SOCIAL CYBER INSTITUTE

Discussion Paper 1/24

Crowdsourcing an Australian cyber intelligence and information militia

Dan Jerker B. Svantesson

June 2024

SOCIAL CYBER INSTITUTE

Discussion Paper 1/24

Crowdsourcing an Australian cyber intelligence and information militia

A call for civilian reserves in hybrid warfare

Dan Jerker B. Svantesson

June 2024

ABOUT THE AUTHOR

Dan Jerker B Svantesson is a Senior Fellow with the Social Cyber Institute. He specialises in international aspects of the IT society, a field within which he has authored or co-authored more than 280 publications, and given presentations in Australia, Asia, Africa, North America, and Europe. Dan is a Professor at the Faculty of Law in Bond University where he is a co-director for the Centre for Space, Cyberspace & Data Law. He is an Associated Researcher at the Swedish Law & Informatics Research Institute, Stockholm University, he 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 authored and contributed to commissioned reports by several international organisations including the UNODC, OECD, UNCTAD, the Commonwealth Secretariat, and the Internet & Jurisdiction Policy Network. He has been identified as the Field Leader for "Technology Law" in studies published by League of Scholars together with *The Australian* for four years (2021, 2020, 2019, 2018), and has given expert opinions before leading courts such as the Court of Justice of the European Union.

ABOUT THE SOCIAL CYBER INSTITUTE

The Social Cyber Institute (SCI) creates new social science insights to complement technology in the fight for a more secure cyberspace. SCI is a non-profit organisation supported by the Social Cyber Group which offers advisory and training services in cyber policy.

ACKNOWLEDGEMENTS

The author would like to acknowledge comments on the draft paper by Professor Glenn Withers AO and Professor Greg Austin, co-founders of the Social Cyber Institute. The author is also grateful for feedback received from the anonymous reviewer as well as from Samuli Haataja, William van Caenegem, Wendy Bonython, and for helpful discussions held with Lachlan McGrath and Franz Carneiro Alphonso on the topic of cyber militias in general. The views are those of the author alone.

ABSTRACT

Australia's cyber environment is under constant attack. The threats are multifaceted and growing. Beyond the well-known cybercrime and cybersecurity challenges, we face a barrage of online mis- and dis-information aimed at undermining our social cohesion. Despite increased emphasis on the cyber domain, our existing public and private capacity is likely insufficient to counter the full range of threats we face in cyberspace. Against this background, Australia must adopt a whole-of-society approach to the defence of the cyber environment. This discussion paper seeks to canvass options for an Australian 'cyber intelligence and information militia'; that is, a 'crowdsourced' civilian volunteer cyber reserve capability fit to engage in open-source intelligence (OSINT) and information warfare. Such a resource could play an important role in supplementing existing or developing capabilities.

Contents

Introduction

Australia's cyber environment is under constant attack and its protection is a whole-of-society concern. The threats are multifaceted and growing. Beyond the well-known cybercrime and cybersecurity challenges, we face a barrage of online mis- and dis-information aimed at undermining our social cohesion.

While Australia is expanding its cyber capabilities in various ways – such as via the REDSPICE initiative that provides in broad terms for a doubling of the budget for cyber defence[1] – our existing public and private capacity is likely insufficient to counter the full range of threats we face in cyberspace. Put bluntly, more is needed and this need is growing rapidly.

Against this background, Australia must adopt a whole-of-society approach to the defence of the cyber environment. A 'crowdsourced' civilian volunteer cyber reserve capability – fit to engage in open-source intelligence (OSINT) and information warfare – could play an important role in this approach supplementing existing or developing, capabilities. To that end, this discussion paper seeks to canvass options for an Australian 'cyber intelligence and information militia'. The discussion is focused on structural and organisational issues regarding such a body, as well as the roles it can play, the risks involved, and the key legal considerations.

Cyber defence – but not just cybersecurity

Some foreign States, such as Estonia, have already established cyber reserve capabilities,[2] and calls to develop a (civilian) cyber reserve capability for Australia are not new. In his ground-breaking work on the topic (dating back to 2016), Greg Austin envisaged a comprehensive 'cyber civil defence force (militia)'[3] noting that such a body could:

> "1. Be the national authority for civil sector dependency mapping of Australia's critical information infrastructure, its data resources and its transmission flows, including international dependencies.
> 2. Provide an auxiliary capability in a disciplined command structure [separate from Border Force] for national civil and military defence response to extreme cyber emergencies.
> 3. Develop, monitor and manage a response system for handling cyber threats to critical national, state and local infrastructure.
> 4. Develop, monitor and manage a national response system for handling serious cyber crime that may affect the national economy or social infrastructure."[4]

More recently, Lachlan McGrath also discussed the possibility of a 'Volunteer Cyber Corps'. He argues that:

