OPERATION TITSTORM: HACKTIVISM OR CYBER-TERRORISM?

KEIRAN HARDY*

Re: Operation Titstorm post #17

Hey the cult is already trying to label us as terrorists and as you put it once you mess with the gover[n]ment things start getting messy. If we don't do damage control then they really will be capable of truthfully calling us terrorists for attacking a government.[1]

I INTRODUCTION

On 10 February 2010, an internet based group of protesters calling themselves 'Anonymous' launched a cyber-attack on the Australian Parliament House website. Aptly named 'Operation Titstorm', the attack was launched by the group to protest against the Rudd government's plans to introduce a mandatory internet filter banning pornographic images of animated characters, small breasted women and female ejaculation. It brought down the website for three days by flooding it with network traffic – up to 7.5 million requests per second – and it bombarded parliamentary email addresses with pornographic material (ironically, of the very kind the government intends to ban). It also

* LLB Candidate, University of New South Wales; Research Assistant, Australian Research Council Laureate Fellowship on Anti-Terrorism Law, Gilbert + Tobin Centre of Public Law, University of New South Wales. I would like to thank the anonymous reviewers for their comments on an earlier version of this paper. Any remaining errors are my own.

1 urbanhawk, 'Re: Operation Titstorm' on Anonymous Activism Forum, *Why We Protest* (6 May 2010) <http://forums.whyweprotest.net/292-freedom-expression/operation-titstorm-61002/>.

plastered a selection of this questionable material across the Prime Minister's homepage.[2]

The message above was posted on an online activism forum in response to the attacks. Evidently, some members of Anonymous remain concerned that their activities may leave the realm of mischievous online protest and enter the largely uncharted waters of 'cyber-terrorism'. On first glance, the attacks do not fit into what the general public would probably define as a 'terrorist act'. Nonetheless, important questions remain about the extent to which politically motivated cyber-attacks will qualify as terrorism under Australian law.

This article analyses the facts of Operation Titstorm under the current definition of a terrorist act in the *Criminal Code Act 1995* (Cth) ('*Code*'). Although Operation Titstorm has not been, and most likely will not be, prosecuted under the legislation, this analysis is useful because it brings out some of the problems with applying the current anti-terrorism law framework to politically motivated cyber-attacks. Instead of first defining what is or is not an act of cyber-terrorism, this paper works inductively through the requirements of the Australian definition, examining what will qualify as an act of cyber-terrorism under Australian law. It then considers whether any adjustments are necessary to conform to an appropriate definition.[3]

Part II tests the facts of Operation Titstorm against the definition of a terrorist act under section 100.1 of the *Code*. Part III argues that only a low harm requirement is needed to prove that the political protest exception in section 100.1(3) does not apply, and that there are not sufficient safeguards in the current legislation to maintain a distinction between acts of 'hacktivism'[4] and 'cyber-terrorism'. To this end, this paper suggests some ways that the legislation could

---

2 See Mark Davis, 'Porn Fans Attack Website to Protest against Censorship', *Sydney Morning Herald* (Sydney), 13 February 2010; 'Hackers "Titstorm" the PM and Parliament House', *The Australian* (Sydney), 11 February 2010; Peter Veness, 'Hackers Targets PM's Website in Protest', *Sydney Morning Herald* (Sydney), 10 February 2010. The precise amount of time for which the website remained offline varies between sources; for the purposes of this paper, the author will rely on the three-day period reported by the Sydney Morning Herald. If the website remained offline for substantially shorter periods, then it is possible this could have some factual impact on whether the attack 'seriously' interfered with or disrupted an electronic system for the purposes of section 100.1(2)(f) of the *Criminal Code Act* 1995 (Cth) ('*Code*'), though it will not impact issues surrounding the political protest exception, or the consistency of the Australian definition with other international and domestic definitions of terrorism: see below Pts II(A)(2) and III.

3 While different approaches to the question of 'what is cyber-terrorism?' may certainly be taken, this paper focuses on 'acts of cyber-terrorism' in the strictest legal sense. In the Australian context, particular conduct involving computer systems will only qualify in a court of law as a 'terrorist act' where it satisfies the requirements discussed. Other uses of the internet by 'terrorists' (recruitment, training, operational planning) may be referred to as acts of cyber-terrorism in a broader sense, and may indeed fall under one or more ancillary terrorism offences. For an example of this broader approach in the UK, and a discussion of the strengths and weaknesses of different approaches to defining cyber-terrorism, see Clive Walker, 'Cyber-Terrorism: Legal Principle and Law in the UK' (2005–06) 110 *Penn State Law Review* 625, 627–628, 633–5. The normative question of what 'should' qualify an act of cyber-terrorism is discussed further in Part III below.

4 A portmanteau of 'hacking' and 'activism': see discussion in Part III below.

be improved, in order to reduce the risk that acts of hacktivism will be prosecuted as terrorist acts.

In its current form, Australia's anti-terrorism legislation sets the threshold too low for prosecuting acts of terrorism against electronic systems. While this broad definition will necessarily include acts deserving of the label of cyber-terrorism, it may also include acts of online political protest that are unworthy of the serious penalties involved. This danger results from the low levels of harm and fault required of an act of terrorism against an electronic system in section 100.1(2)(f), combined with the prosecution's low burden of proving that the political protest exception in section 100.1(3) does not apply.

The definition of a terrorist act in section 100.1 of the *Code* should be amended to mitigate this danger by including a serious economic harm requirement and an express fault element in section 100.1(2)(f). This would bring Australian's anti-terrorism legislation in line with definitions of terrorism at international law and in comparable domestic jurisdictions, and with definitions of cyber-terrorism in computer science. It would reduce the risk of prosecuting undeserving offenders, prevent governments from using the anti-terrorism legislation to silence less serious forms of political protest against electronic systems, and avoid any potential chilling effect on the freedom of online political expression.

The government has recognised the vulnerability of Australia's electronic infrastructure to cyber-attack[5] – as well it should – but it should also recognise the threat to legitimate online protest that the current definition of a terrorist act creates. We need to ensure that our anti-terrorism legislation cannot be used to silence legitimate online political protest, lest things 'start getting messy'.

II POLITICALLY MOTIVATED CYBER-ATTACKS AS TERRORIST ACTS UNDER AUSTRALIAN LAW

This Part tests the facts of Operation Titstorm against the requirements of a terrorist act in section 100.1 of the *Code*. A terrorist act must be motivated by a political, religious or ideological cause; it must be intended to influence a government by intimidation or intimidate a section of the public; and, in the case of a cyber-attack, it must seriously interfere with an electronic system. It is likely that Operation Titstorm, or another similar attack, would satisfy these positive requirements. Although Operation Titstorm would also likely satisfy the political protest exception in section 100.1(3), in other cases the prosecution needs only to overcome a low burden in order to prove that this exception does not apply.

5 For some government comments about the threat of cyber-attacks to Australian infrastructure; see Commonwealth, *Parliamentary Debates*, House of Representatives, 4 December 2008, 12549–61 (Kevin Rudd); Commonwealth, *Parliamentary Debates*, House of Representatives, 26 September 2001, 31582–4 (Daryl Williams); Commonwealth, *Parliamentary Debates*, House of Representatives, 27 June 2001, 28641–3 (Daryl Williams).

A Operation Titstorm Satisfies the Positive Requirements of a Terrorist Act

1 *Intention to Advance a Political Cause and Influence a Government by Intimidation*

Section 100.1 of the *Code* defines a 'terrorist act' as an action or threat of action where:

> (a) the action falls within subsection (2) and does not fall within subsection (3); and
> (b) the action is done or the threat is made with the intention of advancing a political, religious or ideological cause; and
> (c) the action is done or the threat is made with the intention of:
> (i) coercing, or influencing by intimidation, the government of the Commonwealth or a State, Territory or foreign country, or of part of a State, Territory or foreign country; or
> (ii) intimidating the public or a section of the public.

Each limb of this definition is an essential element of the offence and must be proved by the prosecution beyond reasonable doubt.[6] Both limbs of paragraph (a) will be dealt with in the following Parts. The references to intention in paras (b) and (c) constitute physical – not fault – elements of the offence.[7] They are the major discriminating factors between an ordinary criminal offence and a terrorist act, which attracts a maximum penalty of life imprisonment.[8] They need not be attributed to the specific individual or individuals committing the terrorist act, so long as the prosecution proves the general intention of a group of offenders.[9]

First, a terrorist act must be intended to advance a political, religious or ideological cause. This is commonly understood as a 'motive' rather than 'intention' requirement; that is, the prosecution must prove the emotional cause behind the prohibited conduct, as opposed to the desire to bring about a particular consequence.[10]

There has not been extensive judicial discussion about the precise meaning of the terms 'political', 'religious' and 'ideological', but there is no reason to suggest that the requirement should be interpreted narrowly. The essential condition is that the act is not motivated by purely private ends. In *R v Mallah*, the NSW Supreme Court distinguished a political, religious or ideological cause from 'some purely personal cause either to secure a passport, or to exact revenge'.[11] Most recently, in *R v Elomar*, the NSW Supreme Court differentiated a political cause from the 'need for financial gain or simply private revenge'.[12] In

