Article

Australian National University

Federal Law Review
2023, Vol. 51(2) 182–204

DOI: 10.1177/0067205X231166697
journals.sagepub.com/home/flr
Sage

White Hat, Black Hat, Slouch Hat: Could Australia's Military Cyber Capability be Deployed Under Commonwealth Call-Out Powers?

Brendan Walker-Munro*

Abstract

In April 2016, then Prime Minister Malcolm Turnbull confirmed the existence of Australia's offensive cyber capability. Said to constitute both a coordinating Information Warfare Division inside the Australian Army as well as dedicated cyberoffensive capability inside the Australian Signals Directorate, the unveiling of this capability was a watershed in Australian defence policy. Yet whilst the literature has briefly examined whether Australia's cyberoffensive capability is congruous with international law, no such analysis under Australia's domestic laws has been undertaken. This paper seeks to partially address this gap in the research by focusing on whether the Australian Defence Force could legally launch cyberattacks against domestic targets under Commonwealth call-out powers.

Accepted 3 May 2022

At a press conference on 21 April 2016, then Australian Prime Minister Malcolm Turnbull did what no other Head of State in the world had ever done — he revealed the existence of his country's offensive cyber capability.[1] Housed within the obscurely named and highly secretive Australian Signals Directorate ('ASD'), and later supported by the newly formed Information Warfare Division within the Australian Defence Force ('ADF'),[2] both the existence of the capability and the Prime Minister's public acknowledgement of it marked a watershed shift in Defence policy.

Other nations soon followed suit with their own disclosures, with other nations of the Five Eyes alliance including the United Kingdom (UK), United States (US) and Canada, admitting to the existence of offensive cyber capabilities.[3] Evidence increasingly began to mount that adversarial

1. Malcolm Turnbull, 'Launch of Australia's Cyber Security Strategy' (Speech, Sydney, 21 April 2016).
2. Fergus Hanson and Tom Uren, *Australia's Offensive Cyber Capability* (Policy Brief, Australian Strategic Policy Institute, 10 April 2018) 5.
3. Jeremy Fleming, 'Director's speech at Cyber UK 2018' (Speech at the CyberUK, 2018 Conference, Manchester, 12 April 2018) <https://www.gchq.gov.uk/pdfs/speech/director-cyber-uk-speech-2018.pdf> accessed 5 February 2023; *United States Cyber Command: Hearing Before the S. Comm. on Armed Services*, 115th Cong. (2018) (statement of Admiral Michael S Rogers, Commander, United States Cyber Command); Government of Canada, *Strong, Secure, Engaged: Canada's Defence Policy* (2017) 41.

* The University of Queensland, Senior Research Fellow, Law and the Future of War Research Group, T C Beirne School of Law, The University of Queensland, Australia. The author may be contacted at B.walkermunro@uq.edu.au. The author received financial support from the Trusted Autonomous Systems Defence CRC.

states such as China, Russia and North Korea — long rumoured to have military cyber capabilities of their own — were also deploying these capabilities to devastating real-world effect.[4]

Further announcements from Australia's Commonwealth government demonstrated an ongoing commitment to the deployment of a military cyber capability.[5] Most recently in 2021, Scott Morrison announced the signing of AUKUS, a trilateral defence pact with the UK and US. One of the major parts of AUKUS was the agreement to share technological developments in quantum computing and cyber capabilities.[6]

In almost every statement associated with these capabilities, we as members of the public have been reassured that these operations will comply with Australia's international obligations, including international humanitarian law ('IHL'). We have also all been told that such cyberattacks will be limited to malicious actors and cybercriminals located overseas. But could they be used here in Australia?

Surprisingly, there has been scant public or academic debate about the legitimacy of domestic ADF cyberattack operations under Australian laws. This could be because it has never been considered necessary, or the idea of using ADF cyberoffensive capabilities to protect Australian assets or citizens domestically has not been fully contemplated. Yet in the increasingly connected economy and society within which Australia operates, where cyberattacks can have devastating real-world consequences,[7] the potential for the ADF to be deployed in response to such attacks is seemingly inevitable.

Understanding the legislative underpinnings for domestic cyberattack operations is important not only to ensure appropriate immunity exists for the ADF, but also to maintain public support for the ADF by proving cyberattack operations are conducted pursuant to the rule of law. Cyberattacks that are not compliant with Australian laws will, conversely, reduce Australia's global reputation, undermine community confidence in the ADF and may also provide grounds for criminal or civil liability against the ADF, its officers or members. For these reasons, it is important that the circumstances under which Australian military cyber capabilities might be deployed can be appropriately articulated and explained.

This paper will contribute to the burgeoning literature on the legality of cyberattacks by examining the domestic legitimacy of the ADF and/or ASD being deployed to engage in cyberattacks within the territorial boundaries of Australia. The focus of my examination will be on the call-out powers contained in the *Defence Act 1903* (Cth) ('*Defence Act*'); however, there are also certain ancillary pathways to the deployment of Australia's cyberoffensive capability that will be discussed — such as under the *Intelligence Services Act 2001* (Cth) ('*IS Act*'). Considerations of IHL and international law,[8] though worthy of consideration, are not in scope.

4. Ed Caesar, 'The Incredible Rise of North Korea's Hacking Army', *The New Yorker* (online, 19 April 2021) <https://www.newyorker.com/magazine/2021/04/26/the-incredible-rise-of-north-koreas-hacking-army>.
5. Malcolm Turnbull, 'Press Conference with The Rt Hon Theresa May MP, Prime Minister of the United Kingdom: 10 Downing Street, London: 10 July 2017' (Press Conference, 10 July 2017); Malcolm Turnbull, 'Speech at the opening of the Australian Cyber Security Centre Canberra' (Speech, 16 August 2018).
6. Scott Morrison, Boris Johnson, Joseph R. Biden, 'Joint Leaders Statement on AUKUS' (Media Statement, 16 September 2021) <https://pmtranscripts.pmc.gov.au/release/transcript-44109>.
7. For example, Colonial Pipeline in the US was hit by a cyberattack in May 2021 which completely disabled the company for nearly a week: Mary-Ann Russon, 'US fuel pipeline hackers "didn't mean to create problems"', *BBC News* (online, 10 May 2021) <https://www.bbc.com/news/business-57050690>; see also Maskun Maskun et al, 'Cyber-Attack: Its Definition, Regulation, and ASEAN Cooperation to Handle with it' (2021) 4(2) *Jambe Law Journal* 131.
8. See, eg, Michael N Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press, 2nd ed, 2017); *Convention on Cybercrime,* opened for signature 23 November 2001, CETS No 185 (entered into force 1 July 2004).

https://doi.org/10.1177/0067205X231166697 Published online by Cambridge University Press

This paper will proceed in four sections. The section 'An Introduction to Cyberoffensive Capability and Cyberattacks' will introduce cyberattacks and discuss Australia's current policy and legal settings surrounding their use. The 'Legislative Support for Domestic Cyberattacks' section will examine the legal provisions which would enable deployment of cyberoffensive capabilities inside Australia's territorial boundaries. A brief history of the Acts permitting calling-out of cyberoffensive assets will also be explored. The 'Canada's Domestic Law Regarding Cyberoffensive Capability' section will then comparatively critique Australia's legislative position to that of Canada, another Five Eyes nation with a keen interest in cybersecurity that has passed specific legislation enabling its cyberoffensive capabilities to be utilised domestically. Finally, the paper will close with the 'Conclusion and Models for Possible Reform' section, which will propose some models which the Commonwealth government might choose to adopt to provide greater certainty, transparency and legitimacy to domestic cyberattack operations.

I An Introduction to Cyberoffensive Capability and Cyberattacks

Unfortunately, the very nature of cyberoffensive activities, as both a critical military asset and involving highly confidential technical capabilities, means that it is attended by a cloud of secrecy that makes public, academic or media debate difficult and confusing. For example, media reporting in 2017 suggested that the ADF could be given the 'green light' to attack cybercriminals in foreign countries[9] — an act that could reasonably be considered an attack under IHL or even a declaration of war. In 2020, global media reported the Petya and SolarWinds attacks on US infrastructure were the first crippling offensives known as a 'cyber Pearl Harbour'. Yet once the dust settled on those events, most cybersecurity scholars questioned the veracity of the media hype.[10]

So, what exactly are cyberattacks? What is a cyberoffensive capability? Australia's cybersecurity strategy does not define either term,[11] nor does Australia's international cyber engagement strategy.[12] The *Defence Act* and *IS Act* likewise contain no relevant assistance in defining these terms.

