www.tca.org.tw/files/Facebook%20Taiwan%20Election%20Report%20ENG.pdf

Den Prystai, ‘From Ukrainians to Ukrainians. 5 Digital Tools and Products Created to Help in Wartime’ (*War Ukraine*, 5 October 2022) https://war.ukraine.ua/articles/digital-tools-created-to-help-in-wartime/

Department of Defence (Cth), ‘Review to Modernise Reserve Force’ (15 July 2025) https://www.defence.gov.au/news-events/news/2025-07-15/review-modernise-reserve-force

Department of Defence (Cth), Strategic Review of the Australian Defence Force Reserves (18 December 2024) https://www.defence.gov.au/about/reviews-inquiries/strategic-review-of-the-adf-reserves

Department of Defense Civilian Cybersecurity Reserve Act, 118th Congress, (2023) https://www.congress.gov/bill/118th-congress/senate-bill/903/text (accessed 20 July 2025)

Estonian Defence League Act (Estonia, consolidated version as of 21 March 2014) https://www.riigiteataja.ee/en/eli/521032014005/consolide

Estonian Defence League, ‘Frequently Asked Questions’ https://www.kaitseliit.ee/en/frequently-asked-questions (accessed 20 July 2025)

‘EU Bans Distribution of Four Russian Media Outlets’, Reuters (18 May 2024) https://www.reuters.com/world/europe/eu-bans-distribution-four-russian-news-outlets-2024-05-17/

Euronews, ‘Ukrainian Brewery Appeals for Molotov Cocktail Donations’ (27 February 2022) https://www.euronews.com/culture/2022/02/27/ukrainian-brewery-in-lviv-appeals-on-social-media-for-molotov-cocktail-donations

Federation of American Scientists, *Collaborative Intelligence: Harnessing Crowd Forecasting for National Security* (Policy Memo, 27 November 2024) https://fas.org/publication/collaborative-intelligence-harnessing-crowd-forecasting-for-national-security/

Fighting Back’ (CNN, 15 December 2023) https://edition.cnn.com/2023/12/15/asia/taiwan-election-disinformation-china-technology-intl-hnk/index.html

Finland, The Act on Voluntary National Defence (556/2007) https://finlex.fi/en/legislation/translations/2007/eng/556 (accessed 21 July 2025)

Finnish Defence Forces, ‘Uuden äärellä: Paikalliskyberpuolustuksen kenttäkoe Rovaniemellä’ (8 September 2023) https://maavoimat.fi/-/uuden-aarella-paikalliskyberpuolustuksen-kenttakoe-rovaniemella- (accessed 21 July 2025)

Forbes, Glenn, Jeff St. Clair and Abbey Marshall, ‘Cleveland Will Be Dealing with Fallout from June Cyber Attack for Weeks, Experts Say’ (26 July 2024) *Ideastream Public Media* https://www.ideastream.org/governmen

t-politics/2024-07-26/cleveland-will-be-dealing-with-fallout-from-june-cyber-attack-for-weeks-experts-say (accessed 20 July 2025)

Förordning (1994:524) om frivillig försvarsverksamhet (SFS 1994:524) (accessed 20 July 2025) https://www.riksdagen.se/sv/dokument-och-lagar/dokument/svensk-forfattningssamling/forordning-1994524-om-frivillig_sfs-1994-524/

Försvarets Radioanstalt (FRO), Grundstadgar för FRO (PDF) https://www.fro.se/_project/_media/FRODOK/FRODOK%20Publik/Dokument/FRO%20Grundstadgar.pdf (accessed 20 July 2025)

Försvarshögskolan, 'About Us' (webpage, 17 July 2025) https://www.fhs.se/en/swedish-defence-university/about-sedu/about-us.html

Försvarsmakten, 'Cyber Defence' (webpage, 27 April 2023) https://www.forsvarsmakten.se/en/about/organisation/cyber-defence/

Försvarsmakten, 'Cybersoldat' (webpage, 17 July 2025) https://jobb.forsvarsmakten.se/sv/utbildning/befattningsguiden/gu-befattningar/cybersoldat/

Försvarsmakten, 'Frivilliga försvarsorganisationer' (accessed 20 July 2025) https://www.forsvarsmakten.se/sv/organisation/frivilliga-forsvarsorganisationer/

Försvarsmakten, 'Frivilligrörelsen får uppdrag inom cyberförsvar och cybersäkerhet' (Högkvarteret, 4 October 2022) https://www.forsvarsmakten.se/sv/aktuellt/2022/10/frivilligrorelsen-far-uppdrag-inom-cyberforsvar-och-cybersakerhetfrivilligrorelsen-far-uppdrag-inom-cyberforsvar-och-cybersakerhet/ (accessed 20 July 2025)