> "The Australian government should establish a part-time, volunteer Civilian Cyber Corps under the jurisdiction of the ACSC [Australian Cyber Security Centre]. This organisation should have a responsibility to support preparatory cyber security uplift for government and non-profit entities, as not to undermine Australia's nascent cyber security industry. The Civilian Cyber Corps should also seek training and incident response outcomes."[5]

One commonality between all the interesting Australian proposals to-date is that they are focused on cybersecurity, seeking to utilise the existing expertise of those members of society who already have adequate technical training to engage with the often complex cybersecurity issues. This paper fully agrees that Australia should develop such cybersecurity-focused reserve capabilities, and in doing so should confront several key questions, such as whether such a body forms part of the Defence structure or not, and how to avoid unduly undermining the private sector's own cybersecurity capabilities at times of crisis. It is also the case that more efforts could usefully be directed at coordination with the (partly foreign) private sector that plays a central role in the Australian cyber domain.[6]

The proposal advanced in this Paper,[7] however, is different. It assigns a broader set of roles to the proposed civilian cyber reserve capability, allowing the involvement of a broader section of the Australian public. This is a significant difference reflecting the diversity of the attacks directed at the Australian cyber environment, including mis- and dis- information. Thus, what is proposed here can supplement the type of cybersecurity-focused reserve capability that has been previously discussed in Australia.

There are credible activities by researchers, NGOs and journalists that monitor and analyse information operations against Australia but these lack a coordinated structure with a proactive agenda, and a focal point for national efforts such as we see in some other countries. Thus, what is proposed here is something new, and it supplements rather than competes with existing initiatives.

Australia's population is relatively small, but it is a population with a generally high level of education. To-date, this is an under-exploited resource in defence against information warfare as well as in OSINT, and given the hardening international climate in which we find ourselves, we no longer can afford to ignore this resource.

Crowdsourcing a civilian cyber capability

The potential willingness to take part in a structure like that proposed above is perhaps best illustrated by the fact that some Australians are already actively volunteering in the ongoing information war online. The most well-known example of this is the so-called 'North Atlantic Fella Organization', or 'NAFO'. NAFO is a virtual community of like-minded people that was formed in response to the Russian 2022 full-scale invasion of Ukraine. Its members engage in the following activities "countering Russian propaganda and disinformation; trolling of Russian officials and official Russian organizations; support of Ukrainian officials and organizations; and fundraising to support Ukraine and its army."[8]

More broadly, Australians have a proud tradition of volunteering for worthy causes in the interest of community safety and national security. We see that, for example in the organisation of 'Neighbourhood Watch' and in the state emergency services.[9] Another interesting example is found in the 'coast watchers' – a volunteer OSINT structure formed after World War I. Equipped with radios, the coast watchers were tasked with providing early warning in the South Pacific.[10] Indeed, in honour of the significant contribution made to Australia's defence by the 'coast watchers', perhaps the proposed 'cyber intelligence and information militia' discussed here could be referred to as the 'cyber watchers'? The naming issue should, however, not be allowed to become a distraction and at least for now, I will continue referring to it as the Australian 'cyber intelligence and information militia'. At any rate, the examples above may arguably suggest that Australians may also be willing to volunteer in relation to an Australian 'cyber intelligence and information militia'.

Many Australians who lack *cybersecurity* training can still help strengthen our defence in the cyber environment. Indeed, anyone with time, patience, and basic computer literacy can play a role in OSINT and information warfare. Thus, the proposal seeks to capture, and make use of, a broad section of the Australian public. In essence, the idea is to 'crowdsource' a civilian cyber capability where each member focuses on tasks within their specific competencies.

With that in mind, what is proposed here is a 'cyber militia' that undertakes defence-related activities (broadly defined) in or pertaining to cyberspace on behalf of the Commonwealth, with the Commonwealth's formal recognition, and under the coordination and guidance of the Commonwealth, but outside the ambit of Australia's regular armed forces or national security structure. Obviously, this would require a degree of risk and associated trust but that should not be difficult to manage (I explore risk mitigation in more detail below).