For the purposes of this paper, a 'cyberattack' is effectively a singular or group of projections of force into the cyberspace domain that 'manipulate, deny, disrupt, degrade or destroy targeted computers, information systems, or networks'.[13] The intention behind the use of force in cyberattacks can — like their real-world counterparts — be directed towards outcomes that vary from the invisible to the catastrophic. For example, a cyberattack could constitute:

- Infiltration of a target computer or network;
- Theft of information from a computer or network;
- Manipulation of accounts or passwords to those accounts;

9. Allie Coyne, 'Australia has created a cyber warfare unit', *ITNews* (online, 30 June 2017) <https://www.itnews.com.au/news/australia-has-created-a-cyber-warfare-unit-467115>.
10. Kevin R Bray, 'A Cyber Pearl Harbor?' (Research Report, Air War College, Air University, 3 February 2017); Sean Lawson and Brandon Valeriano, 'The Russian "Cyber Pearl Harbour" That Wasn't' (Commentary, Cato Institute, 18 December 2020) <https://www.cato.org/publications/commentary/russian-cyber-pearl-harbor-that-wasnt>; Joe Reeder and Tommy Hall, 'Cybersecurity's Pearl Harbor Moment: Lessons Learned from the Colonial Pipeline Ransomware Attack' (2021) 6(3) *The Cyber Defense Review* 15.
11. Department of Home Affairs (Cth), *Australia's Cyber Security Strategy 2020* (6 August 2020).
12. Department of Foreign Affairs and Trade (Cth), *Australia's International Cyber Engagement Strategy* (4 October 2017).
13. Hanson and Uren (n 2) 6.

https://doi.org/10.1177/0067205X231166697 Published online by Cambridge University Press

- Installation of 'ransomware' — a program that encrypts information or data unless a payment is made to the attackers;
- Defacing areas of 'public-facing' data, such as web pages or customer interfaces;
- Deleting or destroying data;
- Disabling critical systems or critical support infrastructure (either temporarily or permanently).

This list is not exhaustive, and future technological breakthroughs may offer new avenues or vehicles for cyberattacks to occur. Take the example of then President George W Bush when he visited Australia in September 2007 for the APEC Summit. The media noticed (apologetically, and almost as a footnote) that during the President's visit to Sydney, mobile phone calls would be blocked by 'a sophisticated counter-terrorism measure to prevent bomb attacks' deployed in a helicopter.[14]

However, this capability is nevertheless one that satisfies the criteria of being a cyberattack, being the deployment of a system that denies (by blocking cell signals from connecting to phone towers) targeted information systems or networks (being the telecommunications system in Sydney).

Cyberoffensive capability, on the other hand, is an umbrella term — it refers to all the technology, systems, hardware and software that can be deployed in support of a cyberattack, but also includes the persons and supporting assets that enable cyberattacks to be pursued. In Australia, cyber-offensive capability is housed within the ASD, a member of the National Intelligence Community (NIC), and thus is subject to the Ministerial oversight located in the *IS Act*.

However, the ADF also contains its own discrete cyberoffensive capability,[15] regulated under the imprimatur of the *Defence Act*. Unlike ASD, the ADF can only be commanded by the Chief of Defence Force ('CDF'),[16] the legal power of which is ultimately drawn from the Governor-General as the sovereign's representative in Australia.[17]

II Legislative Support for Domestic Cyberattacks

The distinction between the nature, domains and capabilities able to be employed by ASD and the ADF for cyberattacks is incredibly important. As I have already described, the legal basis for the operation of these two organisations is not only fundamentally important to ensure their actions comply with the rule of law, but also to protect the constitutional and common law freedoms of the Australian public in the unfortunate event that the ADF must be deployed to restore peace and order.

In conducting this examination, it should be noted that this paper makes a clear distinction between call-outs of ADF-specific capability under pt IIIAAA of the *Defence Act* and other forms of assistance rendered by the ADF, such as disaster relief or Defence Assistance to the Civil Community ('DACC'), which is usually authorised at a lower level (such as by the Joint Operations Support Staff).[18] This paper will focus on pt IIIAAA actions, where the 'use, or potential use, of force (including intrusive or coercive acts) is required by Defence members' in circumstances where

14. 'Mobiles to drop out during Bush visit', *Sydney Morning Herald* (online, 16 May 2007) <https://www.smh.com.au/national/mobiles-to-drop-out-during-bush-visit-20070516-gdq5em.html>.
15. *Australian Defence Cyber Industry Capability* (2021) 4; see also Hanson and Uren (n 2) 6, citing Deputy Chief Information Warfare, Major General Marcus Thompson.
16. *Defence Act 1903* (Cth) s 9 ('*Defence Act*').
17. *Australian Constitution* s 68.
18. Department of Defence (Cth), 'Defence Assistance to the Civil Community Policy' (31 August 2021). Such support is broadly enabled by the *Defence Act* (n 16) s 123AA.

https://doi.org/10.1177/0067205X231166697 Published online by Cambridge University Press

the situation is undoubtedly serious and beyond the scope of State authorities to manage.[19] In that way, the focus of my inquiry will be on the use of ADF cyberoffensive capability to support State law enforcement or defend Commonwealth interests and infrastructure, that is, those roles that Moore would call 'internal security', being the 'operational deployment of the ADF to use force for law enforcement purposes for civil disturbance or major event security'.[20] Where I consider deployment of ASD (ie where they take primacy), these will be examined under the imprimatur of their enabling legislation.

A *Legal Authorisation for ASD Cyberattacks*

Under the *IS Act*, ASD is a statutory authority headed by the Director-General of ASD, a civilian appointment who reports directly to the Minister for Defence.[21] Scrutiny of ASD operations is provided both by the Parliamentary Joint Committee for Intelligence and Security ('PJCIS')[22] and the Inspector-General of Intelligence and Security.[23] In addition to these measures, ASD is also subject to Ministerial privacy rules.[24]

The specific priorities of ASD are established by the *IS Act*.[25] Separate from their function with respect to intelligence gathering, the ASD has several discrete functions that contemplate engaging in cyberattack activity. For example, cyberattacks could be used to:

a) Prevent and disrupt cybercrime undertaken by people or organisations outside Australia[26];
b) Provide assistance to the ADF in support of military operations[27];
c) Provide assistance to the ADF (as a 'Commonwealth authority')[28] in relation to cryptography, communication and computer technologies[29];
d) Provide assistance to the ADF (as a 'Commonwealth authority') consistent with the performance of the functions of the ADF.[30]

With respect to the first of these functions, the *IS Act* requires that the Minister for Defence issue ASD with written directions to not exercise any of its functions with respect to preventing or disrupting cybercrime undertaken or enabled by an Australian person without a Ministerial authorisation.[31] However, the mandated Ministerial directions in the *IS Act* do not prevent (and thus authorisations cannot be sought) ASD from participating in any of its 'provide assistance' functions. Though these may be subject to other directions,[32] these are not mandatory and do not contemplate further authorisations.

19. Department of Defence (n 18) 5.
20. Cameron Moore, *Crown and Sword: Executive power and the use of force by the Australian Defence Force* (ANU Press, 2017) 166.
21. *Intelligence Services Act 2001* (Cth) s 27C ('*IS Act*').
22. Ibid s 28.
23. *Inspector-General of Intelligence and Security Act (1986)* (Cth) ss 8, 9, 9A.
24. *IS Act* (n 21) s 15(1).
25. Ibid s 7.
26. Ibid s 7(1)(c).
27. Ibid s 7(1)(d).
28. Ibid s 3 (definition of 'Commonwealth authority' para (c) includes the Defence Force).
29. Ibid s 7(1)(e).
30. Ibid s 13A.
31. Ibid s 8(1)(a)(iii).
32. Ibid s 8(2)(a).

https://doi.org/10.1177/0067205X231166697 Published online by Cambridge University Press

There is the possibility that the Minister could issue an authorisation for activities involving the deployment of ASD cyberoffensive capabilities inside Australia for the purpose of its assistance functions. The use of the word 'may' in s 9(2) of the *IS Act* suggests that a discretionary power exists for an authorisation to be issued 'in relation to … an activity, or class of activities, specified (whether by name or otherwise) in the authorisation'[33] — in this case, deployment of cyberoffensive capabilities inside Australia. If the Minister chose to do so, they would only need to be satisfied that the authorisation would permit activities necessary for the proper performance of one of ASD's functions (such as the assistance functions), there are satisfactory control arrangements in place to not exceed the authorisation and those arrangements can ensure that the 'nature and consequences of acts done in reliance on the authorisation will be reasonable'.[34]

Nor does the general limitations clause of the *IS Act* prevent that construction. Although the functions of *IS Act* agencies ought only to extend 'to the extent that [national security] matters are affected by the capabilities, intentions or activities of people or organisations outside Australia',[35] this section is specifically subject to a disclaimer if the function relates to inter alia ASD's function to assist the ADF.[36]

The combined effect of the Ministerial directions and authorisations scheme is that whilst the law enforcement function of ASD (preventing and disrupting cybercrime) is carefully regulated by the *IS Act*, the provision of assistance by ASD to the ADF is not. The Minister's issue of directions for ASD's non-cybercrime functions are not mandated. The recent Richardson Review of Australia's NIC identified this anomaly and recommended its correction, noting that there was nothing before the Review that indicated there was ever any intention for ASD to be free of Ministerial oversight in its assistance functions.[37]

Furthermore, the criminal and civil immunities that accrue to ASD due to its status as an *IS Act* agency apply only in respect of acts taken offshore (or those acts taken in Australia to further such offshore acts).[38] As none of the immunities operate to protect ASD if its officers or operatives assist the ADF in a domestic capacity, it is the immunities in the *Criminal Code* that operate.[39] These immunities in s 476.6 state:

> (1) A staff member or agent of an agency (within the meaning of subsection (10)) is not subject to any civil or criminal liability for engaging in conduct inside or outside Australia if:
>
> (a) the conduct is engaged in on the reasonable belief that it is likely to cause a computer-related act, event, circumstance or result to take place outside Australia (whether or not it in fact takes place outside Australia); and

33. Ibid s 9(2)(a).
34. Ibid s 9(1)(a)–(c). Section 9(1)(d) does not apply, as the authorisation does not relate to activities of ASIO: at ss 8(1)(a)(ia)–(ib).
35. Ibid s 11(1).
36. Ibid s 11(3).
37. Dennis Richardson, *Report of the Comprehensive Review of the Legal Framework of the National Intelligence Community: Volume 2 of 4: Authorisations, Immunities and Electronic Surveillance* (Report, 4 December 2020) 126 ('Richardson Review').
38. *IS Act* (n 21) ss 14(1)–(2).
39. *Criminal Code Act 1995* (Cth) ('*Criminal Code*') sch 1, s 476.6.

https://doi.org/10.1177/0067205X231166697 Published online by Cambridge University Press

(b) the conduct is engaged in the proper performance of a function of the agency.