Försvilliga Radioorganisationen (FRO), FRO Lärplattform – campus.fro.se https://campus.fro.se/ (accessed 20 July 2025)

Foundation for Defense of Democracies, '5 Things to Know About ByteDance, TikTok's Parent Company' (12 March 2024) https://www.fdd.org/analysis/2024/03/12/5-things-to-know-about-bytedance-tiktoks-parent-company/

Frivilliga Radioorganisationen (FRO), 'Cyberungdom' https://www.fro.se/web/cyberungdom (accessed 20 July 2025)

Frivilliga Radioorganisationen (FRO), *Grundstadgar* (Fastställda av FRO Riksstämma 2024) https://www.fro.se/_project/_media/FRODOK/FRODOK Publik/Dokument/FRO Grundstadgar.pdf (accessed 20 July 2025)

g0v Taiwan, 'About g0v' (webpage, 24 July 2025) https://g0v.tw/intl/en/

Geneva Convention Relative to the Treatment of Prisoners of War, opened for signature 12 August 1949, 75 UNTS

135 (entered into force 21 October 1950)

Gupta, Kritvi, 'Beyond Censorship: Taiwan's Model for Combating Disinformation' (14 March 2024) *Foreign Affairs Review* https://www.foreignaffairsreview.com/home/beyond-censorship-taiwans-model-for-combating-disinformation

Haataja, Samuli and Dan Svantesson, 'Cyberspace and National Security' in Danielle Ireland-Piper (ed), *National Security Law in Australia* (The Federation Press, 2024)

Haataja, Samuli, 'Cyber Operations against Critical Infrastructure under Norms of Responsible State Behaviour and International Law' (2022) 30(4) *International Journal of Law and Information Technology* 423

Hague Convention (V) respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land, opened for signature 18 October 1907, 205 CTS 299 (entered into force 26 January 1910)

Hird, Karolina et al, 'Russian Offensive Campaign Assessment, 5 January 2023' (Institute for the Study of War, 5 January 2023) https://www.understandingwar.org/backgrounder/russian-offensive-campaign-assessment-january-5-2023

Holmes, Dan, 'Taiwan is Building a Government AI Hivemind' (The Mandarin, 21 August 2024) https://www.themandarin.com.au/253059-taiwan-is-building-a-government-ai-hivemind/

Hsu, Kuang-Cheng and Calvin Chu, 'Taiwan Bolsters Whole-of-Society Defense Resilience' (*Jamestown Foundation*, 29 April 2025) https://jamestown.org/program/chinese-military-drill-escalates-tensions-underscoring-taiwans-commitment-to-whole-of-society-defense-resilience/

'Is Humour the Key to Better AI Governance? Audrey Tang Thinks So' (*Apolitical*, 25 February 2025) https://apolitical.co/solution-articles/en/is-humour-the-key-to-better-ai-governance-audrey-tang-thinks-so

International Committee of the Red Cross*, Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law (ICRC, 2009)*

Jensen, Mikkel Storm, 'Sector Responsibility or Sector Task? New Cyber Strategy Occasion for Rethinking the Danish Sector Responsibility Principle' (2018) 1(1) *Scandinavian Journal of Military Studies* 1

Joseph Menn, 'Hacking Russia Was Off-Limits. The Ukraine War Made It a Free-for-All' *Washington Post* (online, 1 May 2022) https://www.washingtonpost.com/technology/2022/05/01/russia-cyber-attacks-hacking/

Kaska, Kadri, Anna-Maria Osula and Jan Stinissen, *The Cyber Defence Unit of the Estonian Defence League: Legal, Policy and Organisational Analysis* (NATO Cooperative Cyber Defence Centre of Excellence, 2013)

Kosonen, Jarkko and Juha Mälkki, 'The Finnish Model of Conscription: A Successful Policy to Organize National Defence' in Caroline de la Porte and others (eds), *Successful Public Policy in the Nordic Countries* (Oxford University Press, 2022)

KTH Royal Institute of Technology, 'Centre for Cyber Defence and Information Security' (19 March 2025) https://www.kth.se/cdis

Kuang-shun, Yang, 'What Lessons Can Taiwan Share with the World on Election Interference?' (Brookings Institution, 11 June 2024) https://www.brookings.edu/articles/what-lessons-can-taiwan-share-with-the-world-on-election-interference/

KyberVPK, 'Checklist for Victims of a Data Breach' (8 November 2020) https://kybervpk.fi/en/releases/checklist-for-victims-of-a-data-breach/ (accessed 20 July 2025)