Given it being formally recognised by Australia, the cyber militia envisaged here is different from the non-state – often criminal – actors we commonly see engineering cybersecurity breaches. Those non-state actors may enjoy a symbiotic relationship, and possibly a degree of coordination, with state actors, while affording that state plausible deniability by maintaining an appearance of distance from the state in question. In contrast, the proposed Australian 'cyber intelligence and information militia' would operate openly and be formally recognised by the Australian government. This also distinguishes the proposed cyber militia from the activities by bodies such as NAFO discussed above, and by cyber vigilantes, since they are neither acting on behalf of a state, nor with that state's formal recognition or coordination. Additionally, under the definition advanced above, the proposed Australian 'cyber intelligence and information militia' is different to the staff of the military and national security branches and is different to conscripted 'cyber warriors' and the type of 'cyber home guard' used in, for example, the Estonian Defence League's Cyber Unit and the Swedish Home Guard which form part of these countries' national armed forces.[11]

'Control via objectives lists'

A 'cyber militia' of the type envisaged here must be able to operate effectively without direct persistent control and guidance. In the light of that, 'control via objectives lists' seems to be best suited to management and coordination of cyber militia activities. This will involve the relevant body within the Australian government that organises the cyber militia posting a list of government-approved objectives on an appropriate communications medium,[12] and cyber militia members then seeking to achieve those government-approved objectives to the best of their abilities within the predetermined parameters of their operations. Depending on the type of objective the process may also include cyber militia members reporting-back, to the relevant body within the Australian government that organises the cyber militia, on the outcome.

Adopting the 'control via objectives lists' approach comes with several strong advantages and one serious limitation. These are discussed further below (see 'Risks and risk mitigation').

Roles of a 'cyber intelligence and information militia'

As noted by Storm Jensen, a state can principally seek to defend its society in the cyber domain through deterrence, protection, and resilience.[13] A 'cyber intelligence and information militia' can play a role in all three through several different types of activities.

It is possible to envisage a wide range of roles that a 'cyber militia' could perform. Here the focus is on OSINT and information warfare as they seem most central and best suited to the proposed 'cyber intelligence and information militia'. However, a few words are also noted about a possible third potential role; namely, 'cyber espionage'. In addition, while going beyond what is proposed here, a fourth and a fifth potential role are also briefly noted below; that is, 'cyber-attacks' and 'systems support'. However, such roles may be best reserved for a cybersecurity-focused cyber reserve and, of course, existing bodies within Australia's defence structure.

Open-source intelligence (OSINT)

One consequence of the information explosion that has occurred over recent years is that much information of national security interest may be gathered open-source.[14] As noted 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 insights from vast amounts of open source data will only increase in importance."[15]

OSINT may utilise a range of data sources such as social media postings, flight radar trackers, satellite and image maps. Such sources may enable members of an Australian 'cyber intelligence and information militia' to identify developing threats and to track troop movements (analogous to what the coast watchers did) and report these activities.

The proposed Australian 'cyber intelligence and information militia' could, for example, also facilitate the estimation of enemy casualties based on social media postings – a resource-intensive task requiring comparatively limited OSINT skills. Beyond traditional OSINT, there is some potential for a cyber militia to engage in the active production of new intelligence e.g., through means such as the use of private drones.

Importantly, the OSINT role of a cyber militia may also 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.[16]

A cyber militia 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.

Information warfare

An Australian 'cyber intelligence and information militia' may be a valuable tool both for defensive and offensive information warfare.

It seems clear that states are now in a constant state of information warfare.[17] 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.[18] This is a major concern, and the Australian Electoral Commission has recently expressed concerns about its ability to detect and deter AI-generated misinformation at the next federal election, potentially from overseas actors.[19]

An Australian 'cyber intelligence and information militia' can 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.

A perhaps equally important information warfare role for a cyber militia is the influencing of the narrative in both traditional and social media. The Ukraine war is highly illustrative here. Without in any sense downplaying or undermining the importance of the Ukrainian military, it may be argued that the current war will 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 'cyber intelligence and information militia' can be used to steer the narrative, to fact-check, and to point out inaccuracies in, and counter, enemy propaganda. Relatedly, a 'cyber intelligence and information militia' 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, and in relation to all these tasks, people are more effective than the 'bots' commonly utilised by several States.

In addition to the, largely defensive, information warfare tasks outlined above, an Australian 'cyber intelligence and information militia' could undertake certain offensive operations. An illustration of this can be found in the fact that, at the start of the Russian 2022 full-scale invasion of Ukraine, individuals started posting pictures and information about the war on Russian websites, such as hotel and restaurant review sites, with the aim of alerting the Russian public to what was, and still is, occurring in Ukraine. A 'cyber intelligence and information militia' could undertake such offensive information measures and others like it.

Cyber espionage

An Australian 'cyber intelligence and information militia' may potentially also be enabled to engage in cyber espionage based on 'hacking'. Examples from overseas include instances of civilians gaining access to security cameras to support 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 arguably 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, a consideration which favours a cyber militia.