---

6 See *Faheem Khalid Lodhi v The Queen* (2006) 199 FLR 303, 323 [89]–[90], 324 [93] ('*Lodhi*').
7 Ibid 323 [90].
8 *Criminal Code Act 1995* (Cth) s 100.1(1).
9 *Lodhi* (2006) 199 FLR 303, 323 [90].
10 See Ben Saul, 'The Curious Element of Motive in Definitions of Terrorism: Essential Ingredient or Criminalising Thought?' in Andrew Lynch, Edwina MacDonald and George Williams (eds), *Law and Liberty in the War on Terror* (Federation Press, 2007) 28.
11 *R v Mallah* [2005] NSWSC 317 (21 April 2005) [22] ('*Mallah*').
12 *R v Elomar* [2010] NSWSC 10 (15 February 2010) [63] ('*Elomar*').

that case, five men had been convicted of a conspiracy to do acts in preparation for a terrorist act. While determining the appropriate sentences, Whealy J considered that the offenders' motive to protest Australia's involvement in the Iraq war was sufficiently political to satisfy paragraph (b).[13]

Although the recent terrorism cases have invariably involved a 'violent jihad' against the West,[14] there is no reason to suggest that the requirement should be restricted to the motives of Islamic terrorists. In *Thomas v Mowbray*, for example, Kirby J commented that the requirement was potentially 'most extensive in its application', and could extend to attacks against abortion providers, attacks on controversial building developments, and attacks against the interests of foreign governments in Australia.[15]

Under this framework, it is probable that the motives behind Operation Titstorm were sufficiently political to satisfy the motive requirement of a terrorist act. On the Anonymous website – Project Freeweb – the group details its motive to protest the government's plan to 'massively filter and censor Australia's Internets tubes [sic]'.[16] It recognises that censorship is more than just a local issue, and believes that the proposed filter parallels the development of the Echelon signals intelligence program, the US Patriot Act and 'The Great Firewall of China'.[17] The authors of the website state that:

> the Great eBarrier Reef will be a huge black eye for Australia's reputation internationally and put the country in the same corner with the likes of Iran, China and North Korea when it comes to discussing freedom of speech, censorship and net neutrality.[18]

Although, arguably, censorship issues do not endanger human life to the extent of the Iraq war, and do not evoke as fervent a political response as Islamic terrorism, there is no reason that an attack motivated by a government's censorship policies should be considered conceptually different from an attack to protest a government's decision to go to war. It is therefore likely that Operation Titstorm, or another similar cyber-attack directed at domestic political issues, would satisfy the motive requirement of a terrorist act in section 100.1(b) of the *Code*.

---

13 Ibid [171].

14 See, eg, ibid [63]; *R v Benbrika* (2009) 222 FLR 433, 437 [14]–[15]; *R v Atik* [2007] VSC 299 (23 August 2007) [11].

15 *Thomas v Mowbray* (2007) 233 CLR 307, 401. While Kirby J disagreed with the orders of the court in relation to the constitutional validity of the control order legislation, there is no reason to suggest that the majority would have interpreted section 100.1(b) narrowly. See, eg, Gummow and Crennan JJ's comments on the application of section 100.1(c), below n 20, which suggest that the objects of coercion or intimidation are to be given a broad scope under the defence and external affairs powers in section 51(vi) and (xxix) of the *Australian Constitution*.

16 Project Freeweb: Encyclopedia Dramatica (2010) <http://encyclopediadramatica.com/Project_Freeweb>.

17 The Great eBarrier Reef: Encyclopedia Dramatica (2010) <http://encyclopediadramatica.com/The_Great_eBarrier_Reef>; see also, ibid.

18 Project Freeweb: Encyclopedia Dramatica, above n 16. The 'Great eBarrier Reef' is the term used by Anonymous to refer to the firewalls and filters that the government will put in place for its mandatory internet filter (akin to 'the great firewall of China').

Second, a terrorist act must be intended to coerce or influence a government by intimidation.[19] As with the motive requirement, the intimidation requirement in section 100.1(c) has received little judicial discussion directly on point. The essential condition is that the offenders use threats or violence to influence the government to act or refrain from acting in a particular way. In *Thomas v Mowbray*, Hayne J emphasised that 'intimidation' should be read in its ordinary sense; that is, 'the use of threats or violence to force to or to restrain from some action'.[20] In *Elomar*, Whealy J considered that the offenders' intention 'to intimidate … the Government of Australia so as to bring about a change in governmental policy towards the Muslim situation overseas' was sufficient to satisfy paragraph (c).[21]

Operation Titstorm was similarly intended to threaten the Australian government into changing its policy on censorship. Below is an image of a flyer used by Anonymous to recruit members for the attacks:[22]

19 Alternatively, a terrorist act may intimidate the public or a section of the public: *Criminal Code Act 1995* (Cth) s 100.1(c)(ii). This paper focuses on the requirement of influencing a government by intimidation in s 100.1(c)(i) because it is most relevant to the facts of Operation Titstorm. However, either could potentially be used as a source of liability, and a similar analysis would apply.

20 (2007) 233 CLR 307. In this case, as with Kirby J, Hayne J disagreed with the orders of the Court in relation to the constitutional validity of the control order legislation, and so this does not amount to clear precedent on the issue: at 451. However, there is no reason to suggest that the majority would have interpreted section 100.1(c) more narrowly than the ordinary sense of the word. It is clear from the judgment of Gummow and Crennan JJ, for example, that the object of coercion or intimidation may be a government or section of the public either within or outside Australia (due to the combined scope of the defence and external affairs powers in section 51(vi) and (xxix) of the *Australian Constitution*): at 337, 364.

21 [2010] NSWSC 10 (15 February 2010) [171].

22 Asher Moses, 'Operation Titstorm: Hackers Bring down Government Websites', *Sydney Morning Herald* (online), 10 February 2010 <http://www.smh.com.au/technology/technology-news/operation-titstorm-hackers-bring-down-government-websites-20100210-nqku.html>.

In a video posted on YouTube during the attacks, members of Anonymous then delivered the following threat to the Prime Minister:

> Hello, Prime Minister Rudd …
>
> We shall proceed to do everything in our power to annihilate your government's presence on the internet.
>
> You have nowhere to hide, because we are everywhere.
>
> We are Anonymous.
>
> …
>
> Expect us.[23]

The Project Freeweb website also reveals motives that go beyond simple mischief:

> They can dress it up any way they want but – at the end of the day – this isn't about small titties and cartoon dongs … [T]his is all about controlling the flow of information and that's why we have to go to war with them and fight this thinly veiled 'land grab'.[24]

These excerpts may misrepresent the views of some Anonymous members, who are more focused on gaining publicity than on going to war with the government over censorship. One protestor, for example, posted the following in an internet chat room after a similar attack in September 2009:

> <shoza_woghorse> we got what we wanted
>
> …
>
> <shoza_woghorse> the aim was never to take out the siteeeeeeee
>
> <shoza_woghorse> it was to get publicity[.][25]

Nonetheless, because the motive requirement need not be attributed to any particular individual, it is likely that the overall intentions behind Operation Titstorm involved sufficient intimidation of the government to satisfy paragraph (c). The fact that Anonymous' actions were unlikely to influence the government into abandoning its plans to install the filter – as Secretary of the Department of Parliamentary Services Alan Thompson rejoined after the attacks[26] – is irrelevant to the question of whether Anonymous subjectively intended to use threats to influence the government to change its censorship policy.

While these are not the only requirements for a cyber-attack to qualify as a terrorist act, they are the first crucial steps in any prosecution under the legislation. It seems that Operation Titstorm, or another similar cyber-attack, would satisfy the low thresholds of the political motive and intimidation requirements in sections 100.1(b) and (c) of the *Code*. The next section of this paper looks at whether Operation Titstorm satisfies the first limb of paragraph (a)

---

23 Operation Titstorm: Encyclopedia Dramatica (2010) <http://encyclopediadramatica.com/Operation_Titstorm>.

24 Project Freeweb: Encyclopedia Dramatica, above n 16.

25 See Asher Moses, 'Hacked by Hoons: How Attack on PM's Website Unravelled', *Sydney Morning Herald* (online), 10 September 2009 <http://www.smh.com.au/doc/anonymous.pdf>.

26 See Davis, above n 2.

– the harm requirement – and whether the government intended to include cyber-attacks against websites and email systems within the definition of a terrorist act.

2 *Seriously Interferes with an Electronic System*

The first limb of paragraph (a) in section 100.1 of the *Code* states that an action must fall within sub-s (2) to qualify as a terrorist act. Sub-s (2) lists the possible harm requirements of a terrorist act.[27] In the case of a cyber-attack, the relevant harm will likely fall within section 100.1(2)(f),[28] which states that the act will fall within sub-s (2) if it:

> (f) seriously interferes with, seriously disrupts, or destroys, an electronic system including, but not limited to:
>
> (i) an information system; or
>
> (ii) a telecommunications system; or
>
> (iii) a financial system; or
>
> (iv) a system used for the delivery of essential government services; or
>
> (v) a system used for, or by, an essential public utility; or
>
> (vi) a system used for, or by, a transport system.

On face value, it appears that Operation Titstorm would fall within this section, given that its scope theoretically extends to any 'electronic system'. Known as a denial of service attack, Operation Titstorm sent 7.5 million requests per second to the parliamentary website, which overloaded the government server and prevented anyone from accessing its material for the three days it took to restore the server. Separate attacks also flooded parliamentary inboxes and the Prime Minister's homepage with pornographic material. Cyber-attacks such as these are by their very nature designed to seriously interfere with electronic systems. An important question remains, however, as to whether an 'electronic system' could include a website or email system, or whether it is restricted to more essential types of infrastructure akin to those listed in paras (i)–(vi).