KyberVPK, 'Frequently Asked Questions' https://kybervpk.fi/en/faq/ (accessed 20 July 2025)

KyberVPK, 'Team Members' https://kybervpk.fi/en/people/ (accessed 20 July 2025)

Lee, Yimou, 'Chinese Cyberattacks on Taiwan Government Averaged 2.4 Million a Day in 2024, Report Says' (6 January 2025) *Reuters* https://www.reuters.com/technology/cybersecurity/chinese-cyberattacks-taiwan-government-averaged-24-mln-day-2024-report-says-2025-01-06/

Liao, Kitsch Yen-Fan, 'Taiwan Focuses on Societal Resilience and U.S. Cooperation in New Defense Review' (*Jamestown Foundation*, 28 April 2025) https://jamestown.org/program/taiwan-focuses-on-societal-resilience-and-u-s-cooperation-defense-review

Lonergan, Erica and Mark Montgomery, *United States Cyber Force: A Defense Imperative* (Foundation for Defense of Democracies, March 2024)

Maanpuolustuskoulutus MPK, *Maanpuolustuskoulutusyhdistys MPK* https://mpk.fi/en/ (accessed 24 July 2025)

Mačák, Kubo, 'Will the Centre Hold? Countering the Erosion of the Principle of Distinction on the Digital Battlefield' (2023) 105(923) *International Review of the Red Cross* 965

Mahdawi, Arwa, 'Humour over Rumour? The World Can Learn a Lot from Taiwan's Approach to Fake News' (*The Guardian*, 17 February 2021) https://www.theguardian.com/commentisfree/2021/feb/17/humour-over-rumour-taiwan-fake-news

Massingham, Eve and Annabel McConnachie (eds), *Ensuring Respect for International Humanitarian Law* (Routledge, 2020)

McGrath, Lachlan, 'Keyboard Warriors: An Australian Volunteer Cyber Corps' (5 March 2023) *National Institute for Cybersecurity Research* https://www.nisr.org.au/article/keyboar

d-warriors-an-australian-volunteer-cyber-corps

McInnis, Kathleen, Seth G Jones and Emily Harding, 'NAFO and Winning the Information War: Lessons Learned from Ukraine' (Center for Strategic and International Studies, 5 October 2022) https://www.csis.org/analysis/nafo-and-winning-information-war-lessons-learned-ukraine

McWilliams, Anna, *Bibliotekens roll i det civila försvaret* (Report, Totalförsvarets forskningsinstitut, November 2024) https://www.foi.se/rest-api/report/FOI Memo 8635

Michigan Compiled Laws, *Act 132 of 2017* (enacted 24 January 2018) https://www.legislature.mi.gov/documents/mcl/pdf/mcl-Act-132-of-2017.pdf (accessed 20 July 2025)

Mitchell, Olivia, 'Nat'l Guard Assisted on Cleveland Municipal Court Cyber Attack' (5 March 2025) *GovTech* https://www.govtech.com/security/natl-guard-assisted-on-cleveland-municipal-court-cyber-attack (accessed 20 July 2025)

MyGoPen, *MyGoPen ／麥擱騙* (webpage, 25 July 2025) https://www.mygopen.com/

Myndigheten för samhällsskydd och beredskap (MSB), 'MSB – The Swedish Civil Contingencies Agency' (webpage, 17 July 2025) https://www.msb.se/en/

National Governors Association, Re-Envisioning State Cyber Response Capabilities: The Role of Volunteers in Strengthening Our Systems (Report, June 2022) https://www.nga.org/wp-content/uploads/2022/06/Cyber_Civilian_Corps_14June2022.pdf

Office of the President, Republic of China (Taiwan), 'President Lai Observes 2025 Whole-of-Society Defense Resilience Committee Field Exercises' (27 March 2025) https://english.president.gov.tw/NEWS/6933

Office of the President, Republic of China (Taiwan), *Minutes of the 1st Meeting of the Office of the President Whole-of-Society Defense Resilience Committee* (26 September 2024) https://english.president.gov.tw/File/Doc/9d77c4fa-2d84-49ca-8449-e590e1d1ef5c (accessed 20 July 2025)

Office of the President, Republic of China (Taiwan), *Minutes of the 2nd Meeting of the Whole-of-Society Defense Resilience Committee* (26 December 2024) 10 https://english.president.gov.tw/File/Doc/2d7d0a85-9f20-4396-9fb0-3ed2e60136f5 (accessed 20 July 2025)

Office of the President, Republic of China (Taiwan), *Minutes of the 3rd Meeting of the Office of the President Whole-of-Society Defense Resilience Committee* (27 March 2025) https://www.president.gov.tw/File/Doc/c1153ad7-c850-4e23-baec-98cf402c5127