(2) A person is not subject to any civil or criminal liability for engaging in conduct inside or outside Australia if:

(a) the conduct is preparatory to, in support of, or otherwise directly connected with, overseas activities of an agency; and

(b) the conduct:

(i) taken together with a computer-related act, event, circumstance or result that took place, or was intended to take place, outside Australia, could amount to an offence; but

(ii) in the absence of that computer-related act, event, circumstance or result, would not amount to an offence; and

(c) the conduct is engaged in the proper performance of a function of the agency.…

(10) In this section:

agency means ASIS, ASD or AGO.

Though the deployment may well be in proper discharge of a function of ASD in assisting the ADF, both s 476.6(1)(a) and 476.6(2)(b)(i) involve requirements that the conduct have an overseas connection. Without a reasonable belief that a cyberattack in Australia was intended to occur outside Australia — difficult to justify in a call-out situation — the immunities will likely fail to operate in the instance of a domestic deployment of ASD cyberattack capability inside Australia.[40]

Taken together, the operation of the sections in the *IS Act* and *Criminal Code* suggest that prima facie a deployment of ASD's cyberoffensive capability inside Australia's territory would not be lawful. Though problematic on its face, this may be of little moment given Australia's unique approach to the pragmatics of ASD deployment. According to the ADF's Joint Cyber Unit and Joint Operations Command, any deployment of ASD under its 'assistance' functions to the ADF would be classified as a military operation, not a civilian one.[41] Additionally, staff of ASD are instructed in, and bound by, the ADF's Rules of Engagement ('ROE'), which in turn are informed by laws of armed conflict and Australian domestic law.[42] That position aligns with the concept that a domestic deployment of the ADF would inherently be a military-led engagement.

40. Richardson Review (n 37) 22. Such immunities will also not affect the onshore activities of the ADF if the recommendation of the Richardson Review is accepted.
41. Hanson and Uren (n 2) 6.
42. Ibid. See also David Letts and Rob McLaughlin, 'Call-out Powers for the Australian Defence Force in an Age of Terrorism: Some Legal Implications' (2016) 85 *AIAL Forum* 63, 78.

https://doi.org/10.1177/0067205X231166697 Published online by Cambridge University Press

B *Legal Authorisation for ADF Cyberattacks*

Turning attention now to the capabilities of the ADF, the deployment of military forces inside Australia is specifically provided for by pt IIIAAA of the *Defence Act*. This Part, originally inserted in 2000 in response to the Olympics Games in Sydney and then amended again in 2006 and 2018,[43] permits various forms of call-out orders to be made (including contingent or dormant orders, which allow the CDF to deploy only on the occurrence of specified circumstances, triggers or indica).[44]

The suite of amendments has made it clear that the Commonwealth may deploy the ADF either with or without a request from a State, essentially supplementing what would have been an exercise of executive power under s 61 of the *Constitution* by the Governor-General, with a statutory exercise of power supported by the constitutional defence power in s 51(vi). However, executive power may still be invoked by certain preparatory acts or ex ante engagements by the ADF within the scope of its authority.[45] For example, a call-out order is not necessarily required for the physical disposition of ADF assets inside Australia. There is no legislative requirement for the ADF to be asked to 'be' anywhere domestically, only where they are being asked to utilise some capability — as Moore puts it 'the prerogative for control and disposition of the forces means that the ADF has freedom of movement anyway. Call-out just places forces at the disposal of the civil authority to use force'.[46]

Under the *Defence Act*, the first type of call-out is a Commonwealth interests order,[47] and the second is a State protection order.[48] Commonwealth interests orders involve the determination of a real, perceived or anticipated threat to Commonwealth interests,[49] whether in Australia or its offshore regions. Alternately, a state of domestic violence that would (or would be likely to) affect Commonwealth interests must be occurring or likely to occur in Australia.[50] Similarly, a State protection order requires a real, perceived or anticipated occurrence of domestic violence occurring in a State or Territory that has requested the Commonwealth's assistance.[51] Orders are almost always made by the Governor-General,[52] though the Act does permit certain expedited orders to be made Ministerially in serious and urgent emergencies.[53]

It is worth noting that the use of the words 'domestic violence' in the *Defence Act* do not relate to their more contemporary meaning involving intimate partner or family violence — instead, it reflects the language in s 119 of the *Australian Constitution* which obliges the Commonwealth to 'protect every State against invasion and, on the application of the Executive Government of the

43. Michael Head, 'Another Expansion of Military Call Out Powers in Australia: Some Critical Legal, Constitutional and Political Questions' [2019] No 5 *UNSW Law Journal Forum* 1, 1–14.
44. See *Defence Act* (n 16) ss 34, 36 for Commonwealth interests orders and State protection orders, respectively.
45. David Letts and Rob McLaughlin, 'Military Aid to the Civil Power' in Robin Creyke, Dale Stephens, Peter Sutherland (eds), *Military Law in Australia* (The Federation Press, 2019) 117–128.
46. Moore (n 20) 169.
47. *Defence Act* (n 16) s 33.
48. Ibid s 35.
49. This term is not defined in the *Defence Act* (n 16), but a codified list of what the Commonwealth considers in its interests may be found in both the *Constitution* (s 51) and *Criminal Code* (n 39) (s 100.4(5), as it relates to defining a terrorism offence).
50. *Defence* Act (n 16) s 33(1).
51. Ibid s 32.
52. Ibid ss 33(3), 34(3), 35(3) and 36(3). This recognises the Governor-General's role as Commander-in-Chief: *Australian Constitution* s 68.
53. *Defence Act* (n 16) s 51U.

https://doi.org/10.1177/0067205X231166697 Published online by Cambridge University Press

State, against domestic violence', itself derived from US constitutional law[54] wherein nothing short of an armed insurrection capable of threatening the very existence of a State government would qualify.[55] Consistent with that reasoning, in the Addendum to the Explanatory Memorandum, domestic violence is described as 'conduct that is marked by great physical force and would include a terrorist attack, hostage situation, and widespread or significant violence'.[56] Alternately, the conduct must be such that it would 'rupture the social fabric'.[57]

It is important to pause momentarily and observe that the mere involvement of the cyber domain will not matter for determining whether a state of domestic violence exists, as that term is currently contemplated by the *Constitution* or by reference to the legislative history of the *Defence Act*. The relevant focus of the authorising Ministers[58] is upon the *existence or predicted existence* of a set of facts, from which those Ministers will determine that either a state of domestic violence exists, or it does not. Put another way, the mere fact that attacks are launched from cyberspace or only affect online assets is irrelevant for the Ministers' satisfaction that there exists a form of conduct capable of equating to domestic violence.