'Cyber-attacks'

A 'cyber intelligence and information militia' could potentially be used to carry out what broadly may be termed 'cyber-attacks' against designated targets. Such attacks may range from relatively simple denial-of-service attacks to more sophisticated attacks that qualify as 'armed attack' under international humanitarian law (IHL); that is, the set of rules which seek to limit the effects of armed conflict.[20]

A State's ability to deploy a cyber militia undertaking targeted cyber-attacks may be a significant deterrent for a potential attacker. Thus, it may be worthwhile to keep the door open for assigning this role to the members of the proposed 'cyber intelligence and information militia' in times of conflict, while bearing in mind that only a comparatively smaller number of the members may possess the skill set necessary to be able to undertake such work. However, other bodies are clearly better suited for this role and the proposed 'cyber intelligence and information militia' should only ever be considered an emergency supplement if ever allowed to engage in this role.

Systems support

Some members of a 'cyber intelligence and information militia' may have appropriate qualifications to be tasked with simple systems support and cybersecurity roles in a time of crisis. Where members are properly vetted and trained, they may undertake tasks such as keeping an open network operating from community resources such as libraries ensuring Internet connectivity for the Australian public where their normal connections are interrupted. Obviously, however, the support of sensitive systems must be kept in the hands of employed experts.

Having said this, the need for vetting members for this role may make it unsuitable for the structure proposed for the 'cyber intelligence and information militia'. Thus, especially if a separate cybersecurity-focused civilian reserve is created, the systems support role may be left to bodies other than the proposed 'cyber intelligence and information militia'.

It is no doubt possible to envisage additional roles for the proposed 'cyber intelligence and information militia'. However, a cyber militia capable of performing even some of these roles would provide highly valuable deterrence, protection, and resilience. Finally, it may be noted that, as a body aimed at feeding intelligence to Australia's intelligence structure rather than receiving intelligence from it, there will be no need for cyber militia members to gain security clearance.

The structure of a 'cyber intelligence and information militia'

From a structural perspective, there are multiple possibilities when it comes to governance of the activity of the proposed 'cyber intelligence and information militia'. This paper does not aim to express a view on the topic of where, within the Australian government, control over the Australian 'cyber intelligence and information militia' may best be placed. However, it needs to be reemphasised that the envisaged 'cyber intelligence and information militia' is to sit outside the ambit of Australia's regular armed forces or national security structure. It should also be noted that the exact roles in which the Australian 'cyber intelligence and information militia' may engage may depend on what body is tasked with overseeing its activities.

The paper has been drafted based on the assumption that a 'cyber intelligence and information militia' would be managed on the Commonwealth level. However, it ought to be acknowledged that one may, of course, also envisage a state-based organisation instead. Indeed, even if the proposed 'cyber intelligence and information militia' would be managed on the Commonwealth level important questions arise as to what extent the activities overlap with e.g., policing and emergency management – matters addressed on a state level to a great degree. These are matters that must be addressed in detail, but go beyond the scope of this initial discussion paper.

Risks and risk mitigation

There are obvious risks associated with the creation of a 'cyber intelligence and information militia'. While these risks must be taken seriously, they may all be mitigated.

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. The proposed 'control via objectives lists' structure ensures that the body governing the 'cyber intelligence and information militia' can delineate what the cyber militia can and cannot do. Any member of the cyber militia that undertakes activities not conforming to the list of government-approved objectives is simply not acting in the capacity of a cyber militia member and would not enjoy any of the safeguards afforded to members. Thus, a militia member 'going rogue' may be liable to prosecution in the same manner as members of the public may be today.

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. A formally recognised cyber militia ensures 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, such as criminals unofficially doing work for a state.

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

Infiltration

The proposed 'control via objectives lists' structure comes with at least one noteworthy disadvantage; infiltration is all but guaranteed. A foreign power would quite easily be able to have its agents operating in Australia enlist in the Australian 'cyber intelligence and information militia' and would then be able to learn about what is included on the list of government-approved objectives. This must be kept in mind, and it must guide the types of tasks a cyber militia is assigned, as well as how the directions are worded.

Having said that, it is not difficult to formulate objectives that can be effectively pursued by a 'cyber intelligence and information militia' even where the enemy is aware of those objectives.

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 a 'cyber intelligence and information militia' for such purposes. Safeguarding against such a development is crucial.

Thus, just as Australian society has adopted structural safeguards (e.g., oversight[21]) against such practices in various ways, the risk of an abusive utilisation of an Australian 'cyber intelligence and information militia' may be managed by similar safeguards.

Furthermore, the proposed 'control via objectives lists' structure ensures complete transparency as to how Australia uses its 'cyber intelligence and information militia'. This transparency is a powerful tool to address the risk of abuse. In this context, it may also be noted that, any unlawful conduct by cyber militia members can be attributed to Australia under international law on state responsibility as long as the activity corresponds to what has been communicated via the 'objectives lists'.

Risk to individual members

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 cyber militia, it ought to provide appropriate legal safeguards for the participants of that militia. Thus, a practice of states designating individuals as members of their 'cyber militia' has direct benefits for the individuals in question.