There is yet to be any judicial pronouncement on this question,[29] but section 100.1(2)(f) did receive some attention in the Senate before the current definition of a terrorist act was passed. Opposing the inclusion of section 100.1(2)(f) in the Security Legislation Amendment (Terrorism) Bill 2002 (No 2), Senator Harris

---

27 The possible harm requirements of a terrorist act (other than that discussed) in section 100.1(2) are:

> (a) causes serious harm that is physical harm to a person; or
>
> (b) causes serious damage to property; or
>
> (c) causes a person's death; or
>
> (d) endangers a person's life, other than the life of the person taking the action; or
>
> (e) creates a serious risk to the health or safety of the public or a section of the public.

28 There are, of course, other offences that address the problem of hacking and cyber-attacks. This article focuses on the point at which a cyber-attack may be considered terrorism under Australian law. For a range of other offences, see especially *Criminal Code Act 1995* (Cth) div 477; *Crimes Act 1900* (NSW) pt 6.

29 To date there have not been any prosecutions for an electronic cyber-attack under section 100.1(2)(f). The closest a terrorism prosecution has come is *Lodhi*, in which the accused used the internet to download images of Australia's military facilities: see *R v Lodhi* (2005) 199 FLR 236, 241 [23].

asked the Minister for Justice and Customs (Senator Ellison) whether section 100.1(2)(f) envisioned an attack to an email system:

> Senator Harris: Again I pose the question to Senator Ellison: does this 'interfering with an electronic system' include email? Is it a terrorist act to interfere with an email system for the purpose of advancing a political, religious or ideological cause? Because this definitely can be read in that manner under this Act.
>
> …
>
> Senator Ellison: Of course, an email might be part and parcel of such interference with an electronic information system. You might have the denial of service through the use of emails. That is, a lot emails are employed to cut off service of a government instrumentality … It does not necessarily say that an email in itself can be a terrorist act, but certainly an email can be part and parcel of an action which constitutes a terrorist threat.[30]

Evidently, the government intended that denial of service attacks to 'government instrumentalities' would be caught under section 100.1(2)(f). Presumably this would include more serious cyber-attacks that prevented statutory bodies or state owned corporations from providing services to the general public (for example, if a cyber-attack prevented EnergyAustralia from supplying the public with gas and electricity).[31] It is less apparent whether this would include cyber-attacks against parliamentary websites, which only prevent people logging onto the website from retrieving the requested information. Directly on point was a question from Senator Greig:

> Senator Greig: Let us consider … that you have culture jamming or hacking into a web site which has a political cause – for example, activists jamming or defacing the parliamentary web site … Are we going down the path of bringing about a situation where activists … might be deemed to have committed a terrorist act, or be engaged in terrorism, by engaging in hacking or cracking through the World Wide Web where it could be identified that behind that there was to some small degree political cause?
>
> …
>
> Senator Ellison: That is precisely the point of the provision for 'lawful advocacy, protest or dissent …' … But if the action oversteps that, and you have serious interference with an electronic system and the threat is made with the intention of advancing a cause, then you could have some problem. You could face some liability, as I see it.[32]

Although the Minister did not provide a definite answer on the issue (and putting aside for the moment the question of whether the political protest exception in section 100.1(3) applies), he did not deny the possibility that jamming or defacing the parliamentary website could be included within section 100.1(2)(f).

Of course, the Minister's prediction will not be determinative in a court of law. Nonetheless, his approach seems broadly consistent with the phrase 'electronic system', because denial of service attacks do not simply affect a

30 Commonwealth, *Parliamentary Debates*, Senate, 24 June 2002, 2453 (Len Harris); Commonwealth, *Parliamentary Debates*, Senate, 24 June 2002, 2456–7 (Chris Ellison).

31 *Heritage Act 1977* (NSW) s 4 (definition of 'government instrumentality').

32 Commonwealth, *Parliamentary Debates*, Senate, 24 June 2002, 2482 (Brian Greig, Chris Ellison).

website in isolation, but slow down the physical computer systems 'behind' the targeted website.[33] These computers operate website server software, which enables browsers to request and retrieve the various scripts and documents that constitute the website. In the case of federal government websites, these computer servers are largely housed by private companies under secure Defence Signals Directorate accredited protocols.[34] When overloaded with a sufficient number of simultaneous requests, these computer systems slow down to the point where their content becomes effectively unavailable. Thus a denial of service attack against the parliamentary website would have a direct effect on the physical electronic system that enables that website to be accessed.

It is unlikely that flooding an email inbox with obscene material would disrupt an electronic system to the same extent as a denial of service attack. While the secure federal government servers also host email software that enables parliamentary email inboxes to be accessed,[35] simply flooding these inboxes with unwanted images would not disrupt the physical computers operating the email software. It would, of course, cause inconvenience for the email recipients, but in small volumes this would not have any more significant effect on the electronic system that allows those emails to be accessed. The electronic mail system would work as per usual, only the emails would have a different content to that which was expected. Nonetheless, if an email system may be considered an electronic system (in the same way that a website may be considered an electronic system), then it is possible that one could 'seriously interfere' with that system from the browser's end without requiring a more direct effect on the computers that house its software. The same logic would also apply to the attacks that plastered obscene images across the Prime Minister's homepage.

Whatever the case, it is important to recognise that a cyber-attack may qualify as a terrorist act under section 100.1(2)(f) even where it does not cause – and is not intended to cause – any lasting physical or economic damage. This will be examined further in Part III. For the moment, it is sufficient to note that the lowest harm threshold for section 100.1(2)(f) to apply is when an act 'seriously interferes with … an electronic system', and that the government did not rule out the possibility that the provision could extend to cyber-attacks against websites and email systems.

In terms of the level of intent required of the harm caused in section 100.1(2)(f), this could be implied as either intention or recklessness, depending on how the provision comes to be interpreted. In its review of the sedition

---

33 For an explanation of denial of service attacks, see United States Computer Emergency Readiness Team ('CERT'), *Understanding Denial-of-Service Attacks* (4 November 2009) US CERT <http://www.us-cert.gov/cas/tips/ST04-015.html>. For a more complex typology see Felix Lau et al, *Distributed Denial of Service Attacks* (28 February 2001) Berkeley <http://www.eecs.berkeley.edu/~ljilja/papers/smc00_edited.pdf>.

34 See, eg, Government Secure Hosting Australia, *DSD Gateway Accredited Secure Gateway Hosting Macquarie Telecom* (2010) <http://www.macquarietelecom.com/hosting/government_server_hosting_australia.htm>.

35 See ibid.

provisions in section 80.2 of the *Code*, the Australian Law Reform Commission ('ALRC') noted that, where a physical element of an offence makes no reference to fault, it will be implied as requiring either intention or recklessness, depending on whether it proscribes *conduct* or a *result*.[36] This process relies upon section 5.6 of the *Code*, which provides that:

> (1) If the law creating the offence does not specify a fault element for a physical element that consists only of conduct, intention is the fault element for that physical element [; and]
>
> (2) If the law creating the offence does not specify a fault element for a physical element that consists of a circumstance or result, recklessness is the fault element for that physical element.

It is unclear which of these two standards section 100.1(2)(f) requires. To 'seriously interfere' with an electronic system appears to involve conduct (in contrast to wording such as 'causes serious interference', which would be more akin to a circumstance or result). To 'destroy' an electronic system appears to involve the opposite, by proscribing a circumstance or result, while 'disrupts' could arguably be interpreted either way: 'engages in a process of disrupting' (conduct) or 'causes disruption' (a result). Arguably, therefore, an act that *seriously interferes* with an electronic system would require intent, an act that *destroys* an electronic system would only require recklessness, and an act that *disrupts* an electronic system could fall either way. Whether or not Anonymous seriously interfered with or disrupted the parliamentary website would be open to debate on the facts. If, however, Anonymous' actions fell under the disrupts limb of the test, and this was considered to be a result rather than conduct, then the prosecution would only need to prove that Anonymous was reckless as to whether their actions would disrupt the parliamentary server.

Without any judicial pronouncement on the issue it is impossible to definitively gauge the application of section 100.1(2)(f) to the facts of Operation Titstorm, or the particular level of intent required by that provision. Nonetheless, it seems unlikely, given the broad intended scope of the provision, that Anonymous would be able to prove that they did not intend to 'seriously interfere with … an electronic system' by jamming the parliamentary website. It is less evident whether Anonymous' attacks against parliamentary inboxes and the Prime Minister's homepage would qualify under the same provision, although there is still a good argument to be made in this regard.

It is therefore likely that Operation Titstorm (or at least its denial of service attack against the parliamentary website) would satisfy the positive requirements of a terrorist act in section 100.1 of the *Code*. It was intended to advance a political cause, influence the government into changing its policy on censorship, and seriously interfere with or disrupt an electronic system. The next section analyses whether Anonymous would be able to rely on the second limb of paragraph (a) – the political protest exception – to avoid the application of section 100.1.

---

36 ALRC, *Fighting Words: A Review of Sedition Laws in Australia*, Report No 104 (2006), 177–8 [8.43].

B Only as Good as Its Weakest Link: The Political Protest Exception

The second limb of paragraph (a) provides that an action will not qualify as a terrorist act if it falls within sub-s (3). Sub-s (3) provides that an:

> (3) Action falls within this sub-s if it:
>
> (a) is advocacy, protest, dissent or industrial action; and
>
> (b) is not intended:
>
> (i) to cause serious harm that is physical harm to a person;
>
> (ii) to cause a person's death; or
>
> (iii) to endanger the life of a person, other than the person taking the action; or
>
> (iv) to create a serious risk to the health or safety of the public or a section of the public.