White's exposition on the internal security prerogative in cyberoperations is also telling.[59] Outside the common law doctrine of necessity — which would authorise the Commonwealth to deploy its military forces in the defence of itself against actual and threatened disturbances[60] — he argues the Commonwealth retains a prerogative, derived from s 61 of the *Constitiution* and endorsed in case law such as *Sharkey*,[61] to deploy forces as it sees fit. Though the High Court of Australia may have been sceptical about the reach of the prerogative,[62] their reservations are limited in application to the *Defence Act* on several grounds. Firstly, the *Maritime Powers Act 2013* (Cth) in *CPCF* purported to bind the Commonwealth in all its capacities, something conspicuously absent from the *Defence Act*. Secondly, the *Maritime Powers Act 2013* (Cth) lacked an enabling provision similar to that found in s 51ZD of the *Defence Act*, which applies statutory clarity to the notion that the call-out order provisions '[do] not affect any utilisation of the Defence Force that would be permitted or required, or any powers that the Defence Force would have' if those powers were disregarded.[63]

In any event, I also consider there is another way for the Ministers to achieve the requisite satisfaction to request the making of a call-out order. Essentially, this involves considering any cyber threat (whether or not attended by real-world acts or actions) as a threat to Commonwealth interests given that the Commonwealth retains legislative primacy under s 51(v) of the *Constitution* for 'telegraphic, telephonic, and other like services', the breadth of which has already been deemed sufficient to capture the cyber domain, the Internet and future forms of telecommunications.[64] Given

54. *United States Constitution* art IV § 4; *Civil Disturbance Statutes* 10 USC § 331 (1964).
55. Michael Head, 'Calling out the Troops — Disturbing Trends and Unanswered Questions' (2005) 28(2) *UNSW Law Journal* 479, 481.
56. Samuel White and Andrew Butler, 'Reviewing a Decision to Call out the Troops' (2020) 99 *AIAL Forum* 58, 58.
57. Samuel White, 'Keeping the Peace of the iRealm' (2021) 42(1) *Adelaide Law Review* 101, 113.
58. Being the Prime Minister, Attorney-General and Minister for Defence: *Defence Act* (n 16) s 31.
59. See Samuel White, 'A Shield for the Tip of the Spear' (2021) 49(2) *Federal Law Review* 210.
60. *R v Home Secretary of State for the Home Department, Ex parte Northumbria Police Authority* [1989] QB 26.
61. *R v Sharkey* (1949) 79 CLR 121 ('*Sharkey*'); see also White (n 59) 210.
62. *CPCF v Minister for Immigration and Border Protection* (2015) 255 CLR 514 ('*CPCF*').
63. Cf *CPCF*, where the High Court did not believe the Commonwealth could 'having failed to enter through the front door … enter through the back door and in effect achieve the same result by that means of entry': at [141].
64. *R v Brislan; Ex parte Williams* (1935) 54 CLR 262; Paul Kildea and George Williams, 'The Constitution and Commonwealth Proposals for New Media Regulation' (2013) 18 *Media and Arts Law Review* 2, 2–16; Explanatory Memorandum, Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (Cth), 37 [47].

https://doi.org/10.1177/0067205X231166697 Published online by Cambridge University Press

that White suggests '[i]t is difficult to envisage a situation of civil order in the modern, globally connected world where some aspect of a Commonwealth interest would not be threatened or endangered', any potential for intrusion, damage or disablement of the internet would trigger a Commonwealth interest contemplated by the *Defence Act*.[65]

Presuming a Commonwealth interests order or State protection order has been made, the CDF is required to comply. In deploying the ADF, the CDF must have regard to the following:

- Directions of the Minister as to the way in which the Defence Force is to be utilised[66];
- That the ADF may not be used to stop or restrict any protest, dissent, assembly or industrial action, except if there is a reasonable likelihood of death, serious injury or serious damage to property[67];
- The order issued to him or her and the purpose it is intended to remedy[68];
- The operations of, and the obligation to cooperate with, the Police forces of the State or Territory to which the ADF has deployed[69]; and
- That a member of the ADF must not be utilised for a particular task unless a member of the Police force has requested that task be performed.[70]

Once deployed, the ADF may utilise the full range of its capabilities in pursuing the purpose/s of the order issued by the Governor-General. The ADF is vested with a significant suite of powers to pursue that purpose, including the 'right to shoot to kill someone escaping detention, search premises without warrants, detain people without formally arresting them, seal off areas and issue general orders to civilians'.[71] In areas declared as 'specified areas',[72] or containing 'declared infrastructure',[73] persons may be compelled to produce documents and answer questions,[74] searched (without limitation as to whether the search is intimate or forensically invasive).[75] Persons may also be arrested without warrant and detained until they are able to be placed in police custody.[76]

Most controversially, members of the ADF may use 'reasonable and necessary force',[77] in the exercise of those powers (except for using force to compel production of documents or answers to questions,[78] which would nullify a person's privilege against self-incrimination). This also includes using lethal force against persons to protect life or prevent serious injury of persons, protect declared infrastructure, prevent a person fleeing detention or to destroy aircraft or vessels.[79]

65. White (n 56) 133, citing *Victoria v Commonwealth* (1975) 134 CLR 338, 412–13; see also the High Court's acceptance of the information environment as involving the *Constitution* in *LibertyWorks Inc v Commonwealth* (2021) 391 ALR 188.
66. *Defence Act* (n 16) s 39(3) (a).
67. Ibid s 39(3)(b).
68. Ibid s 40(1)(a)(i).
69. Ibid s 40(1)(a)(ii).
70. Ibid s 40(1)(b). Though this does not require transfer or abrogation of the chain of command: ss 39(3) and (4).
71. Michael Head, 'The Military Call-Out Legislation — Some Legal and Constitutional Questions' (2001) 29(2) *Federal Law Review* 273.
72. *Defence Act* (n 16) s 51.
73. Ibid s 51H.
74. Ibid ss 51D(2)(i), 51L(3)(g).
75. Ibid ss 51A, 51L(3)(c)–(d).
76. Ibid ss 51D(3)(d), 51L(3)(e).
77. Ibid s 51*N*(1).
78. Ibid s 51*N*(2).
79. Ibid ss 51*N*(3) and (5).

https://doi.org/10.1177/0067205X231166697 Published online by Cambridge University Press

So, does this framework authorise the ADF to engage in cyberattacks during a domestic deployment? As a threshold question, it would be important to identify who is engaging in the cyberattack — is it the ADF using its own inherent capability? Or is it the ASD operating under ADF command and control?

C ADF Inherent Capability

If the ADF seeks to deploy its own inherent cyberoffensive capability inside Australia pursuant to a call-out order under the *Defence Act*, this is a decision of the CDF. The CDF would need to be satisfied that the use of the capability, or the engagement in cyberattacks, would be 'reasonable and necessary' for the purpose specified in the call-out order.[80] The use of any cyberoffensive capability would also need to be 'as far as reasonably practicable' in cooperation with the Police Force of the host State or Territory and pursuant to a request from that Force to perform a task (such as hacking into, disabling or destroying a computer or network).[81] Whilst it is axiomatic that Police Forces have their own computer experts, those personnel are likely to be experts in forensics and not information warfare. The ADF would — in the author's view — be highly likely to be requested to use cyberattacks given that the Police Force does not possess such a capability.

Those preliminary matters having been settled, the ADF would then be permitted to use its inherent cyberoffensive capability inside Australia for the object of achieving the purposes of the call-out order. The use of electronic equipment by ADF members in particular ways as determined by that ADF member is specifically authorised by the *Defence Act* under the pt IIIAAA provisions — whether explicitly authorised by the Minister in a general case,[82] in relation to a specified area,[83] or in protection of declared infrastructure.[84] These provisions appear sufficiently elastic to contemplate an ADF cyberoffensive capability being deployed generally in support of a call-out.

Cyberattacks as a methodology could also be explicitly authorised by the Minister for Defence in writing, in which case such attacks could be conducted to capture or recapture a location or thing, to prevent or put an end to acts of violence or threats to safety, free hostages, control the movement of a vehicle or even to destroy an aircraft or vessel.[85] A cyberattack against a thing that causes or could cause death or serious injury — such as shutting down an aircraft's engines in flight or turning off an electric car's engine — could also be authorised if the use of force was 'reasonable and necessary' in the circumstances.[86] Cyberattacks for similar purposes are also implicitly authorised by the use of ADF powers in either specified areas or in protection of declared infrastructure.[87] Yet the exact legality of the use of a cyberattack to take the life of another person by crashing their plane — outside of the scenario of self-defence or emergency, or in the realm of an armed conflict — is 'intensely problematic and contentious'.[88]

Curiously, the language in the *Defence Act* also supports a contention that the cyberoffensive capability could ostensibly be utilised to assist the ADF with the discharge of its search and

80. Ibid ss 33(3), 34(3), 35(3), 36(3). The obligation is imposed by s 39(2), and subject to ss 39(3) and 40.
81. Ibid ss 40(1)(a)(ii), 40(1)(b).
82. Ibid s 46(7)(i).
83. Ibid s 51D(2)(j).
84. Ibid s 51L(3)(h).
85. Ibid ss 46(1)(a), 46(5), 46(7).
86. Ibid ss 51N(1)(a), 51N(3)(a), 51N(5).
87. Ibid ss 51D(2)–(3) and 51L(2)–(3).
88. Letts and McLaughlin (n 45) 132.

https://doi.org/10.1177/0067205X231166697 Published online by Cambridge University Press

seizure powers.[89] For example, cyberattacks that bypass encryption or passwords could allow ADF members to remotely search encrypted computers or mobile phones and seize any data of relevance. These attacks could either be authorised as an exercise of the 'operation of electronic equipment' provision, authorised under a CDF search determination,[90] or as a consequence of the exercise of 'incidental powers' in furtherance of a specific other power (ie the search power).[91]

The only potential limitation of the use of cyberattacks in support of searches are whether cyberattacks involve a 'use of force', as force may not be used against a thing to compel the production of documents (ie such as those that might be contained within a computer or network).[92] An in-depth analysis of whether cyberattacks involve use of force is beyond the scope of this paper; however, it is sufficient to note that 'use of force' in domestic law is traditionally centred on physical acts or acts with a physical outcome.[93] It is also worth noting that, at least from an ADF perspective, a cyberattack would need to be compliant with whatever extant ROE applied as part of the *Defence Act* pt IIIAAA deployment (which are standing orders issued by the CDF or his/her delegate, and outline when and under what circumstances ADF members may use force, including lethal force).