Under the proposed structure, members of Australia's 'cyber intelligence and information militia' would be afforded protection in the form of legal indemnity. But it needs to be re-emphasised that where members of the cyber militia undertake any activities not conforming to the objectives list, they are not acting in the capacity of a cyber militia member and these legal safeguards do not apply.

Support from and to our allies

The discussion so far has focused on the creation of an Australian 'cyber intelligence and information militia'. However, it is also appropriate to consider two related issues, namely that of:

(1) Australians' engaging in the operations of a foreign cyber militia; and
(2) Foreigners joining an Australian 'cyber intelligence and information militia'.

The reason these matters cannot be ignored in the discussion is found in the fact that an Australian 'cyber intelligence and information militia' could benefit greatly from the 'surge capacity' that could be obtained by opening participation to citizens of allied countries; at least at a time of crisis. Similarly, Australia could take steps to facilitate Australians providing a surge capacity for the cyber militias of our allies. As noted by Austin and Khaniejo: "national cyber defence is more easily achieved […] through alliances (with like-minded countries)."[22] Current discussions about the option for Australia to recruit Defence staff from allies may be said to support this notion.

The sort of cyber militia cooperation canvassed above raises some legal issues under international law (see *Legal issues and solutions* below).

Legal issues and solutions

In setting up an Australian 'cyber intelligence and information militia', account must be taken of applicable international law including rules regarding use of force, the non-intervention principle, sovereignty, proportionality, and necessity. These matters are discussed in more detail elsewhere,[23] and it is not the intention to get into details here. However, two key considerations deserve special mention.

The principle of distinction

The principle of distinction requires that parties to an armed conflict at all times distinguish between civilians and combatants and between civilian objects and military objectives.[24] While a central feature of IHL, this principle is increasingly difficult to maintain, not least in the cyber domain.[25] In this context we must, however, draw a clear distinction that has not always been sufficiently noted in the debates; that is, while the principle of distinction remains of central importance for guiding the behaviour of those engaging in cyber-attacks, the situation is more complicated for defenders.

When attacks on a State's cyber environment is a whole-of-society matter, it is hard to see how the cyber defence could be anything but a whole-of-society matter. Thus, calls to keep civilians out of the cyber defence are unrealistic and do not stand in the way of the formation of an Australian 'cyber intelligence and information militia'. Rather, it may help shape the lists of government-approved objectives used to guide the 'cyber intelligence and information militia'. Thus, Australia ought to formulate its objectives lists in a manner that ensures that cyber militia members do not cross the threshold of being classed as 'civilians directly participating in hostilities'.

Due diligence

A key challenge in the context of Australians participating in the activities of an allied country's cyber and information militia comes from the obligation of 'due diligence' articulated by the International Court of Justice's *Corfu Channel* judgment; namely, "it is every State's obligation not to allow knowingly its territory to be used for acts contrary to the rights of other States".[26] A cyber militia could potentially undertake hostile acts contrary to the rights of other States and where Australia has knowingly allowed its territory to be used for such, it may be violating the due diligence principle.

Whether Australia adopts a militia along the lines of what has been proposed here or not, there is already a need to address the legal status of those Australian's currently acting as part of a foreign militia. In other words, Australian's currently acting as part of a foreign militia is a 'now problem'. To address this potential concern, I have offered a law reform proposal (see Appendix A) for situations where Australians participate in an allied country's cyber militia. It covers only activities that are defensive in nature since they potentially can be limited to activities that are not contrary to the rights of other States. However, for clarity, Australian lawmakers may wish to define what they accept as 'defensive' activities.

Finally, when it comes to the international legal landscape, it may also be noted that the need for transparency and accountability – as provided by the structure proposed here – has been emphasised several times, including in a 2021 report by the United Nations' Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security.[27]

Low cost and fast implementation

Measures adopted to protect Australia's national security are typically costly to acquire and slow to deploy. A cyber militia may be costly depending on its structure and capabilities. For example, writing about the 'cyber civil defence force' he envisaged, Austin noted that: "To achieve such capabilities country-wide, the investment required may be of the order of billions of dollars, rather than millions.".[28] However, as is illustrated by the volunteer 'IT Army' rapidly established by Ukraine in what appears to have been a predominantly improvised response to Russia's aggression, a cyber militia can also be established quickly and at a comparatively low cost depending on structure and capabilities.

Having said that, the potency of a cyber militia can be significantly enhanced by training. For example, instructions ought to be provided in the methods of OSINT. The training could usefully also address the requirements for securely documenting materials in a manner making it possible to later verify the authenticity of the materials. This could be crucial e.g., when it comes to documenting alleged war crimes, but also more generally to increase the reliability of the intelligence created by the cyber militia.

Furthermore, cyber militia members ought to be trained to understand the information warfare environment including the propaganda methods of potential adversaries, and how to effectively present a counter-narrative where it is justified to do so.