Ohio Cyber Range Institute, *Capability Statement* (April 2023)

https://www.ohiocyberrangeinstitute.org/_files/ugd/63659b_f99c01a55c4d40558896754bfc118483.pdf (accessed 20 July 2025)

Ohio Cyber Reserve, 'About' https://ohcr.ohio.gov/about (accessed 20 July 2025)

Ohio Revised Code (US) https://law.justia.com/codes/ohio/2024/

Ole Valmis, *Ole Valmis* (webpage, 25 July 2025) https://www.olevalmis.ee/en

PBS, 'How Taiwan Preserved Election Integrity by Fighting Back Against Disinformation' (27 January 2024) https://www.pbs.org/newshour/world/how-taiwan-preserved-election-integrity-by-fighting-back-against-disinformation

Pejic, Jelena, 'Extraterritorial Targeting by Means of Armed Drones: Some Legal Implications' (2014) 96(893) *International Review of the Red Cross* 67

Räddningsverket (Myndigheten för samhällsskydd och beredskap), *Handbok i krisberedskap: Struktur för myndigheters och kommuners planering* (MSB rapport RIB 2023:12, 2023) https://rib.msb.se/filer/pdf/30951.pdf (accessed 20 July 2025)

Riksrevisionen, *Government Control of National Information and Cyber Security – Both Urgent and Important* (Summary, 13 April 2023) https://www.riksrevisionen.se/download/18.2008b69c18bd0f6ed3f26657/1686569981836/RiR_2023_8_summary.pdf (accessed 20 July 2025)

Schmitt, Michael N and William Casey Biggerstaff, 'Ukraine Symposium – Are Civilians Reporting With Cell Phones Directly Participating in Hostilities?' (*Articles of War*, 2 November 2022) https://lieber.westpoint.edu/civilians-reporting-cell-phones-direct-participation-hostilities

Schmitt, Michael N, 'Deconstructing Direct Participation in Hostilities: The Constitutive Elements' (2010) 42(3) *New York University Journal of International Law and Politics* 697

Schmitt, Michael N, 'Extraterritorial Lethal Targeting: Deconstructing the Logic of International Law' (2013) 52(1) *Columbia Journal of Transnational Law* 77

Schmitt, Michael N, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press, 2017)

Schreiber, Mark E et al, *Creating a Cyber Volunteer Force: Strategy and Options* (Report, McDermott Will & Emery, March 2023) https://www.mwe.com/insights/creating-a-cyber-volunteer-force-strategy-and-options

Singleton, Craig, 'China' in Bradley Bowman (ed), *Cognitive Combat: China, Russia, and Iran's Information War Against Americans* (Foundation for Defense of Democracies, 2024)

Soesanto, Stefan, *The IT Army of Ukraine: Structure, Tasking, and Ecosystem* (Report, Centre for Security

Studies, 2022) https://css.ethz.ch/en/publications/risk-and-resilience-reports/details.html?id=/t/h/e/i/the_it_army_of_ukraine

Stradner, Ivana and John Hardie, 'Russia' in Bradley Bowman (ed), *Cognitive Combat: China, Russia, and Iran's Information War Against Americans* (Foundation for Defense of Democracies, 2024)

Svantesson, Dan, 'Legal Safeguards for the Volunteers of Ukraine's Cyber Militia' (*Verfassungsblog on Matters Constitutional*, 23 March 2022) https://verfassungsblog.de/legal-safeguards-for-the-volunteers-of-ukraines-cyber-militia/ (accessed 21 July 2025)

Svantesson, Dan, 'Regulating a "Cyber Militia" – Some Lessons from Ukraine, and Thoughts about the Future' (2023) 6(1) *Scandinavian Journal of Military Studies* 86

Swedish Armed Forces, 'Vykort från ett land i väntans tider' (webpage, 25 July 2025) https://www.forsvarsmakten.se/sv/information-och-fakta/var-historia/artiklar/vykort-fran-ett-land-i-vantans-tider/

Swedish Civil Contingencies Agency, *If Crisis or War Comes* (2024) https://www.msb.se/sv/publikationer/om-krisen-eller-kriget-kommer-pa-engelska/

Taiwan Cybersecurity Agency, *Facebook Taiwan Election Report* (PDF, n.d.) https://www.tca.org.tw/files/Facebook%20Taiwan%20Election%20Report%20ENG.pdf (accessed 27 July 2025)