It is perhaps more apposite to observe what use of force means in the law enforcement context, given that an ADF call-out would (at least notionally) be focused on restoring law and compliance with the civil power. In law enforcement, 'use of force' is analogous to 'the amount of effort required by police to compel compliance by an unwilling subject'.[94] A person whose phone is being hacked by an ADF cyberattack is also unlikely to be aware of that fact. On those grounds, it is difficult to imagine that a cyberattack would be considered a use of force (at least in the terms contemplated by s 51N of the *Defence Act*); however, such an interpretation runs counter to a person's common law privilege against self-incrimination.[95]

Searches of computers or networks facilitated by ADF cyberattacks also may not be lawful in the context of searches that are entitled to be observed, such as those conducted under a CDF search determination,[96] or searches of aircraft or vessels.[97] In those cases, it is difficult to contemplate how an ADF member could remotely search computers or networks covertly and still be observed by the owner of premises or master/captain of an aircraft or vessel, a matter which would render the conduct of the search unlawful.[98]

89. *Defence Act* (n 16) s 46(7) (d)–(e) permits an ADF member to search persons, locations or things for things that may be seized, or persons who may be detained, in relation to the call-out order — the Act does not appear to limit such searches to the physical world.
90. Ibid s 51A(2).
91. Ibid ss 46(9), 51L(5).
92. Ibid s 51N(2).
93. See, eg, *Criminal Code Act 1899* (Qld) s 245 which defines assault inter alia as 'A person who strikes, touches, or moves, or otherwise applies force of any kind to, the person of another …' and defines 'applies force' as 'includes the case of applying heat, light, electrical force, gas, odour, or any other substance or thing whatever if applied in such a degree as to cause injury or personal discomfort'.
94. Australian National Audit Office, *Management of the Use of Force Regime* (Auditor-General Report No 30, 5 May 2016) 1.
95. See, for example, *X7 v National Crime Commission* (2013) 248 CLR 92.
96. *Defence Act* (n 16) s 51C(1).
97. Ibid s 51E(2).
98. Ibid s 51S(1).

https://doi.org/10.1177/0067205X231166697 Published online by Cambridge University Press

D *ASD Support to ADF Operations*

The situation is significantly different if the ASD provides support to the ADF under a call-out order. This is because of two major limitations to the application of the *Defence Act*. Firstly, a call-out order issued by the Governor-General directs the CDF to 'call-out the Defence Force',[99] which means the ADF as constituted by the Royal Australian Navy, Australian Army and the Royal Australian Air Force, but no other forces (such as ASD).[100] Secondly, powers that accrue under pt IIIAAA are vested either in the CDF (such as issuing search determinations) or in 'Defence members', being 'any officer, sailor, soldier or airman'.[101] Members of ASD are civilians and are not subject to the *Defence Act*.

However, the provisions that permit deployment of electronic equipment under a call-out order also permits an ADF member to 'direct a person to operate … machinery or equipment (including electronic equipment) in a particular manner'.[102] As there is no limitation on the classes of persons to whom such a direction might be given, an ADF member *might* direct a civilian member of ASD to engage in a cyberattack or otherwise deploy a cyberoffensive capability, in circumstances where ASD were perhaps taking only an observational role (and not providing assistance). One assumes that the cyberattack is being performed either as an exercise of the electronic equipment direction power or incidental to the exercise of some other power (such as conducting a search or capturing/recapturing a facility or thing). In either case, the ASD civilian is acting under the imprimatur of the ADF member's powers.

E *The Legal Nature of Protections for the ADF and ASD*

Despite the somewhat convoluted nature of the interactions between the *IS Act* and *Defence Act*, such an analysis remains important. The ADF must ensure that Australian servicemen and women, and the people who may assist them (including ASD but also the State and Territory police), are properly protected from liability where their actions are consistent with Australian law. Conversely, the Australian public has both a vested interest and legal right to ensure that their constitutional and common law privileges are not abrogated arbitrarily, even in a state of domestic emergency.

Part IIIAAA operations will not be protected by combatant immunity, the common law doctrine which shields uniformed Service personnel from criminal liability for their actions when engaging in lawful acts of belligerency.[103] If the ADF deploys to a State or Territory suffering domestic violence, and the use of reasonable and necessary force (including lethal force) is contemplated by the Act in support of that deployment, uniformed ADF members might qualify for that

99. Ibid ss 33(3), 34(3), 35(3), 36(3).
100. Ibid ss 4, 17.
101. Ibid s 4.
102. Ibid ss 46(7) (i), 51D(2) (j), 51L(3) (h).
103. *Shaw Savill and Albion Co Ltd v Commonwealth* (1940) 66 CLR 344, 361 ('*Shaw Savill*').

https://doi.org/10.1177/0067205X231166697 Published online by Cambridge University Press

protection.[104] But would armed Australian citizens, against whom the ADF might deploy, be considered an 'enemy' against which the forces of the Crown are operating?[105]

A fulsome examination of combatant immunity is not in scope here; however, whether combatant immunity would apply in a call-out situation is a grey area.[106] In any event, as ASD employees are not uniformed personnel nor 'Defence members' under any Defence legislation, they receive no benefit of the immunity.

Even in a call-out situation, ADF and ASD activities undertaken within Australia's domestic confines will be subject to Australian criminal and civil law, particularly the *Criminal Code*.[107]

The *Defence Act* makes clear that the Commonwealth criminal law continues to apply, even under a pt IIIAAA order.[108] In such a case, ADF members will likely have some immunity from ordinarily illegal conduct which, in the context of this paper, would include the offences in relation to telecommunication services and computer offences.[109]

The first of the immunities applying to ADF members are the 'good faith' provisions. An ADF member exercising a power under a call-out order who fails to comply with any obligation (such as wearing uniform whilst exercising a pt IIIAAA power) is taken to have not exercised the power validly unless the exercise was in 'good faith'.[110] Though the exercise of the power may be validated by good faith, criminal and/or civil liability may still attach, unless the exercise of the power was also performed under an valid call-out order, infrastructure declaration, specified area declaration or authorisation.[111] If the order or declaration was valid but the power exercised in bad faith, the ADF member would likely face charges under either the *Defence Force Discipline Act 1982* (Cth) or even civilian criminal laws.[112]

The second of the immunities applying to ADF members are the 'superior orders' provisions. An ADF member will have recourse to such a defence under a pt IIIAAA call-out, unlike the narrower defence in the *Criminal Code*.[113] An ADF member will be excused from *any* criminal act if they obeyed an order that was not manifestly unlawful in circumstances where 'the member had no reason to believe that circumstances had changed in a material respect since the order was given' and 'the member had no reason to believe that the order was based on a mistake as to a material fact'.[114] Whilst an ADF member does not have to question orders (and often is not able to do so without

104. See Rymn J. Parsons, 'Combatant Immunity in Non-International Armed Conflict, Past and Future' (2014) 1(1) *Homeland & National Security Law Review* 1.
105. See *Shaw Savill* (n 103).
106. International analogues are of limited utility in this space: see generally Steven Haight, *The War on Terror, Intelligence, Convergence and Privacy* (Senior Service College Fellowship Thesis, US Army War College, 31 May 2012) <https://apps.dtic.mil/sti/pdfs/ADA592703.pdf>; Michael K Caswell, '*R (Khan) v the Secretary of State for Foreign & Commonwealth Affairs*: UK Courts-The Pontius Pilot of Drone Strikes' (2015) 23(2) *Tulane Journal of International & Comparative Law* 539.
107. *Criminal Code* (Cth) (n 39) sch 1.
108. *Defence Act* (n 16) s 51Y. This provision is consistent with the provisions of the *Defence Force Discipline Act 1982* (Cth) which apply the laws of the Jervis Bay territory to the conduct of Defence members: at s 61(3).
109. *Criminal Code* (n 39) pts 10.6–10.7.
110. *Defence Act* (n 16) s 51S(1).
111. Ibid s 51S(2).
112. *Defence Act* (n 16) s 51Y(3) and the attached Note makes clear that although State and Territory police may investigate criminal conduct by ADF members, ultimately authority to bring a civilian charge vests in the Commonwealth Director of Public Prosecutions (CDPP), not the DPP of the host State or Territory.
113. Only as against allegations of crimes against humanity or torture: *Criminal Code* (Cth) (n 39) ss 268.116, 274.4.
114. *Defence Act* (n 16) s 51Z(2)(e).

https://doi.org/10.1177/0067205X231166697 Published online by Cambridge University Press

exposing themselves to discipline), this defence requires that the ADF member was not deliberately ignorant of the possible existence of contraindicating states of affairs.[115]

Yet neither of these immunities will apply to activities undertaken by ASD on the orders or instructions of an ADF member.[116] Instead, it is highly likely that ASD activities undertaken on the ADF's orders would be covered by the ASD-specific immunities under either the *IS Act* or *Criminal Code*.[117] Ironically, in examining ASD support to ADF operations, the ADF recently told the Richardson Review that there may be 'circumstances in which the ADF must engage in activity that could give rise to liability under Australian criminal law but cannot access ASD authorities and immunities'.[118]