Formalising the training through contemporary micro-credential systems of accreditation would also make the militia much more attractive to potential participants. Thus, the training cost may be seen as a necessary recruitment expense.

In addition to the costs associated with the noted training, the effectiveness of an Australian 'cyber intelligence and information militia' could be boosted by the creation of a dedicated app. Such an app could be used to communicate the objectives lists, but it could also be set up to make the reporting by cyber militia members more efficient. The experience of creating an app during the COVID pandemic suggest that it is better to develop the app sooner rather than later to avoid working under time pressure.

The cost of the training and the relevant app will be low and should be seen in the light of the broader societal need for upskilling when it comes to areas such as information literacy (with the aim of teaching people how to think, not what to think), 'cyber hygiene', and cybersecurity. It may also be hoped that skills developed amongst cyber militia members can spread organically to the broader community, or at the minimum raise much needed public awareness of the threats facing our society.

A matter of urgency

Australia and its citizens are under constant attack in the form of 'cyber-attacks' and cyber-espionage, as well as influence campaigns e.g., in the form of mis- and dis- information. This state of constant hybrid warfare by those who wish to do us harm is not a temporary inconvenience. It is a persistent and serious threat to Australia, our democracy, and our way of life. We need to muster all our resources to counter these foreign measures. In the words of Austin and Khaniejo:

> "[T]here is no clear demarcation between peace and war in cyberspace. There is a blurring of the boundaries between competition, crisis and conflict, and countries experience a steady state of at least 'competition' during peacetime. They must therefore plan to build cyber defence and resilience in a manner that accounts for this perpetual state of tension."[29]

Regrettably, we also need to prepare for things to get worse, and the risk of military conflict in our region cannot be excluded. Should such a situation arise, our already strained resources would be under significant added stress. Consequently, we need to strengthen our deterrence, protection, and resilience in the cyber environment. Indeed, doing so may help prevent an open and/or military confrontation.

A 'crowdsourced' civilian volunteer cyber reserve capability in the form a 'cyber intelligence and information militia' as proposed here may be a valuable – and much-needed – addition to Australia's security and defence capabilities. In a sense, it is a whole-of-society response to a whole-of-society challenge.

APPENDIX 1: Proposal for a ‘*Designated Cyber Militia Bill*’[30]

Article 1

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

1. A foreign State has established the Cyber Militia;
2. That foreign State has invited foreigners to join its Cyber Militia; 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 cyber militia is conditioned on State oversight and control; after all, as is implied in the term ‘militia’ properly applied in the Australian historical context, we are here talking about volunteers carrying out activities in an organised manner based on orders issues by a State. In my 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 cyber militia. 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 cyber militia. Under this approach, the starting point is that Australians are prevented from joining a foreign cyber militia to the extent that their activities fall foul of cybercrime laws, and only where the Australian government has recognised as valuable the activities of the foreign cyber militia 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, I fear that such a structure would be 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. I am here predominantly thinking of Taiwan.

Article 2

Unless the activities constitute a violation of international law, a genuine member of a *Designated Cyber Militia* 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 Cyber Militia*;
2. Undertaken based on an order issued by the foreign State in command of the *Designated Cyber Militia*; and
3. Defensive in nature.

Explanatory comments

Article 2 seeks to set criteria for when a member of a *Designated Cyber Militia* 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 I opted for this structure 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 Cyber Militia* 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 my 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 Cyber Militia* 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 Cyber Militia* 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 Cyber Militia* under Article 2.

This does not prevent the Commonwealth cooperating in the case of allegations of war crimes 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 Cyber Militia* 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 Cyber Militia, 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.