As with the other requirements of a terrorist act, there has been little judicial discussion about the precise application of section 100.1(3). Nonetheless, there are two main points that we can glean from the case law and Senate debates about the application of the provision. These suggest that the prosecution will only need to overcome a low burden in order to prove that the exception does not apply.

First, the onus is on the prosecution to prove beyond reasonable doubt that section 100.1(3) does not apply. In *Lodhi*, the defendant was charged with a number of terrorism offences: collecting a document connected with preparation for a terrorist act; doing an act in preparation for a terrorist act; making a document connected with preparation for a terrorist act; and possessing a thing connected with preparation for a terrorist act. Spigelman CJ quashed the indictment on appeal and remitted it to the trial judge because the Crown had not pleaded section 100.1(3). His Honour held that the Crown 'is required to establish beyond reasonable doubt that the action was not advocacy, protest, dissent or industrial action or was not intended to have one of the effects identified in (b) of sub-s (3)'.[37]

While *Lodhi* appears to be decided in favour of the defendant, it sets a low threshold for the prosecution to prove that the political protest exception does not apply. To prove beyond reasonable doubt that the exception *does* apply would require a defendant proving both limbs of the exception: that the action is advocacy, protest, dissent or industrial action *and* that the action is not intended to cause one of the listed harms. To prove beyond reasonable doubt that the exception *does not* apply requires the prosecution to prove merely one element of the second limb: that the action is intended to cause any one of the harms listed in sub-s (b). This distinction becomes apparent from Spigelman CJ's use of 'or' in the above excerpt, which contrasts with the use of 'and' in the legislation.[38] This means that the political protest exception is only as good as its weakest link: if the prosecution can prove that the act was intended to 'create a serious risk to the

37 *Lodhi* (2006) 199 FLR 303, 324 [93].

38 Presumably, because he states that the onus is on the prosecution, the inference is that the act *was* intended to have one of the listed harms.

… safety of … a section of the public', then, regardless of whether the action can be properly characterised as 'protest' or 'dissent', the exception will not apply.

Second, it is apparent that a certain level of intended harm will bring an act outside the terms 'protest', 'advocacy', 'dissent' and 'industrial action'. In *R v Atik*, a member of the Benbrika organisation pleaded guilty to intentionally being a member of, and providing resources to, a terrorist organisation.[39] That organisation intended to detonate explosives and incendiary devices to cause serious injury to civilians. The Crown submitted that 'the nature of the actions proposed … took them outside the concepts of "advocacy, protest, dissent or industrial action" that the Code recognises might excuse what would otherwise amount to terrorist activity'.[40] This submission was challenged neither by the defendant nor the Victorian Supreme Court.

While this does not amount to clear precedent on the issue, the Court's reasoning appears consistent with the government's intentions in enacting the provision. Following the debate about whether disrupting the parliamentary website would fall within section 100.1(2)(f), the Minister for Justice and Customs explained his earlier submission in respect of the political protest exception: 'I clarify my earlier remarks and say that there should be an intention to harm … So if you are doing it with intention to harm then you fall foul of the subsection.'[41] The Minister rejected a suggestion that 'minor' political protests would fall foul of the exception,[42] but left open the possibility that serious political protests could be prosecuted as terrorist acts. It seems, therefore, that whether or not an act can be properly characterised as political protest, a certain level of intended harm will take the protest outside the political protest exception in section 100.1(3).

During debate in the Senate, the Minister provided an example of the point at which this level of harm will be reached. When asked whether the S11 protests in Melbourne (in September 2000) would qualify as a terrorist act, the Minister answered that they most definitely would.[43] During those protests, approximately 10 000 protesters laid siege to Melbourne's Crown Casino and blocked hundreds of delegates from attending a World Economic Forum on the impact of globalisation. The protest was largely non-violent, although it involved some isolated hostilities. The Premier of Western Australia Richard Court had his car ringed by protesters for an hour; the car's tyres were slashed and its body defaced with spray-paint. Five police officers were injured and two were taken to

39 [2007] VSC 299 (23 August 2009) [9].

40 [2007] VSC 299 (23 August 2007) [9].

41 Commonwealth, *Parliamentary Debates*, Senate, 24 June 2002, 2482 (Chris Ellison).

42 Ibid 2445 (Chris Ellison).

43 Ibid 2485–6 (Bob Brown, Chris Ellison). In the Senate Hansard, Senator Brown refers to the 'S18' protests in Melbourne whilst Premier Steve Bracks was in office. The 'S11' protests occurred in Melbourne in 2000 while Premier Bracks was in office, and followed similar protests at the World Trade Organization in Seattle in 1999. They are well known as one of the largest contemporary Australian political protests (and for the forceful actions of the Victorian Police) and so Senator Brown is likely referring to this event: see media reports, below n 44.

hospital. One trainee hotel worker was hospitalised with a broken jaw, female casino staff were harassed and ambulance staff were abused.[44] While these are undoubtedly serious matters, the S11 protests set a low harm requirement for an act of terrorism deserving life imprisonment. If this threshold were adopted in court, the prosecution would only need to overcome a low burden to prove that the political protest exception does not apply.

It is unlikely that the freedom of political communication – implied from sections 7 and 24 and the wider structure of the *Australian Constitution* – would act to expand this possible scope of section 100.1(3), or restrict the application of sections 100.1(1) and (2), in cases that exceed legitimate criticism of government policies. The approach taken by the High Court in *Lange v Australian Broadcasting Corporation*,[45] and later modified in *Coleman v Power*,[46] provides that a law will be invalid, or construed more narrowly, if it (1) effectively burdens freedom of communication about government or political matters and (2) is not reasonably appropriate and adapted to serve a legitimate end in a manner that is compatible with the maintenance of the constitutionally prescribed system of representative and responsible government.[47] The implied freedom includes non-verbal conduct[48] and so could include an online protest such as Operation Titstorm, although the Court made clear in *Levy* that the freedom was not absolute, and only extended to 'what is necessary to the effective working of the *Constitution*'s system of representative and responsible government.'[49]

When considering what is necessary to maintain a system of responsible government, the High Court has repeatedly held that words or conduct designed to intimidate governments will not fall within the ambit of protected political communication. In *Australian Capital Television Pty Ltd v Commonwealth*, for example, Mason CJ stated that 'Parliament may regulate the conduct of persons with regard to elections so as to prevent intimidation and undue influence, even though that regulation may fetter what otherwise would be free communication.'[50] So it seems likely that an act – such as Operation Titstorm – that satisfied section 100.1(c) by intending to influence a government by intimidation would not fall within the ambit of constitutionally protected political communication, regardless of how the rest of section 100.1 came to be applied.

This seems to have played out recently in an anti-terrorism context when the ALRC considered the constitutionality of sedition offences criminalising the urging of conduct by 'force or violence'. The ALRC noted that such conduct was 'quite different from the kind of criticism of government that the cases on the

---

44 See 'Melbourne under Siege: Premier Trapped as Protests Erupt at World Economic Forum', *The Australian* (Sydney), 12 September 2000; Andrew Rule, Claire Miller and Paul Robinson, 'Battle of Melbourne', *The Age* (Melbourne), 12 September 2000.

45 (1997) 189 CLR 520 ('*Lange*').

46 (2004) 220 CLR 1.

47 *Lange* (1997) 189 CLR 520, 567; *Coleman v Power* (2004) 220 CLR 1, 50 (McHugh J). The latter judgment added the words 'in a manner' to the second limb.

48 *Levy v Victoria* (1997) 189 CLR 579, 595 (Brennan CJ) ('*Levy*').

49 (1997) 189 CLR 579, 624 (McHugh J).

50 (1992) 177 CLR 106, 142–3; see also *Coleman v Power* (2004) 220 CLR 1, 54 (McHugh J).

constitutional protection of freedom of political communication aim to protect',[51] and advised that the provisions did not infringe the implied freedom because they could not be 'construed in such a way as to capture mere criticism of government action'.[52] It seems that a similar analysis would apply to the current definition of a terrorist act in section 100.1, which cannot be construed to capture 'mere criticism of government action' as long as section 100.1(c) requires a genuine element of intimidation. Of course, the implied freedom of political communication may act as a brake on the arbitrary use of the anti-terrorism legislation against acts that *do not* involve this genuine element of intimidation, and the courts will likely apply sections 100.1(c) and (3) with this in mind. Nonetheless, it is unlikely that the freedom will have a substantive effect in the majority of cases involving acts that exploit the system of representative government by attempting to intimidate governments into changing their policies.

Again, however, without extensive judicial consideration it is not evident what precise level of harm would be required of an act to fall foul of the political protest exception. More importantly, in the case of Operation Titstorm, it seems unlikely that jamming and defacing the parliamentary website would reach the level of intended harm of the S11 protests and fall foul of sub-s (3): there was no physical altercation between protesters and police, and there was no serious physical damage to persons or property. Nonetheless, this assessment, and the future application of sub-s (3) to politically motivated cyber-attacks, depends upon a number of unanswered questions about the similarities and differences between political protest in the 'real' and 'cyber' worlds. For example, is having 10 000 protesters preventing people from accessing a building the same as having 10 000 (or more likely 10 million) server requests preventing people from accessing a website? Is defacing a car with spray-paint the same as defacing a website with pornographic material? Is physically disrupting an international forum the same as disrupting that forum by altering delegates' personal details or blacking out the electricity grid?