Again, the Richardson Review observed anomalies with the interaction of immunities between ASD and the ADF, but as the support of agencies covered by the *IS Act* supporting the ADF was not within the Terms of Reference for the Richardson Review, little more was said.[119] The Richardson Review did however note that any current immunities given to the ADF for intelligence activities cover only their *offshore* activities, and not those within the boundaries of Australia. Thus, the Richardson Review recommended that the ADF not be immunised at all in respect of the telecommunications offences in the *Criminal Code*.[120] Despite that recommendation, the Government committed in its response to the Review to examine the immunities applying to joint ASD-ADF operations and 'to bring forward legislative amendments to address such uncertainty'.[121]

F Conclusion to S II

Under Australian law (both the *IS Act* and *Defence Act*) it is conceivably possible that cyberattacks could form part of any ADF response or deployment under a pt IIIAAA order. Whether the authorising Ministers approve the use of such capabilities under the legislative pathways to making pt IIIAAA orders, or the CDF considers it necessary and appropriate to deploy such capabilities in the context of any given order, there appears no legislative basis prohibiting the use of cyberoffensive capability. Further, the preservation of the executive power by the *Defence Act*[122] and *Defence Regulation*[123] supports the contention that — absent a legislative grant — the Commonwealth may exercise its prerogative to use the ADF's capabilities as it sees fit.[124] In the event that executive power does not flow into the cyber domain (which I do not believe is likely), the Commonwealth may also have recourse to the exercise of the 'internal security prerogative' as White describes it, even the common law defence of necessity, to achieve much the same outcome.[125]

115. David Lanham, 'Wilful Blindness and the Criminal Law' (1985) 9(5) *Criminal Law Journal* 261; cited in *Bahri Kural v R* (1987) 162 CLR 502, [12] (Toohey and Gaudron JJ).
116. As ASD staff are civilians and not Defence members, they do not have the benefit of the superior orders defence: *Defence Act* (n 16) s 51Z(2).
117. *IS Act* (n 21) s 14; *Criminal Code* (n 39) s 476.6.
118. Though this statement was not made in the context of call-outs, but rather the offshore operations of ADF members: Richardson Review (n 37) 224.
119. Richardson Review (n 37) 222.
120. Ibid 225–6.
121. *Commonwealth Government Response to the Comprehensive Review of the Legal Framework of the National Intelligence Community* (Report, 4 December 2020) 1, 23.
122. *Defence Act* (n 16) s 51ZD.
123. *Defence Regulation 2016* (Cth) s 69.
124. Cameron Moore, 'Military Law and Executive Power' in Robin Creyke, Dale Stephens and Peter Sutherland (eds), *Military Law in Australia* (Federation Press, 2019) 69, 78; *Plaintiff M68/2015 v Minister for Immigration and Border Protection* (2016) 257 CLR 42.
125. White (n 57) 132–5.

https://doi.org/10.1177/0067205X231166697 Published online by Cambridge University Press

Furthermore, cyberattacks are arguable (at the very least, they are not prima facie prohibited) as forming part of the considerable suite of powers vested by the *Defence Act* in the event of an ADF call-out. In such instances, the identity and capacity of the person undertaking the cyberattacks is highly relevant. An ADF member engaging in a cyberattack with a military objective has a far wider scope of legislative permission, as opposed to an ASD civilian undertaking a cyberattack in response to the coordinating instructions of a military officer.

What will be critical in reconciling these provisions is achieving 'coherence and consistency between the essential elements of the regime and correlative authorisations elsewhere in legislation'.[126] The immunities that could attach to cyberoffensive actions will vary, dependent again on the identity and capacity of the person engaging in the cyberattack. Whilst both ADF and ASD members might have access to certain immunities that preclude both criminal and civil liability for their conduct, the coverage of those immunities remains patchy and ill-formed — something recognised by the Australian Government as a worthwhile target of reform.

III Canada's Domestic Law Regarding Cyberoffensive Capability

I intend to now turn from Australian jurisprudence and conduct a brief comparative examination of the Canadian legislation regarding cyberoffensive capabilities. Canada was chosen as a case study jurisdiction for several reasons. Firstly, Canada is a member of the Five Eyes Alliance alongside Australia, and so these countries are more likely to share similar intelligence approaches and methodologies.[127] Secondly, Canada and Australia share a strong history of cooperation at the juncture of both cyberspace and national defence.[128] Thirdly, Canada — like Australia — is a member of the British Commonwealth and possesses a Federalised common law legal system that is founded upon laws inherited from Britain at the time of independence.[129]

Canada's national security apparatus is similar, but not identical, to that of Australia. Canada possesses a statutory national security intelligence organisation known as the Canadian Security Intelligence Service ('CSIS')[130] as well as the Communications Security Establishment ('CSE').[131] Whilst CSIS has a national security and protection responsibility that extends both within and without Canada, the CSE is entirely focused on foreign and overseas-based threats. Between the two agencies, they perform roles analogous to Australia's Security Intelligence Organisation ('ASIO') and the Australian Secret Intelligence Service ('ASIS'). The corollary to Australia's Ministry of Defence is the Canadian Department of National Defence ('DND'), while its Canadian Armed Forces ('CAF')[132] is a functional equivalent to the ADF.

Updates to the Canadian national security laws in 2015 resulted in a significant change in mandates and operational priorities of the CSIS, CSE and DND. Consistent with those changes, the CSE's statutory mandate became to 'degrade, disrupt, influence, respond to or interfere with the

126. Letts and McLaughlin (n 45) 130.
127. Nikola Pijović, 'The Cyberspace "Great Game": The Five Eyes, the Sino-Russian Bloc and the Growing Competition to Shape Global Cyberspace Norms' (Conference Paper, International Conference on Cyber Conflict, 25–28 May 2021).
128. Maxandre Fortier, *Rethinking Canada's Defence Strategy: What Lessons Can We Learn from the UK and Australia?* (Policy Brief No 7, Network for Strategic Analysis, January 2021) 4–5.
129. William Tetley, 'Mixed Jurisdictions: Common Law v Civil Law (codified and uncodified)' (2000) 60(3) *Louisiana Law Review* 677, 684.
130. *Canadian Security Intelligence Service Act*, RSC 1985, c C-23 ('*CSIS Act*').
131. *Communications Security Establishment Act*, SC 2019, c 13 ('*CSE Act*').
132. *National Defence Act,* RSC 1985, c N-5 ('*ND Act*').

https://doi.org/10.1177/0067205X231166697 Published online by Cambridge University Press

capabilities, intentions or activities of a foreign individual, state, organization or terrorist group as they relate to international affairs, defence or security'.[133]

CSE is empowered to:

- Carry out 'activities on or through the global information infrastructure to help protect … federal institutions' electronic information and information infrastructure'[134];
- Help protect 'electronic information and information infrastructures designated under subsection 21(1) as being of importance to the Government of Canada'[135] — essentially a corollary to Australia's designated infrastructure provisions in the *Defence Act*; and
- Render technical assistance to the DND and CAF.[136]

However, CSE is statute barred from operating within the domestic boundaries of Canada in a manner that brooks little creative interpretation. The enabling Act makes clear that the whole of CSE capability may not be used in Canada, against a Canadian or person in Canada, or in any way inconsistent with the *Canadian Charter of Rights and Freedoms*.[137] This accords with the rare public admissions of CSE activities, where these capabilities are used exclusively overseas.[138] CSE cyberattack operations are also subject to joint Ministerial authorisation by both the Minister for National Defence and the Minister for Foreign Affairs.[139] In some cases, actions may also need to be approved by the Intelligence Commissioner.[140] Whilst it is possible that — like the situation in Australia — the CSE could render 'technical assistance' to the CAF domestically and/or as part of a call-out order, no cyberattacks or projection of cyberoffensive capability could be conducted lawfully as part of rendering that assistance.[141]

On other hand, CSIS does have a specific mandate to operate inside Canada. If CSIS believes that a threat exists to the security of Canada, CSIS is empowered to 'take measures', whether those measures occur within or outside Canada, to reduce the threat.[142] There is no statutory bounds placed on what those measures are, except to the extent such measures must be reasonable and proportional in the circumstances, and otherwise compliant with the *Canadian Charter of Rights and Freedoms*.[143]

CSIS operations do have a form of 'get-out' discretion; a judge may issue a warrant that authorises the taking of threat reduction measures, irrespective of whether those measures comply with the *Canadian Charter of Rights and Freedoms* and/or could constitute a breach of Canadian law.[144] The only limitation on these forms of CSIS activities is a broad prohibition on causing death or bodily harm, obstructing the course of justice or violating the sexual integrity of an individual.[145]