REFERENCES

[1] Australian Signals Directorate, 'Redspice', undated, https://www.asd.gov.au/about/what-we-do/redspice.
[2] https://www.kaitseliit.ee/en/history-of-the-edl-cu. See further: Kadri Kaska, Anna-Maria Osula, and LTC Jan Stinissen, The Cyber Defence Unit of the Estonian Defence League (2013), https://ccdcoe.org/uploads/2018/10/CDU_Analysis.pdf, and Eneken Tikk, 'Civil defence and cyber security: a contemporary European perspective', in Greg Austin (Ed.), *National Cyber Emergencies : The Return to Civil Defence* (Routledge 2020) 76-92. For an interesting overview of US developments, see: Greg Austin, 'US Policy: from cyber incidents to national emergencies', in Austin (Ed.), *National Cyber Emergencies*, 31-59.
[3] See e.g. Mina Martin, 'A cyber security expert has called on Australia to 'build a cyber militia soon' as the country looks to defend against increasing attacks', Insurance Business, 9 June 2016, https://www.insurancebusinessmag.com/au/news/breaking-news/australia-needs-to-build-a-cyber-militia-says-cyber-expert-57578.aspx.
[4] Greg Austin, 'Australia Needs Civil Defence against the Cyber Storm', UNSW Research Group on Cyber War and Peace Policy Report (2019), p. 8, https://www.social-cyber.co/_files/ugd/15144d_225b0b0b86b84580b07cbb0c670583f2.pdf?index=true.
[5] Lachlan McGrath, 'Keyboard Warriors: An Australian Volunteer Cyber Corps' (March 5, 2023) https://www.nisr.org.au/article/keyboard-warriors-an-australian-volunteer-cyber-corps.
[6] See further: Austin, 'Australia Needs Civil Defence Against The Cyber Storm', p. 7.
[7] The proposal draws, builds, and expands, upon research findings previously presented in: Dan Svantesson, 'Regulating a "Cyber Militia" – Some Lessons from Ukraine, and Thoughts about the Future', *Scandinavian Journal of Military Studies*, 6(1) (2023), pp. 86–101. See also Dan Svantesson, 'Ukraine is recruiting an "IT army" of cyber warriors. Here's how Australia could make it legal to join', The Conversation (March 7, 2022) https://theconversation.com/ukraine-is-recruiting-an-it-army-of-cyber-warriors-heres-how-australia-could-make-it-legal-to-join-178414.
[8] NAFO Asia Pacific, 'Want to help Ukraine online? Join NAFO!', undated, https://nafo.ukrainians.org.au/.
[9] As noted by Gary Waters: 'The existing state emergency services could provide a suitable model for any new cyber civilian defence corps or militia'. See Gary Waters, 'National cyber emergency policy for Australia: Critical infrastructure', in Austin (Ed.), *National Cyber Emergencies*, p. 105, and also McGrath, 'Keyboard Warriors'.
[10] See further: ANZAC Portal, 'Coastwatchers played a vital role in the Pacific war', last updated, 15 November 2022, https://anzacportal.dva.gov.au/stories/australians-wartime/coastwatchers-played-vital-role-pacific-war; Cove Talk, 'Australia's Secret Army', 5 December 2023, 'https://cove.army.gov.au/article/covetalk-australias-secret-army, and in more detail: Michael Veitch, *Australia's Secret Army* (Hachette Australia, 2022).
[11] In the case of Sweden, mention may also be made of the Psychological Defence Agency established in 2022 (https://www.mpf.se/psychological-defence-agency).
[12] This may be, for example, an official webpage, a social media channel, or perhaps more appropriately a specifically developed app.
[13] M. Storm Jensen, (2018) 'Sector responsibility or sector task? New cyber strategy occasion for rethinking the Danish sector responsibility principle', *Scandinavian Journal of Military Studies*, 1(1), 1–18. DOI: https://doi.org/10.31374/sjms.3.
[14] See further: Ben Scott, 'Adapting Australian intelligence to the information age', ANU National Security College (2023), https://nsc.crawford.anu.edu.au/sites/default/files/publication/nsc_crawford_anu_edu_au/2023-12/ben_scott_ausint_web_nsc.pdf.
[15] IC OSINT Strategy 2024-2026 (2024), at 2, https://www.dni.gov/files/ODNI/documents/IC_OSINT_Strategy.pdf.
[16] Bergengruen, V. (2022, April 18). 'How Ukraine is crowdsourcing digital evidence of war crimes'. *Time*. Retrieved from https://time.com/6166781/ukraine-crowdsourcing-war-crimes/.
[17] See further: Kevin C Desouza and Atif Ahmad, 'Weaponised information systems for political disruption', in Austin (Ed.), *National Cyber Emergencies,* 126-147; and Chris Dufour, Tim Newberry and Rachel Azafrani, 'Dezinformatsiya', in Austin (Ed.), *National Cyber Emergencies*, 148-170.
[18] Commonwealth of Australia. (2021, December). Select committee on foreign interference through social media – First interim report. Retrieved from https://parlinfo.aph.gov.au/parlInfo/download/committees/reportsen/024741/toc_pdf/FirstInterimReport.pdf;fileType=application%2Fpdf.
[19] Josh Butler, 'AEC warns it doesn't have power to deter AI-generated political misinformation at next election', *The Guardian*, 20 May 2024, https://www.theguardian.com/australia-news/article/2024/may/20/aec-australian-electoral-commission-ai-deepfakes-election?utm_source=substack&utm_medium=email. See more generally Dennis Broeders (2021) 'The (im)possibilities of addressing election interference and the public core of the internet in the UN GGE and OEWG: a mid-process assessment', *Journal of Cyber Policy*, 6:3, 277-297, DOI: 10.1080/23738871.2021.1916976, https://www.tandfonline.com/doi/full/10.1080/23738871.2021.1916976.
[20] International Committee of the Red Cross, 'What is International Humanitarian Law?', (2004, July). Retrieved from https://www.icrc.org/en/doc/assets/files/other/what_is_ihl.pdf.
[21] Consider for example the intelligence oversight structure. (See Parliament of Australia, Joint Committee on Intelligence and Security, 'Advisory Report on the Intelligence Oversight and Other Legislation Amendment (Integrity

Measures) Bill 2020', February 2022, https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/IntegrityMeasuresBill/Report/.