If these questions could be answered in the positive – and there are certainly conceptual similarities between them – then it is probable that a more serious version of Operation Titstorm would satisfy all of the requirements of a terrorist act. If, for example, Operation Titstorm had been directed at an international forum on censorship, and caused a level of harm that was considered to be the digital equivalent of the S11 protests, then this would likely satisfy the positive requirements in sections 100.1(b), (c) and (2), and fall foul of the political protest exception in section 100.1(3).

The next Part reaches the crux of this analysis, by investigating whether this conclusion is satisfactory, and whether additional protections need to be put into place to prevent less serious forms of online political protest from being prosecuted as terrorist acts.

---

51 ALRC, *Fighting Words*, above n 36, 143 [7.17]–[7.18].

52 Ibid 144 [7.20].

III PROBLEMS WITH THE CURRENT DEFINITION OF A TERRORIST ACT AGAINST AN ELECTRONIC SYSTEM

If online political protest can be prosecuted as a terrorist act by intending an analogous level of harm to the S11 protests, then the *Code* sets the threshold too low for prosecuting acts of electronic terrorism in Australia. The political protest exception does not have sufficient safeguards to maintain the important distinction between acts of hacktivism and acts of cyber-terrorism. This distinction could be maintained in the legislation by amending section 100.1(2)(f) to include a serious economic harm requirement and an express fault element. These changes would bring Australia's anti-terrorism legislation in line with definitions of terrorism at international law and in comparable domestic jurisdictions, and with definitions of cyber-terrorism in computer science. They would reduce the risk of prosecuting undeserving offenders, prevent governments from using the anti-terrorism legislation to silence less serious forms of political protest against electronic systems, and avoid any potential chilling effect on the freedom of online political expression.

A Inadequate Political Protest Exception

The political protest exception in section 100.1(3) received much opposition in the Senate before it was passed in its current form; allegedly, it creates the possibility that many legitimate forms of democratic protest will be prosecuted as terrorist acts.

Primarily, this opposition revolved around the argument that many legitimate forms of political protest involve a serious risk to the safety of a section of the public, which is the weakest link in the political protest exception. Senator Brown, for example, argued for the Greens that:

> [t]here are many actions taken by community organisations or unions which, it could be argued, create a serious risk to the health or safety of the public … Protest very often is intended to be obstructive and can have risky consequences. The very nature of protest is to exhibit commitment and very often, in the process of exhibiting commitment, to involve oneself in risk, and potentially involve others in risk as well.[53]

Senator Brown gave the examples of nurses or doctors taking industrial action and environmentalists protesting in treetops.[54] He asks,

> How could nurses who were on strike say that they did not know that there were some risk to some members of the public, as far as their health and wellbeing is concerned, when beds were actually being closed through that strike action?[55]

---

53 Commonwealth, *Parliamentary Debates*, Senate, 24 June 2002, 2481 (Bob Brown). Senators Brian Greig and Natasha Stott Despoja also expressed dissatisfaction with the political protest exception: see Commonwealth, *Parliamentary Debates*, Senate, 24 June 2002, 2355, 2475 (Brian Greig); Commonwealth, *Parliamentary Debates*, Senate, 24 June 2002, 2405–6 (Natasha Stott Despoja).

54 Commonwealth, *Parliamentary Debates*, Senate, 24 June 2002, 2481, 2486 (Bob Brown).

55 Ibid 2487 (Bob Brown).

The rationale for supporting these forms of political protest, despite the fact that they create a serious risk to the safety of a section the public, is that political protest is 'fundamental to a functioning democracy'.[56] For a government to use the anti-terrorism provisions to silence opposition to its policies would amount to a fundamental breach of responsible government.[57]

Of course, one might argue that it is unlikely that the government will use the anti-terrorism legislation to prosecute mischievous acts such as Operation Titstorm. To the Greens and Australian Democrats, however, it does not matter whether the anti-terrorism provisions *will* be used in such a way; it is sufficient that they create the *possibility* that future governments will use the provisions to silence legitimate forms of dissent.[58] It is about limiting the institutions of a democratic government, such that their powers cannot be abused in the event of exceptional circumstances justifying extreme action.[59]

It is also about the *perceived*, as well as actual, impact of the laws on the civilian population: McNamara, for example, has emphasised the importance of analysing the scope of anti-terrorism legislation not merely in terms of 'the position of persons who are suspected of supporting or engaging in terrorist activities', but also in terms of those people 'who are in neither of those positions'.[60] The purpose of engaging in this analysis is to see whether the legislation is likely to create a chilling effect on legitimate forms of political expression, which may occur where protestors become concerned their actions will be targeted under criminal legislation.[61] Indeed, this article's opening quote, in which one Anonymous member has already expressed concern that they will be targeted as terrorists by the Australian government, reveals the reality of this chilling effect.

Even if these arguments are accepted, however, and the legislation should be strengthened so that governments will not be able (and will not be seen to be able) to prosecute legitimate acts of democratic protest, the question still remains: was Operation Titstorm a legitimate form of democratic political protest? Should a similar but slightly more serious cyber-attack be prosecuted as an act of terrorism?

As argued above, acts that intend to change government policy through intimidation are unlikely to qualify as 'legitimate' forms of protest for the purposes of the implied freedom of political communication, because such acts will not be compatible with a system of representative government. In this narrow sense, Operation Titstorm was *not* a legitimate form of democratic

---

56 Ibid 2486 (Bob Brown).

57 Senator Stott Despoja described it as an 'outrage': see Commonwealth, *Parliamentary Debates*, Senate, 24 June 2002, 2405–6 (Natasha Stott Despoja).

58 Commonwealth, *Parliamentary Debates*, Senate, 24 June 2002, 2356 (Brian Greig); Commonwealth, *Parliamentary Debates*, Senate, 24 June 2002, 2406 (Natasha Stott Despoja).

59 Commonwealth, *Parliamentary Debates*, Senate, 24 June 2002, 2407 (Natasha Stott Despoja).

60 Lawrence McNamara, 'Closure, Caution and the Question of Chilling: How Have Australian Counter-Terrorism Laws Affected the Media?' (2009) 14 *Media and Arts Law Review* 1–2.

61 See ibid; see also David Hume and George Williams, 'Advocating Terrorist Acts and Australian Censorship Law' (2009) 20 *Public Law Review* 37.

political protest, because it intended to intimidate the Rudd Labor government into abandoning its plans to install a mandatory internet filter. It does not follow, however, that all illegitimate cyber-protests should therefore qualify as acts of cyber-terrorism. Nor does this conclusion detract from the possibility of the legislation having a chilling effect on legitimate acts of online political protest, which do not eventuate due to fear of criminal liability. Nor does it detract from the Greens' broader point, which is that governments should not have the power to silence political protest merely because it intends to create a serious risk to the health or safety of the public. Until this standard is raised, section 100.1 of the *Code* is incapable of distinguishing between cyber-attacks that are worthy of the label of cyber-terrorism and those that may be illegitimate – and even unlawful – but are nonetheless unworthy of the cyber-terrorism label and the serious penalties involved.

When conceptualising this distinction, it is important to consider the phenomenon of hacktivism, a form of online protest that uses the techniques of hacking computer systems for political purposes. Conway has argued that hacktivists do not see themselves as violent criminals bent on the destruction of innocent life, but as the 'heirs to those who employ the tactics of trespass and blockade in the realm of real-world protest'.[62] Although acts of hacktivism and terrorism may display some similar characteristics, Conway argues, the fact remains that 'terrorism is an extreme and violent occupation, and far more aberrant than prankish hacking'. Hacktivists, despite their 'propensity for expensive mischief', have not demonstrated that they are 'willing to jeopardise lives … for a political cause'.[63] According to Conway, it would be going too far to label these hacktivists as cyber-terrorists.

Of course, to some extent it is irrelevant how hacktivists see their own actions, but these comments do provide some insight into the motives of hacktivists such as the Anonymous group, and the particular blame we should ascribe to their actions. So long as acts of hacktivism do not intend to cause serious harm to a civilian population, there remains a fundamental conceptual difference between politically motivated cyber-attacks and acts of cyber-terrorism.

So much has been recognised by Dorothy Denning, a former Professor of Computer Science at Georgetown University and one of the foremost experts on issues of cybercrime and cyber-terrorism. In evidence given to the Special Oversight Panel on Terrorism of the US House of Representatives Committee on Armed Services, Denning testified that:

> [c]yberterrorism … is generally understood to mean unlawful attacks and threats of attack against computers, networks, and the information stored therein … Attacks that lead to death or bodily injury, explosions, plane crashes, water

62 Maura Conway, 'Hackers as Terrorists? Why It Doesn't Compute' [2003] (12) *Computer Fraud and Security* 10–13. This seems to bear out in this article's opening quote, in which some members of Anonymous were concerned about being labeled as terrorists. See also Gabriel Weimann, 'Cyberterrorism: The Sum of All Fears?' (2005) 28 *Studies in Conflict and Terrorism* 129, 135–6.

63 Maura Conway, above n 62, 13.

> contamination, or severe economic loss would be examples. Serious attacks against critical infrastructure could be acts of cyberterrorism, depending on their impact. Attacks that disrupt nonessential services or that are mainly a costly nuisance would not.[64]

This definition has since been cited in a number of authoritative sources.[65] It makes clear that cyber-attacks involving serious additional consequences should qualify as acts of terrorism, and mischievous acts that disrupt nonessential services should be properly left in the domain of less serious computer offences.