133. *CSE Act* (n 131) s 19.
134. Ibid s 18(a).
135. Ibid s 18(b).
136. Ibid s 20.
137. Ibid s 22(1).
138. Alex Boutilier, 'Canadian spy agency targeted foreign hackers to "impose a cost" for cybercrime', *Global News* (online, 6 December 2021) <https://globalnews.ca/news/8429008/canadian-spy-agency-targets-cybercrime/>.
139. *CSE Act* (n 131) ss 29–31.
140. Ibid ss 27(2), 28(1), 39(3).
141. Ibid s 22(2).
142. *CSIS Act* (n 130) s 12.1(1).
143. *Canada Act 1982* (UK) ch 11, sch B pt I ('*Canadian Charter of Rights and Freedoms*').
144. *CSIS Act* (n 130) ss 12.1(3.2), 12.1(3.4), 21.1.
145. Ibid s 12.2(1).

https://doi.org/10.1177/0067205X231166697 Published online by Cambridge University Press

These provisions collectively, in the author's view, could permit CSIS to undertake cyberattacks inside Canada, so long as such activities comport with the agency's threat reduction mandate. Yet — and this is perhaps the most crucial point under Canada's national security legislation — CSIS does not have an assistance function in the same manner as CSE. CSIS cannot assist the CAF. The threat reduction function bestowed on CSIS is entirely separate from its intelligence cooperation function (which specifically includes cooperating with the CAF on matters of national security and defence intelligence).[146] In turn, CSIS' intelligence function may not be used domestically against any Canadian citizen, permanent resident or corporation within the confines of national or provincial law.[147] Effectively, the legislation statute bars the CSIS and CAF from cooperating on 'threat reduction' activities, with the maximum possible extent of cooperation between CSIS and the CAF coming from the sharing of information regarding potential threats, and the actions taken by each organisation in response to them.[148]

Whilst it is possible that CSIS and either of the DND or CAF could share information regarding threats to Canadian security and could implicitly coordinate actions in engaging in cyberattacks by understanding what each agency was doing, Canadian law quite effectively separates the threat reduction functions of CSIS from the military functions of the CAF.

A *Effect of a Call-Out Under Canadian Law*

Though it has been demonstrated above that neither the CSE nor CSIS will be capable of rendering assistance to the CAF in the conduct of cyberattacks, this does not obviate the cyberoffensive capabilities being developed by the CAF. This is especially the case given the amendments to Canadian national security legislation giving CAF a wider scope for cyber activities.[149] CAF public documents have taken up this mantle, making clear that the forces have embraced 'conducting active cyber operations against potential adversaries in the context of government-authorized military missions'.[150]

Call-out powers in Canadian law are prima facie far simpler than their Australian counterparts. There exists no unilateral capacity for the CAF to be called out in protection of Canadian interests — a call-out is triggered only by a written request by the Attorney-General of a province, on threat of 'a riot or disturbance of the peace, beyond the powers of the civil authorities to suppress, prevent or deal with'. That riot or disturbance must also be of such a scope and nature to require the deployment of the CAF.[151] A request must be in writing and must comply in all respects with the proscribed form laid out in the *ND Act*.[152]

In the event of a call-out from a provincial Attorney-General, it is a matter for the Chief of the Defence Staff (or their delegate) to determine what — if any — elements of the CAF will be deployed in response to the request. This could relevantly include such cyberoffensive capabilities

146. Philippe Lagassé, 'Defence intelligence and the Crown prerogative in Canada' (2021) 64(4) *Canadian Public Administration* 539.
147. *CSIS Act* (n 130) ss 16(1)–(2).
148. Ibid ss 19(2) (c)–(d); cf *ND Act* (n 132) ss 75(b)–(c).
149. N B Marshall, *Offensive Cyber in the Canadian Armed Forces: Opportunities from Bill C-51* (Service Paper JCSP 42, Canadian Forces College, 2015).
150. *Strong, Secure, Engaged* (n 3) 15.
151. *ND Act* (n 132) s 275.
152. Ibid ss 279–80.

https://doi.org/10.1177/0067205X231166697 Published online by Cambridge University Press

as the Chief of the Defence Staff considers 'necessary for the purpose of suppressing or preventing any actual riot or disturbance or any riot or disturbance that is considered as likely to occur'.[153]

Once called-out, CAF members are vested with considerable powers, as they are effectively deemed as police constables, bound instead by the Code of Service Discipline and the military chain of command rather than police executive structures.[154] A situation of call-out in Canada is also temporally unlimited, as the decision to end the deployment of the CAF lies entirely at the satisfaction of the Chief of Defence Staff, with no statutory bounds or expiration dates.[155]

Immunities for Defence members are equally concise under Canadian law. A member of the CAF is excused from liability for any act performed that is consistent with the Code of Service Discipline, 'unless the officer or non-commissioned member acted, or omitted to act, maliciously and without reasonable and probable cause'.[156] To avoid doubt, members of the CAF also remain subject to the jurisdiction of the civil courts of Canada, even during a call-out period.[157]

B *Conclusion to S III*

The Canadian framework is, it would appear, far more permissive of the concept of domestic cyberattacks being conducted by military pursuant to a call-out than would be the case in Australia; however, there are several critical differences that bear considering.

The threshold to initiating a call-out of the CAF is far higher than Australia, requiring an actual 'riot or disturbance' beyond the control of the civil power, rather than the more nebulous 'domestic violence'. The CAF also cannot be called out prospectively under conditional orders. Unlike Australia, Canada does not possess at all a legislative head of power that contemplates protecting its own interests in the same manner as a Commonwealth interests order.

However, Canada does more clearly delineate the role of its agencies with cyberoffensive capabilities. CSE is statute barred from domestic operations or operations against Canadian citizens, consistent with its mandate as a foreign security intelligence agency. CSIS — whilst it has a clear 'threat reduction' mandate to act against threats to Canadian security — cannot perform such activities for or on behalf of the CAF, and the intelligence sharing function between CSIS and CAF would be mutually exclusive of any potential CSIS involvement in CAF cyberoffensive activities.

IV Conclusion and Models for Possible Reform

Having briefly examined the legislative bases for Defence deployments in both Australia and Canada, I believe that it can be concluded that both frameworks tacitly permit the use of a cyberoffensive capability.

In the context of Australia however, our legislation lacks some of the flexibility and clarity inherent in the Canadian statutes dealing with both call-out powers generally and the use of cyberattacks specifically. Although pt IIIAAA was substantially remade as recently as 2018, there

153. Ibid s 278.
154. Ibid s 282.
155. Ibid s 283. However, the provincial Attorney-General must conduct an inquiry within 7 days of the call-out and present the report to the Queen's Privy Council for Canada: ibid s 281.
156. Ibid s 270.
157. Ibid s 286.

https://doi.org/10.1177/0067205X231166697 Published online by Cambridge University Press

exists several proposals for reform that bear considering for greater certainty, transparency and legitimacy of domestic cyberattack operations.[158]

A *Model 1: Statutory Review of Part IIIAAA*

Perhaps the simplest and most cost-effective avenue of reform would be to incorporate an analysis of cyberattacks and cyberoffensive capabilities as a specific Term of Reference when the statutory review of pt IIIAAA is conducted. Though such a review may be undertaken at any time, it must be performed every five years,[159] meaning a review would be due on or before 10 December 2023.

This proposal has the benefit of ease — the term could be consolidated into a mandated legal review of pt IIIAAA that will occur, irrespective of whether the government agrees with the positions taken in this paper. A review would also have the benefit of examining other aspects of pt IIIAAA powers, determining whether they are meeting their statutory objectives and offering opportunity for public debate and submissions as to the appropriate form of call-out orders.

The review could also — in a far more exacting and detailed way than was possible here — compare Australian call-out powers to those in other jurisdictions to identify global best practice. Evidence for the review could be led from domestic law experts from other jurisdictions as to the challenges and opportunities available from their perspectives.

Conversely, there are drawbacks to this model of reform. A statutory review will inevitably take significant time and resources. Further, if the proposals contained in this paper are considered as part of a statutory review commenced in 2023, it may be one or two more years before the amendments pass Parliament. Such delay is contrary to providing a degree of certainty to ADF and ASD senior officers who — even at the time of writing — may well be preparing plans that involve deployment of cyber capabilities in support of Australia's civil power.

B *Model 2: Recognition of Cyberattack Operations as Part of National Security Legislation*

Another option for Commonwealth Parliament would be consideration of modifying Australia's national security legislative framework to better recognise cyberattacks and cyberoffensive capabilities, with a clear indication that NIC agencies and the ADF are — subject to the existing Ministerial direction and authorisation framework — permitted to engage in those forms of activities in the prosecution of an agency/ADF function.