[22] Greg Austin and Natallia Khaniejo (2024) 'Impact of the Russia–Ukraine War on National Cyber Planning: A Survey of Ten Countries', International Institute of Strategic Studies, p. 3, https://www.iiss.org/research-paper/2024/01/impact-of-the-russia-ukraine-war-on-national-cyber-planning-a-survey-of-ten-countries/.

[23] Dan Svantesson, 'Regulating a "Cyber Militia" – Some Lessons from Ukraine, and Thoughts about the Future', *Scandinavian Journal of Military Studies*, 6(1) (2023), pp. 86–101.

[24] International Committee of the Red Cross, 'The Principle of Distinction', (2023, March), Retrieved from: https://www.icrc.org/sites/default/files/wysiwyg/war-and-law/03_distinction-0.pdf.

[25] Kubo Mačák, 'Will the centre hold? Countering the erosion of the principle of distinction on the digital battlefield', IRRC No. 923 (June 2023) https://international-review.icrc.org/articles/will-the-centre-hold-923.

[26] International Court of Justice, Corfu Channel Case, United Kingdom v Albania, Judgment, Merits, (1949), p. 22, https://www.icj-cij.org/sites/default/files/case-related/1/001-19490409-JUD-01-00-EN.pdf.

[27] United Nations. (14 July 2021). Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security (A/76/135), https://digitallibrary.un.org/record/3934214/files/A_76_135-EN.pdf?ln=en.

[28] Greg Austin, 'Australia Needs Civil Defence against the Cyber Storm', UNSW Research Group on Cyber War and Peace Policy Report (2019), p. 10, https://www.social-cyber.co/_files/ugd/15144d_225b0b0b86b84580b07cbb0c670583f2.pdf?index=true.

[29] Austin and Khaniejo, 'Impact of the Russia–Ukraine War on National Cyber Planning', p. 6.

[30] This proposal, and the explanatory comments, was first published in: Svantesson, D. J. (2022, March 23). 'Legal safeguards for the volunteers of Ukraine's cyber militia'. Verfassungsblog on Matters Constitutional. Retrieved from https://verfassungsblog.de/legal-safeguards-for-the-volunteers-of-ukraines-cyber-militia/.

SOCIAL CYBER INSTITUTE

The **Social Cyber Institute** (SCI) creates new social science insights to complement technology in the fight for a more secure cyberspace. SCI is a non-profit organisation supported by the Social Cyber Group which offers advisory and training services in cyber policy.

Director: Professor Glenn Withers (glenn.withers@socialcyber.co)

SOCIAL CYBER ACADEMY

The **Social Cyber Group** (SCG) and **Blended Learning International** (BLI) join forces to deliver exciting international learning experiences with high business and policy relevance, through the Social Cyber Academy. Our dedicated partners in similar professional education activities in the recent years have included the **Korea Development Institute** and the **Global Development Learning Network** of the World Bank. The leaders of SCG and BLI rely on decades of experience in university-based and professional education in the US, the UK, Australia and Asia. Other clients of our Academy leaders in the field of education delivery in Australia have included: the Australian Department of Defence, Department of Home Affairs, Australian Public Service Commission, Australian Indigenous Leadership Council, Billabong Aboriginal Development Corporation, Australian Securities Exchange, Commonwealth Bank, QANTAS Engineering, Salvation Army, Sydney Ferries Corporation, ACT Government (transport services), Soldier On, and the Victorian Parliament. Internationally, our Academy leaders have partnered with the Distance Learning Centre (Sri Lanka), National Organisation of Science Teachers and Educators (Philippines), United International College (China), Tanri Abeng University (Indonesia), Tongji University (China), the Singapore Exchange, National Economic Action Council (Malaysia), University of Mauritius, and the Vietnam Cryptographic Agency.

Director: Lisa Materano (lisa.materano@socialcyber.co)

SOCIAL CYBER GROUP

Our senior researchers have decades of experience in advising government from inside and outside, often at senior levels, and working with business leaders to address their research needs. Clients have included the UK Foreign Office, the UK Ministry of Defence, the UK Cabinet Office, the European Commission, the New South Wales government, the Australian Department of Foreign Affairs and Trade, the Australian Director General of National Intelligence, the Graduate Research Institute for Policy Studies in Tokyo.

Director: Professor Greg Austin (greg.austin@socialcyber.co)