It is unlikely that anyone would dispute this crucial distinction,[66] but its absence from the current anti-terrorism legislation should not be taken lightly. There is a real danger that acts of hacktivism will not be protected by the political protest exception, because the weakest link of section 100.1(3) requires the low threshold of intending to 'create a serious risk to the safety of a section of the public'. The dangers of this are apparent not only from the comments by the Greens and Australian Democrats above, but also in the potential chilling effect this may have on online political expression in Australia if hacktivists become concerned that their actions may be targeted under the legislation. The next section suggests some ways that the threshold for these requirements could be raised, in order to reduce the risk that governments will be able to use the anti-terrorism legislation to target forms of online political protest that are unworthy of the label of cyber-terrorism.

B Amending Section 100.1(2)(f)

To say that there is a fundamental difference between acts of hacktivism and acts of cyber-terrorism is not to say that someone declaring themselves a hacktivist could never commit an act deserving life imprisonment under the anti-terrorism legislation, or that hacktivists should not be subject to less severe criminal penalties. It is also not to deny the possibility of a devastating cyber-attack against Australia's critical infrastructure. However, until politically motivated cyber-attacks satisfy the existing elements of a terrorist act *and* intend to cause a more serious level of harm to Australian infrastructure, they should not be labelled, or prosecuted, as terrorist acts. Section 100.1(2)(f) of the *Code* should be amended to include a serious economic harm requirement and an express fault element. This would bring Australia's definition of a terrorist act in line with definitions of terrorism at international law and in comparable domestic

---

64 Dorothy Denning, 'Cyberterrorism: Testimony before the Special Oversight Panel on Terrorism, Committee on Armed Services, US House of Representatives' (23 May 2000) <http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html>.

65 See, eg, Walker, above n 3, 633–4; Weimann, above n 62, 135; Gregor Urbas, 'Cyber Terrorism and Australian law' (2005) 8(1) *Internet Law Bulletin* 1, n 5; see also the Symantec Security Response White Paper on Cyberterrorism (2003) 4 <http://www.symantec.com/avcenter/reference/cyberterrorism.pdf> ('Symantec White Paper').

66 The Symantec White Paper did note that 'it is very different from the definition that appears to be operationally held by the media and the public at large': Symantec White Paper, above n 65, 4. The divergence of media and popular opinions should not, however, impact on a rational assessment of the appropriate form to be given to section 100.1(2)(f).

jurisdictions, and with definitions of cyber-terrorism in computer science. It would ensure that the anti-terrorism legislation could only be used to prosecute those cyber-attacks truly deserving of the label of cyber-terrorism.

1 *Serious Economic Harm Requirement for Property Damage*

Although there is no single definition of terrorism at international law, Young has undertaken a detailed study of the various international instruments containing definitions of terrorist acts.[67] He argues that there is 'striking consistency in the form, themes and philosophy of the various conventional statements on terrorism'.[68] This synthesised international definition is not legally binding but does provide a useful yardstick for gauging the appropriateness of domestic anti-terrorism legislation. For consistency with international law, Young argues that a definition of terrorism must proscribe

> [t]he serious harming or killing of non-combatant civilians and the damaging of property with a public use causing economic harm done for the purpose of intimidating a group of people or a population or to coerce a government or international organization.[69]

Young makes clear, in this definition and elsewhere, that serious property damage is not a sufficient level of harm to constitute a terrorist act at international law; this property damage must also result in economic harm.[70] Article 1(b) of the *International Convention for the Suppression of Terrorist Bombings*, for example, requires that an attack against infrastructure be made with 'intent to cause extensive destruction of such a place, facility or system, *where such destruction results in or is likely to result in major economic loss*.'[71]

Some commentators have questioned the value of synthesising definitions of terrorism at international law and of comparing domestic and international definitions. Lim, for example, has argued that

> international law has nothing to say … about whether an ordinary murderer convicted under domestic penal law also becomes a terrorist because of the political or other motivation he has in committing murder. International law is silent on the question of what terrorism is.[72]

While it is true that there is no *unified* definition of terrorism at international law, it cannot be said that international law provides no useful guidance on the

---

67 See Reuven Young, 'Defining Terrorism: The Evolution of Terrorism as a Legal Concept in International Law and Its Influence on Definitions in Domestic Legislation' (2006) 29 *Boston College International and Comparative Law Review* 23–105.

68 Ibid 64.

69 Ibid.

70 Ibid 90.

71 *International Convention for the Suppression of Terrorist Bombings*, opened for signature 15 December 1997, 2149 UNTS 284 (entered into force 23 May 2001) art 1(b) (emphasis added) ('*Bombings Convention*').

72 C L Lim, 'The Question of a Generic Definition of Terrorism Under General International Law' in Victor V Ramraj, Michael Hor and Kent Roach (eds), *Global Anti-Terrorism Law and Policy* (Cambridge University Press, 2005) 37, 61.

nature of terrorist acts.[73] In his leading work *Defining Terrorism in International Law*, Ben Saul argues that a synthesised definition of terrorism can be deduced from the 'international community's identification of the underlying wrongfulness of international terrorism'.[74] According to Saul, if one views terrorism as a crime that seriously violates human rights, then one must define terrorism as 'any serious, violent, criminal act intended to cause death or serious bodily injury, or to endanger life, including by acts against property'.[75] While this definition does not identify economic harm as a requirement of property damage, it does suggest that a harmful act against property must *at least endanger life* in order to reach the level of intended harm of a terrorist act.

Serious property damage is a separate head of harm under section 100.1(2)(b), but may be considered analogous to section 100.1(2)(f) insofar as an electronic system can be considered public or private 'property' (for example, the federal government owns the servers that were affected by Anonymous' denial of service attack). In this respect, section 100.1(2)(f) of the *Code* is inconsistent with definitions of terrorism at international law, because it attaches no additional harm requirement to the interference with, or destruction of, an electronic system: all that is simply required is that an act 'seriously interferes with, seriously disrupts, or destroys, an electronic system'. The list of possible electronic systems in subsections (i)–(vi) does nothing to limit this broad scope, precisely because the definition is 'not limited to' those systems.

Out of five Commonwealth jurisdictions with broadly comparable offences relating to electronic or other infrastructure systems – Australia, New Zealand,[76] Canada,[77] the UK[78] and the Republic of South Africa[79] – only New Zealand in section 5(3)(d) of the *Terrorism Suppression Act 2002* (NZ) attaches any additional requirement to this peculiar form of property damage. It provides, as in Saul's definition, that the serious interference with or disruption to an infrastructure facility must also be 'likely to endanger human life'. And even then, Alex Conte, former legal adviser to the Chief of the New Zealand Defence Force, has argued that this requirement is still too broad and should be 'confined to conduct that is likely to cause death or serious bodily injury.'[80]

Similar guidance is provided by the recent Preamble to the *Council of Europe Convention on the Prevention of Terrorism*, which recalls that 'acts of terrorism have the purpose by their nature or context to … seriously destabilise or destroy

---

73 See International Commission of Jurists, *Assessing Damage, Urging Action: Report of the Eminent Jurists Panel on Terrorism, Counter-Terrorism and Human Rights* (International Commission of Jurists, 2009) 7.

74 Ben Saul, *Defining Terrorism in International Law* (Oxford University Press, 2006) 65.

75 Ibid.

76 *Terrorism Suppression Act 2002* (NZ) ss 5(2), (3)(d).

77 *Anti-Terrorism Act 2001* SC 2001 c 41, s 83.01(b)(ii)(E).

78 *Terrorism Act 2000* (UK) c 11, s 1(2)(e).

79 *Protection of Constitutional Democracy Against Terrorist and Related Activities Act 2004* (SA) s 1(1)(xxv)(a)(vii).

80 Alex Conte, *Counter-Terrorism and Human Rights in New Zealand* (New Zealand Law Foundation, 2006) 372.

the fundamental political, constitutional, economic or social structures of a country or an international organisation.'[81] While this wording is not offered as a strict definition, and does not set any legislative requirement for Australia, Lord Carlile noted in his independent review of the UK definition of terrorism that

> [t]he *Council of Europe Convention* is of signal importance, as it brought the Council into line with the zero tolerance approach of the United Nations confirmed at the 2005 Madrid Summit. It should be noted that the Council of Europe is the source and owner of the *European Convention on Human Rights*.[82]

The possible scope of the Australian definition remains far below the standard set by this *Convention* of 'signal importance' to the UK, which describes acts of terrorism as being designed to seriously destabilise or destroy political, constitutional, economic or social – and not merely 'electronic' – systems. While a cyber-attack against an electronic system *could* seriously destabilise or destroy these fundamental structures, there is no such additional requirement in the Australian legislation. One might question why the Australian (and indeed the UK)[83] legislation sets a standard so far below these international and regional definitions of terrorism, and especially the Council of Europe Convention, which is mandated by the owner of the *European Convention on Human Rights*.[84]

The level of harm required by section 100.1(2)(f) of the Australian *Code* could be made broadly consistent with these definitions by amending the provision to include a serious economic harm requirement. As it currently stands, section 100.1(2)(f) prohibits acts that 'seriously interfere with, disrupt, or destroy an electronic system' where these acts do not aim to seriously destabilise the Australian economy, or indeed result in any amount of economic harm. If section 100.1(2)(f) were amended to include a serious economic harm requirement, it would be broadly consistent with Young's synthesised international definition,[85]

---

81 *Council of Europe Convention on the Prevention of Terrorism*, opened for signature 16 May 2005, CETS No 196 (entered into force 1 June 2007), preamble.