For example, the concept of a 'cyber security incident' is given statutory force in Australia's national security legislation in the *Security of Critical Infrastructure Act 2018* (Cth). Such incidents include the unauthorised access to, modification, or deletion of data and/or the impairment of a computer or data in Australia's critical infrastructure.[160] That infrastructure is in turn inclusive of assets such as ports, petroleum/natural gas lines and terminals, broadcasting towers, telecommunications networks, banks, and food and grocery stores.[161]

158. I have rejected any proposition that the Government would not undertake any law reform, or is otherwise uninterested in law reform of the Defence Act. The Government's response to the Review made clear that government was on notice as to the issue of immunities for the ADF as well as the whole of cooperation between the ADF and ASD, and has committed to correcting any deficiencies: Richardson Review (n 37).
159. *Defence Act* (n 16) ss 51ZB(1)–(2).
160. *Security of Critical Infrastructure Act 2018* (Cth) s 12M.
161. Ibid div 2.

https://doi.org/10.1177/0067205X231166697 Published online by Cambridge University Press

Either the *Security of Critical Infrastructure Act 2018* (Cth) (or similar legislation) could be modified to include a statutory definition of a cyberattack (which could subsume the definition of a cybersecurity incident to include a connexion to a person or organisation conducting, directing or performing activities in prosecution of the incident), or the definition of cyberattack below could be included in the uniform electronic surveillance Bill proposed by the Richardson Review.[162]

This reform could also look internationally at how cyberattacks are treated in domestic law in overseas jurisdictions, where cyberattacks have been recognised in legislation in various ways. In the European Union (EU), cyberattacks are defined broadly and inclusively[163]:

> 3. For this purpose, cyberattacks are actions involving any of the following:
>
> (a) access to information systems;
>
> (b) information system interference;
>
> (c) data interference; or
>
> (d) data interception,
>
> where such actions are not duly authorised by the owner or by another right holder of the system or data or part of it, or are not permitted under the law of the Union or of the Member State concerned.

As a part of Australia's national security framework, any amendment to the national security laws will trigger the jurisdiction of the Independent National Security Legislation Monitor (INSLM)[164] to review the Act and its mechanisms of operation. Such scrutiny will undoubtedly yield additional recommendations that could sharpen the legislative basis for cyberattacks conducted in pursuance of national security objectives.

Such reforms and oversight could equally give greater precision to other *IS Act* agencies seeking to use cyberoffensive capabilities in a legally permissive way outside the pt IIIAAA space. For example, cyberattacks are not defined with reference to ASD's cybercrime jurisdiction[165] nor that of the other *IS Act* agencies, despite those agencies having clear mandates that involve responses to cyberattacks from foreign and non-State actors. A comprehensive statutory definition would not only give transparency to what *are* lawful cyberattacks (ie those performed by ADF or *IS Act* agencies in compliance with Australian domestic law) but also what *are not* lawful (ie those performed by foreign actors, cybercriminals or terrorists, or those lacking proper Ministerial authorisation).

The drawback to this proposal is that the *Criminal Code* already includes significant legal definitions of various combinations of conduct that would be covered by any attempted definition of 'cyberattack'.[166] By introducing a new definition of 'cyberattack', the intended purpose of providing transparency and clarity could be frustrated by contributing to an already bloated national security criminal offence framework.

162. Richardson Review (n 37) ch 27.

163. *Council Regulation (EU) 2019/796 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States*, [2019] OJ L 129/1, art 1(3).

164. Established by the *Independent National Security Legislation Monitor Act 2010* (Cth).

165. *IS Act* (n 21) s 7(1)(c).

166. For example, see *Criminal Code* (n 39) ss 477.1 (Unauthorised access, modification or impairment with intent to commit a serious offence), 477.2 (Unauthorised modification of data to cause impairment), 477.3 (Unauthorised impairment of electronic communication), 478.1 (Unauthorised access to, or modification of, restricted data).

https://doi.org/10.1177/0067205X231166697 Published online by Cambridge University Press

It should also be considered that the exact mechanisms of what is or is not a cyberattack will change dependent on the underlying technology. By enshrining the term cyberattack in legislation, we essentially affix a definition at a point-in-time; nevertheless, technology has a habit of emerging in ways that defy legal regulation.[167] Following this model of reform runs the very real risk of only permitting the ADF or ASD to undertake certain proscribed forms of cyberattack, even where those forms of cyberattack might be inconsistent with the best technology or best practice.

C Model 3: Adoption of Statutory Barriers, viz Canada

A third and final proposal for reform would be for Australian law to adopt a clear and 'bright line' rule[168]that discriminates between what can and cannot be done in cyberspace by the ADF and ASD under a pt IIIAAA order. The need for such a delineation solves the question of attribution — by adopting such a rule, actions undertaken by ADF personnel that are pursued for a military purpose (under the direction of the CDF) can be distinguished from those undertaken by ASD personnel (under the direction of the Executive). This enables both ex ante and *ex post* analysis to conclude what actions are lawfully supported by the frameworks supporting each organisation, and which are not. It also supports legislative clarity on situations in which a cyberattack may be used to achieve a lethal outcome — such as using a computer to shut down an aircraft's engines in flight.

By way of comparison, Australia could look to Canada for a mechanism that adequately separates the domestic responsibilities of ASD, the ADF and other *IS Act* agencies in the same way that legislation separates CSIS, CSE and the CAF in Canada.

To follow this model of reform, the Australian government could use reforms of the *IS Act* proposed by the Richardson Review to frame changes that would explicitly limit ASD cyberattack operations. For example, the *IS Act* could be modified to require Ministerial authorisation for pursuit of ASD's 'assistance to military operations' function.[169] Bringing this function into the Ministerial direction/authorisation framework would not only give the scheme greater transparency but would allow for Ministers to provide direct oversight of one of the agency's most important functions. Indeed, the Review clearly contemplated that this form of amendment should occur.

On the other hand, Australia could more fulsomely follow the Canadian example and modify the *IS Act* to make it clear that the cyberoffensive capability of ASD is to be used solely outside Australia, including in circumstances where ASD is discharging its 'assistance' function to the ADF for a military operation. This would — following the Canadian example—possibly remove doubt that where cyberattacks are contemplated by the ADF in dealing with violence or unrest under a pt IIIAAA order, they must be using their own inherent cyberoffensive capabilities in doing so. ASD would thus be limited to rendering only 'technical assistance' under the *IS Act* in a manner that clearly precludes them from acting as *agent provocateur* for the ADF.

The level of clarity provided by a blanket prohibition against cyberattacks inside territorial Australia has its obstacles. There may come a time where, both societally and militarily, the use of cyberattacks in

167. Gregory N Mandel, 'Legal Evolution in Response to Technological Change' in Roger Brownsword, Eloise Scotford and Karen Yeung (eds), *The Oxford Handbook of Law, Regulation and Technology* (Oxford University Press, 2017) 225.

168. For use of the term, see Andrew McLetchie, 'The Case for Bright-Line Rules in Fourth Amendment Jurisprudence: Adopting the Tenth Circuit's Bright-Line Test for Determining the Voluntariness of Consent' (2001) 30(1) *Hofstra Law Review* 225.

169. *IS Act* (n 21) s 7(1)(d). This could also be achieved by a non-mandated *IS Act* direction: cf *IS Act* (n 21) s 8(2)(a).

https://doi.org/10.1177/0067205X231166697 Published online by Cambridge University Press

accordance with properly formulated ROE becomes commonplace. Conflicts may be fought almost entirely in cyberspace. In that future, it is likely that the use of cyberattacks is implicitly accepted by the members of Australian society as an important military tool in protecting their safety and freedoms. In such a case, banning or prohibiting the ADF from having access to the wealth of knowledge and technical assets available to ASD, despite ASD having a legislatively mandated function to help the ADF, may well be considered an 'own goal' in terms of national security.[170]

D *Final Observations*

I have attempted here to conduct a brief exploration of the Australian legislative landscape that may give life to the use of cyberoffensive capabilities by the ADF within Australia's domestic borders. Obviously, the very idea of Australian personnel hacking into Australian-owned computers and networks is at best legally challenging and at worst, dystopian fiction. Despite that, clarity in the legal frameworks for the exercise of the *Defence Act's* pt IIIAAA powers should be a significant objective, considering that matters of life and death of Australian civilians may literally hang on the outcome.

Compared to Canada, Australia's legislation appears to be overly complex and convoluted. Furthermore, there exists the very real possibility that the ADF and/or ASD could be deployed domestically and — without any malice or negligence — commit crimes against Commonwealth law because of the spotty, incomplete patchwork of immunities applying to domestic cyberoperations.

Perhaps future research could focus on whether Australian personnel would receive the protection of combatant immunity in a domestic call-out scenario — do Australian citizens qualify as the 'operations against the enemy' to which the immunity is directed? Or perhaps we ought to consider whether the public policy grounds exist for immunising the ADF for telecommunications offences abroad, given that the Review and the Government seem split on the issue. Finally, we might consider what other jurisdictions might be grappling with the problem of legalising domestic cyberattack programs (such as the UK or US) and how their legislation might be adapted for our own domestic purposes.

In any event, I am of the view that the law requires reform, and this paper addresses some (but clearly not all) of the models that could achieve it. I consider that the proposals are modest and timely and utilise some of the existing reform options that either are, or shortly will be, put in train by government. The alternative — where the Governor-General directs the CDF to deploy troops, who then break the law despite the most honourable intentions — is almost too horrible to contemplate.

ORCID iD

Brendan Walker-Munro https://orcid.org/0000-0001-5484-1145

170. For an example of the term, see Philip Coorey, 'China kicks Australia — and scores a global own goal', *Australian Financial Review* (online, 3 December 2020) <https://www.afr.com/politics/federal/china-kicks-australia-and-scores-a-global-own-goal-20201202-p56k1a/>.

https://doi.org/10.1177/0067205X231166697 Published online by Cambridge University Press