Taiwan Executive Yuan, 'Measures to Prevent the Harm of Misinformation' (防制假訊息危害因應作為) (in Chinese) (Executive Yuan, accessed 24 July 2025) https://www.ey.gov.tw/Page/448DE008087A1971/c38a3843-aaf7-45dd-aa4a-91f913c91559

Taiwan FactCheck Center, '2024 Presidential Election: Combating Disinformation with Fact-Checks, Media Collaboration, and Public Empowerment' (webpage, 25 December 2023) https://en.tfc-taiwan.org.tw/en_tfc_288/

Taiwan FactCheck Center, 'Who We Are' (webpage, 25 July 2025) https://en.tfc-taiwan.org.tw/en_tfc_298/

Taiwan FactCheck Center, Taiwan FactCheck Foundation (English Website) (webpage, 25 July 2025) https://en.tfc-taiwan.org.tw/

Taiwan Ministry of National Defense, Taiwan's 2025 Quadrennial Defense Review (March 2025) https://tsm.schar.gmu.edu/wp-content/uploads/2025/03/Taiwans-2025-QDR.pdf

Taiwan, *National Security Bureau, Analysis on China's Cyberattack Techniques in 2024* (5 January 2025) https://www.nsb.gov.tw/en/#/%E5%85%AC%E5%91%8A%E8%B3%87%E8%A

8%8A/%E6%96%B0%E8%81%9E%E7%A8%BF%E6%9A%A8%E6%96%B0%E8%81%9E%E5%8F%83%E8%80%83%E8%B3%87%E6%96%99/2025-01-05/Analysis%20on%20China's%20Cyberattack%20Techniques%20in%202024 (accessed 20 July 2025)

Te-chin, Liu*, 2025 Society-wide Defense Resilience Commission Field Exercise Observation Report* (2025 全社會防衛韌性委員會 實地演練觀察報告) (National Security Council Deputy Secretary-General, 2025) https://www.president.gov.tw/File/Doc/0c5cf1c5-cc5e-40cf-9d5d-48b9c75d5722

Texas Department of Information Resources, *Texas Volunteer Incident Response Team* (webpage, 25 July 2025) https://dir.texas.gov/information-security/cybersecurity-incident-management-and-reporting/texas-volunteer-incident

Tikk, Eneken, 'Civil Defence and Cyber Security: A Contemporary European Perspective' in Greg Austin (ed), *National Cyber Emergencies: The Return to Civil Defence* (Taylor & Francis, 2020)

Tobin, Meaghan and Amy Chang Chien, 'Taiwan, on China's Doorstep, Is Dealing with TikTok Its Own Way' (The New York Times, 16 May 2024) https://www.nytimes.com/2024/05/16/business/tiktok-taiwan.html

Totalförsvarets forskningsinstitut (FOI), *Glimt – vår nya vapen* (Glimt digital platform, launched January 2025) https://glimt.nu/ (accessed 20 July 2025)

United Nations Executive Office of the Secretary-General, UN Global Risk Report (Report, February 2024) https://unglobalriskreport.org/UNHQ-GlobalRiskReport-WEB-FIN.pdf

United Nations, Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security (Report, A/76/135, 14 July 2021)

United States Department of State, 'About Us – Global Engagement Center' (webpage, 24 July 2025) https://2021-2025.state.gov/about-us-global-engagement-center-2/

US Cyberspace Solarium Commission, *Building a Trusted ICT Supply Chain* (Report, October 2021)

US Cyberspace Solarium Commission, *Final Report* (March 2020)

US Department of Defense, *Military and Security Developments Involving the People's Republic of China* (Report, 18 December 2024) https://media.defense.gov/2024/Dec/18/2003615520/-1/-1/0/MILITARY-AND-SECURITY-DEVELOPMENTS-INVOLVING-THE-PEOPLES-REPUBLIC-OF-CHINA-2024.PDF (accessed 20 July 2025).

US National Commission on Military, National, and Public Service, *The Final Report of the National Commission on Military, National, and Public Service* (March 2020)

Väljataga, Ann, *Cyber Vigilantism in Support of Ukraine: A Legal Analysis* (Report, NATO Cooperative Cyber Defence Centre of Excellence, March 2022) https://ccdcoe.org/uploads/2022/04/Cyber-vigilantism-in-support-of-Ukraine-a-legal-analysis.pdf (accessed 21 July 2025)

Weinberg, Michael, '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/ (accessed 21 July 2025)

Wisconsin Emergency Management, *Wisconsin Cyber Response Team* (webpage, 25 July 2025) https://wem.wi.gov/wisconsin-cyber-response-team

Wither, James Kenneth, 'Back to the Future? Nordic Total Defence Concepts' (2020) 20(1) Defence Studies 61