82 Lord Carlile of Berriew, *The Definition of Terrorism* (International Commission of Jurists, 2007) 18. The Madrid International Summit on Democracy, Terrorism and Security was held between 8–11 March 2005 and hosted heads of state and government, leading scholars and key policymakers in the wake of the 2004 terrorist attacks: see About Safe-Democracy.org: International Summit on Democracy, Terrorism and Security (2005) <http://summit.clubmadrid.org/info/about-safedemocracyorg.html>.

83 See Carlile, above n 81. Despite Lord Carlile's insistence on the importance of the *Council of Europe Convention*, it did not appear to have any significant impact on his recommendations. Lord Carlile merely noted that '[t]here is no single definition of terrorism that commands international approval', and his one substantive recommendation (that the definition be amended to provide that an act will only qualify as terrorism if it intends to *intimidate*, and not merely to influence, the target audience) was eventually rejected by the UK government: at 47; *The Government Reply to the Report by Lord Carlile of Berriew QC – Independent Review of Terrorism Legislation: The Definition of Terrorism*, (Command Paper No 7058, the UK Parliament, 2007) 3 [11]; *Terrorism Act 2000* (UK) c 11, s (1)(b).

84 *Convention for the Protection of Human Rights and Fundamental Freedoms*, opened for signature 4 November 1950, 213 UNTS 221 (entered into force 3 September 1953).

85 Young does not strictly require that the economic damage be 'serious'. However, he considers that the above definition is merely a 'minimum' definition of terrorism at international law and added protections can be built into domestic definitions, so long as the domestic definitions create no greater risk that offenders unworthy of the terrorist label are caught under the provisions: see Young, above n 67, 46.

the definition of a terrorist act against infrastructure in the *Bombings Convention*, and the definition offered by the Council of Europe, which contemplates the destabilisation of a national economy. It would also be consistent with definitions of cyber-terrorism in the field of computer science: Denning's definition above, for example, contemplates 'severe economic loss' as a requirement of an act of cyber-terrorism. Writing for the Australian Computer Emergency Response Team ('AusCERT'), Kerr has also argued that acts of cyber-terrorism should not include 'cyber-attack techniques which are incapable of causing bodily harm, fear or *serious economic damage*'.[86]

If section 100.1(2)(f) were amended to include a serious economic harm requirement, a cyber-attack could only be prosecuted where it rose above the level of mere nuisance and had some wider and more significant economic effect. Aside from conforming to the above definitions, the requirement of 'serious' or 'major' economic damage would reduce the risk that mere 'economic harm' might be satisfied by the cost of repairing a website server, or parliamentary workers taking time out of their day to clear a cluttered inbox. The revised section 100.1(2)(f) offered below borrows the South African wording of economic harm contained in its definition of 'terrorist activity', which captures the flavour of 'major economic damage', as well as the destabilisation of a national economy envisioned by the *Council of Europe Convention.*

2 *Express Fault Element*

Amending section 100.1(2)(f) to include an express requirement of intention for interfering with an electronic system would bring this subsection in line with definitions of terrorism in comparable domestic jurisdictions. Out of the five Commonwealth democracies named above, only Australia possibly implies recklessness as the fault level required for an act of terrorism that disrupts or destroys an electronic system or infrastructure facility.

By contrast, the UK definition requires that the act be '*designed* seriously to interfere with or seriously to disrupt an electronic system'.[87] The Canadian definition requires that the act 'intentionally … causes serious interference with or serious disruption of an essential service, facility or system'.[88] The New Zealand definition, as mentioned above, requires that an act is 'intended to cause … serious interference with, or serious disruption to, an infrastructure facility, if

86 Kathryn Kerr, 'Putting cyberterrorism into context', Australian Computer Emergency Response Team (AUSCERT) (2003) <http://www.auscert.org.au/render.html?cid=2997&it=3552> (emphasis added). This negative definition is expressed with 'or' rather than 'and', so economic harm is not expressed as a positive requirement of a terrorist act. However, seeing as inducing 'fear' is not a requirement of the *Code*, the proposed amendment would at least make one improvement on the current definition. For some examples of definitions that include creating 'fear' in a civilian population as a possible physical element of a terrorist act, see *Terrorism Suppression Act 2002* (NZ) s 5(2)(a) (expressed as inducing 'terror'); *Protection of Constitutional Democracy Against Terrorist and Related Activities Act* RSA 2004 c 1 s 1(1)(b)(ii) ('terror, fear or panic').

87 *Terrorism Act 2000* (UK) c 11, s 1(2)(e) (emphasis added).

88 *Anti-Terrorism Act 2001* SC 2001, c 41, s 83.01(b)(ii)(E).

likely to endanger human life'.[89] The South African definition states that the act must be is 'designed or calculated to cause serious interference with or serious disruption of an essential service, facility or system'.[90]

While the possible differences between 'designed, 'calculated' and 'intended' are acknowledged,[91] each of the definitions in these comparable domestic jurisdictions includes an express requirement that the offender in some way *means* to engage in the prohibited conduct or cause a particular result.[92] Out of the above provisions, Canada appears to set the highest requirement, in that the offender must *intend* to and actually *cause* the relevant interference. In the UK, New Zealand and South Africa, it appears that the system does not have to *actually* be interfered with,[93] although the offender must *intend* to cause such interference. This is one advantage of the Australian provision over three of its counterparts: it does require *actual* interference with an electronic system and not merely an intention to interfere. Nonetheless, section 100.1(2)(f) of the Australian *Code*, in making no reference to fault,[94] is the only one of these five definitions that could include offenders who are reckless as to whether their acts are likely to disrupt or destroy electronic systems.

While the ALRC in its report on sedition offences noted that recklessness is quite close to the level required by intention,[95] it nonetheless recommended that the word 'intentionally' be inserted into section 80.2 in order to put the fault element for that offence 'beyond doubt'.[96] It noted that this was already an express requirement of the offences of: delivering, placing, discharging or detonating an explosive or lethal device;[97] directing the activities of a terrorist organisation;[98] being a member of a terrorist organisation;[99] recruiting a person to join a terrorist organisation;[100] and providing training for terrorism.[101] It also

89 *Terrorism Suppression Act 2002* (NZ) ss 5(2), (3)(d).

90 *Protection of Constitutional Democracy Against Terrorist and Related Activities Act 2004* (South Africa) s 1(1)(xxv)(a)(vii).

91 See Kent Roach, 'A Comparison of South African and Canadian Anti-Terrorism Legislation' (2005) 18 *South African Journal of Criminal Justice* 127, 135, which discusses the difference between the South African 'designed or calculated' and the Canadian 'intentionally'. Roach believes that '"designed or calculated" should be interpreted as a subjective form of fault … Indeed, "designed or calculated" could be interpreted to refer to *dolus directus*, the highest form of fault in South African criminal law' implying there is little, if any, difference between the two requirements.

92 This is separate to and distinct from the 'intention' required by the various political protest exceptions, which, as discussed above, only require a low burden of proof to overcome.

93 See George Syrota, 'The Definition of "Terrorist Act" in Part 5.3 of the Commonwealth Criminal Code' (2007) *University of Western Australia Law Review* 307, 341, comparing the Australian and UK definitions and concluding that the Australian definition is narrower because the offender must actually cause interference with the system.

94 See above Part II(A)(2).

95 See ALRC, *Fighting Words*, above n 36, 177 [8.42]: '[i]n federal criminal law, recklessness is much closer to intentionality, requiring that the person be aware of a substantial risk and circumstances that make it unjustifiable to take the risk and nevertheless proceed with the conduct.'

96 Ibid 180–1, 223 (Recommendation 10–2(a)).

97 See *Criminal Code Act 1995* (Cth) s 72.3(1).

98 See *Criminal Code Act 1995* (Cth) s 102.2(1).

99 See *Criminal Code Act 1995* (Cth) s 102.3(1).

100 See *Criminal Code Act 1995* (Cth) s 102.4(1).

emphasised the importance of clarifying the intention requirement in order to promote community understanding of the law, and to avoid any chilling effect on legitimate forms of political expression where protestors become concerned that their actions may unintentionally extend into the realm of serious criminal activity.[102]

It is not entirely clear why an express intention requirement is absent from the Australian definition. The ALRC's recommendations, the serious nature of the penalties involved and the inconsistency of the Australian provision with other domestic definitions, all make a persuasive case for including an express intention requirement in the Australian definition of a terrorist act against an electronic system.

3 *Revised Section 100.1(2)(f)*

By including a serious economic harm requirement and an express fault element, a revised section 100.1(2)(f) prohibiting an electronic act of terrorism might look like the following:

> (2) Action falls within this subs if it intends to:[103]
>
> …
>
> (f) seriously interfere with, seriously disrupt, or destroy, an electronic system including, but not limited to:
>
> (i) an information system; or
>
> (ii) a telecommunications system; or
>
> (iii) a financial system; or
>
> (iv) a system used for the delivery of essential government services; or
>
> (v) a system used for, or by, an essential public utility; or
>
> (vi) a system used for, or by a transport system
>
> and thereby causes any major economic loss or extensive destabilisation of an economic system or a substantial devastation of the national economy of a country.[104]

Another possible amendment to restrict the application of section 100.1(2)(f) would be to include a requirement that the offender disrupt an 'essential' service, which would be consistent with Denning's widely cited definition of cyber-

---

101 See *Criminal Code Act 1995* (Cth) s 102.5(1).

102 ALRC, *Fighting Words*, above n 36, 180 [8.55].

103 If the words 'intends to' were inserted in the first limb of sub-s (2) in this way, this would mean the express intention requirement would apply to all of the possible listed harms of a terrorist act and not merely those against electronic systems. Although a comprehensive discussion of these other limbs is outside the scope of this paper, this wording is intentional, as it would similarly comply with the analysis in Part III(B)(2).

104 The final words are borrowed from the South African definition of 'terrorist activity': *Protection of Constitutional Democracy Against Terrorist and Related Activities Act 2004* (South Africa) s 1(1)(xxv)(a)(vii). In that Act, the economic harm requirement is one of the independent possible harms in the definition of 'terrorist activity' and is not tied to its infrastructure provision in section 1(1)(xxv)(a)(vi) (broadly comparable to section 100.1(2)(f) of the *Code*). If these two elements were tied together, however, the definition of a terrorist act against an electronic system in section 100.1(2)(f) of the *Code* would be broadly consistent with the definitions of terrorism and cyber-terrorism offered above.

terrorism. It would also be broadly consistent with the *Council of Europe Convention*, which contemplates destabilisation of the 'fundamental' structures of a country. It is a requirement of both the Canadian and South African definitions[105] and would be a welcome improvement to a provision that could theoretically be applied to acts against nonessential websites and email systems. Alternatively, a lower standard of this requirement could be achieved by removing the words 'an electronic system including, but not limited to'. This would confine the application of section 100.1(2)(f) to only those electronic systems listed in subsections (i)–(vi) and reduce the risk that cyber-attacks against parliamentary websites and inboxes will be prosecuted as terrorist acts where these do not have some wider effect on critical infrastructure.

In addition to the major economic harm requirement, section 100.1(2)(f) could also be amended to include a major environmental harm requirement, such that an action would constitute a terrorist act where it causes *either* major economic loss *or* major environmental damage. This may not be strictly necessary, as major environmental damage would be likely to result in major economic loss in most cases, but it could focus the provision more appropriately on cyber-attacks specifically designed to cause harm to the Australian environment (for example, if an offender attempted to contaminate the water supply by launching a cyber-attack on a local government's sewage control system).[106] This would remove the possibility that a serious cyber-attack could escape liability because it only caused environmental harm.

In one combination or another, these amendments would raise the bar for prosecuting acts of electronic terrorism in Australia. They would ensure that the anti-terrorism legislation could only be used to prosecute those cyber-attacks deserving the label of cyber-terrorism. This paper has most strongly recommended amending the provision to include a serious economic harm requirement and an express fault element, because these changes would bring the provision in line with definitions of terrorism at international law and in comparable domestic jurisdictions. The precise standard that should be required, however, is still open for debate. Parliament might, for example, decide that acts of cyber-terrorism should only include attacks against *essential* electronic systems; or it might decide to conform to the New Zealand definition, which requires that an attack against infrastructure also be likely to endanger human life. It might consider the higher standard of 'intending' to cause major economic or environmental harm. Whatever form this debate might assume, any dialogue on raising the standard required of this provision would be beneficial, not only to

105 See *Anti-Terrorism Act 2001* SC 2001 c 41, s 83.01(b)(ii)(E); *Protection of Constitutional Democracy Against Terrorist and Related Activities Act 2004* (South Africa) s 1(1)(xxv)(a)(vii).

106 See, eg, *R v Boden* [2002] QCA 164 (10 May 2002), in which a disgruntled engineer interfered remotely with the Maroochy Shire Council's sewage control system and released raw sewage into the local water supply. In that case, the attack was not motivated by a political cause and therefore could not be prosecuted as a terrorist act. However, if the attack *had* been motivated by a political cause (and had satisfied the other requirements of a terrorist act), it is possible that it would escape liability under the first proposed amendment if it had only caused environmental, and not economic, damage.

avoid prosecuting undeserving offenders, but also to avoid any chilling effect on the freedom of online political expression. The common goal of such a dialogue should be to ensure that serious acts of cyber-terrorism are appropriately criminalised, whilst acts of hacktivism – at a minimum, those that do not involve serious additional consequences – are securely and properly left in the domain of less serious computer offences.[107]

One might argue that these amendments are unnecessary, because the political protest exception is designed to prevent the prosecution of acts that are not intended to create a 'serious risk to the safety of a section of the public', and that only those acts deserving the cyber-terrorist label will fall foul of section 100.1(3). Without extensive judicial consideration to rely upon, it is indeed possible that the political protest exception will have a broader effect in the future than Part III(A) suggests. If that is the case, then there would be no harm in including these additional requirements in order to put that question beyond doubt, and in order to avoid any potential chilling effect on the freedom of online political expression. Considering that a person who interferes with the normal operation of a carriage service *without* the intent to commit a serious offence[108] may only receive a maximum of two years rather than life imprisonment, it would indeed seem wise, as Wong has argued, to ensure 'that any laws drafted or amended to deal with these activities are enacted with a clear understanding as to the distinctions between them.'[109]

As Deputy Assistant Attorney-General John Malcolm testified before the US Senate Judiciary Subcommittee on Terrorism, Technology and Homeland Security in 2004, '"hacktivists" who deface web sites in order to convey a political message will rarely qualify as cyberterrorists.'[110] In the Australian context, as the *Code* currently defines a terrorist act against an electronic system – at a standard far below comparable international and domestic definitions – such a claim cannot stand.

III CONCLUSIONS

The prosecution of cyber-attacks as terrorist acts is an uncertain area of Australian law, but one that will assume increasing significance in the age of digital crime. To date, little judicial or academic attention has been given to the precise application of section 100.1(2)(f) of the *Code*, and the application of the political protest exception in relation to the phenomenon of hacktivism.

---

107 See especially *Criminal Code Act 1995* (Cth) div 477; *Crimes Act 1900* (NSW) pt 6, for a range of offences.

108 See *Criminal Code Act 1995* (Cth) s 474.6(5).

109 Mary W S Wong, 'Terrorism and Technology: Policy Challenges and Current Responses' in Victor V Ramraj, Michael Hor and Kent Roach (eds), above n 72, 199, 207.

110 John Malcolm, 'Virtual Threat, Real Terror: Cyberterrorism in the 21st Century' (2004) <http://www.globalsecurity.org/security/library/congress/2004_h/040224-malcolm.htm>, cited in ibid at n 28 of that text.

While Operation Titstorm may appear to be a gimmicky test case for these issues, it is a useful factual example that teases out some of the problems with applying the current definition of a terrorist act to politically motivated cyber-attacks. It shows that the threat of cyber-attacks does not simply come from Islamic terrorists bent on destroying Australia's economy and infrastructure; it also comes from hacktivists who, while determined to achieve a particular political outcome, are really in the business of expensive mischief rather than the destruction of civilian life. It also reveals the potential breadth of section 100.1(2)(f), which could theoretically be applied to acts of hacktivism against nonessential websites and email systems.

Because of the important distinction between acts of hacktivism and acts of terrorism, it is not sufficient to assume that the problem of cyber-terrorism is covered by section 100.1(2)(f) without looking more closely at whether it also criminalises less serious forms of cyber-attack. While there may be some similarities between hacktivism and cyber-terrorism, there remains a fundamental conceptual difference between the two, and sufficient safeguards should be put in place to maintain this distinction in the Australian definition of a terrorist act.

It is likely that Operation Titstorm, or another similar cyber-attack, would satisfy the positive requirements of a terrorist act in section 100.1 of the *Code*. In other cases, the prosecution will only need to overcome a low harm requirement in order to prove that the political protest exception in section 100.1(3) does not apply. This means that a politically motivated cyber-attack may be prosecuted as a terrorist act where it merely intends to influence a government by intimidation, seriously interferes with an electronic system, and intends to create a serious risk to the safety of a section of the public. While acts that create a 'serious risk to the safety of a section of the public' will necessarily include those deserving the cyber-terrorist label, the uncertain scope of the political protest exception creates a risk that less serious cyber-attacks in the form of hacktivism will also qualify under the legislation. While this does not mean that acts of hacktivism will necessarily be prosecuted under the legislation, it nonetheless risks creating a chilling effect on legitimate forms of online political protest if hacktivists become concerned that their actions will be targeted under the provisions.

Section 100.1(2)(f) of the *Code* should be amended to include a serious economic harm requirement and an express fault element. This would mean that governments would be confined to prosecuting as terrorist acts those cyber-attacks that intend to seriously interfere with, disrupt or destroy electronic systems and cause serious harm to the Australian economy. It would also bring the Australian definition of a terrorist act in line with definitions of terrorism at international law and in comparable domestic jurisdictions, and with definitions of cyber-terrorism in computer science. Whether this standard is acceptable, and whatever precise standard the legislation should require, may well be open to debate for some time to come. The common goal of any dialogue, however, should be to ensure that acts of cyber-terrorism are appropriately criminalised, whilst acts of hacktivism – at a minimum, those that do not involve serious additional consequences – are securely and properly left in the domain of less serious computer offences.

While acts of hacktivism may cause great nuisance, inconvenience and political embarrassment, we need to ensure that an appropriate line is drawn between offenders that are reckless as to whether their cyber-attacks will disrupt or destroy nonessential electronic systems and those that are intended to have severe additional consequences for the Australian government and its civilian population. Currently, the definition of an electronic terrorist act in section 100.1(2)(f) of the *Code* fails to sufficiently address this distinction.