1. Introduction

Soon after 9/11, domestic parliaments engaged in a frenzy of lawmaking to counter an unprecedented, amorphous, transnational terrorist threat. Nearly 10 years have passed since this (frequently controversial) legislation was hastily enacted, and there is no reason to suspect that governments will take it off the books any time in the foreseeable future. While these laws have certainly attracted a wealth of academic literature, one issue that is often overlooked by commentators is how this legislation — designed primarily for large-scale acts of Islamic terrorism, which intend to cause death and serious bodily injury within civilian populations — will apply to new threats such as biological, economic, environmental and ‘cyber’ terrorism. While most people would recognise an act of Islamic suicide terrorism if they saw one, these other forms are largely speculative extensions of historical ideas about terrorism, and raise a number of unanswered questions about how to appropriately define terrorist acts, both in political discourse and in criminal legislation: Does an attack have to kill or injure real people to qualify as an act of terrorism? Can an act of terrorism cause pure economic loss? Can an act of terrorism be directed at websites and email systems? Must an act of terrorism create a shocking public spectacle, or may it also cause protracted damage behind the scenes, in the depths of government financial and military servers?

This article cannot answer all of these questions, but it does provide a framework for future debate by providing an overview and critique of the legislation that would be used to prosecute cyber-attacks as acts of terrorism in five western democracies. It focuses on four Commonwealth democracies — Australia, the United Kingdom, Canada and New Zealand — because each of these jurisdictions has enacted very similar definitions of terrorism, including specific provisions relating to attacks against electronic systems and other infrastructure. It then contrasts these Commonwealth

---

1 A cyber-attack may take a number of forms, including denial-of-service attacks, codes, worms, malicious software ('malware'), Trojan horses, or any other electronic attempt to undermine a computer system. This article focuses on the point at which such attacks will qualify as acts of terrorism under the federal (national) anti-terror legislation of each domestic jurisdiction. The Commonwealth legislation does not distinguish between different techniques used to launch cyber-attacks, so long as the attack satisfies the more general harm and fault requirements of a terrorist act. However, these jurisdictions do distinguish between cyber-attacks directed against 'electronic systems', 'services', 'facilities', 'systems' and 'infrastructure facilities': see discussion in Pt II below. The US legislation specifies that an attack involve the 'transmission of a program, information, code, or command': see 18 USC 1030(a)(5)(A)(i) and discussion in Pt III.

While the US post-9/11 response is generally considered to be synonymous with the terms ‘draconian’ and ‘exceptionalist’ – if not ‘unlawful’ – these two pieces of legislation in fact reveal a measured, informed approach to criminalising acts of cyber-terrorism. The US legislation finely calibrates its penalties according to the level of harm caused by cyber-attacks, and reserves the maximum penalty for cyber-attacks that cause or attempt to cause death. By contrast, the four Commonwealth definitions are blunt instruments that set extraordinarily low harm thresholds and maximum penalties of life imprisonment for all acts of terrorism directed at electronic systems and other infrastructure.

### 2. Attacks against electronic systems and infrastructure facilities in Commonwealth anti-terror laws

This section provides an overview and critique of the legislation that would be used to prosecute cyber-attacks as terrorist acts in four Commonwealth democracies: Australia, the United Kingdom, Canada and New Zealand. It provides some context surrounding the enactment of the legislation, and compares and contrasts the requirements for an act to qualify as an act of cyber-terrorism in each jurisdiction. All four of the Commonwealth definitions provide extraordinarily low harm requirements for acts of terrorism directed against electronic systems and other infrastructure. Only Canada requires that the targeted infrastructure be ‘essential’ to the country, and only New Zealand requires that the attack be ‘likely to endanger human life’, yet all attract a maximum penalty of life imprisonment.

#### 2.1. Australia

Australia’s definition of terrorism was inserted into s 100.1 of the federal Criminal Code Act 1995 (Cth) (‘Australian Criminal Code’) by the Security Legislation Amendment (Terrorism) Act 2002 (Cth) (‘SLAT Act’). The SLAT Act was the main piece of legislation in a package of five government bills which formed Australia’s main legislative response to the events of September 11. As amended by the SLAT Act, the Australian Criminal Code now provides a maximum penalty of life imprisonment for ‘terrorist acts’ committed in any jurisdiction, which are defined in the following terms:

- a terrorist act means 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

Subsection (2) lists the possible harm requirements of a terrorist act. While this list includes a number of other possible harms, a cyber-attack would most likely fall within para (2)(f), which specifically prohibits acts of terrorism against electronic systems:

- (2) Action falls within this subsection 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

While no prosecutions have been sought under s 100.1(2)(f) to date, the wording of the provision makes clear that it extends to attacks that seriously interfere with or disrupt any ‘electronic system’, including nonessential forms of infrastructure.

---

2 Of course, other less serious computer offences exist in each domestic jurisdiction, and the provisions below are also broad enough to include physical attacks to electronic systems and other infrastructure. However, this paper addresses the issue of ‘cyber-terrorism’ in the strictest legal sense, as these are the only federal (national) offences of ‘terrorist acts’ in each jurisdiction. Other uses of the internet by terrorists (recruitment, training, communication) may be referred to as ‘cyber-terrorism’ in a broader sense, and may attract liability under one or more ancillary offences: see Clive Walker, ‘Cyber-Terrorism: Legal Principle and Law in the UK’ (2005–2006) 110 Penn State Law Review 625, 627–628, 633–635 for an example of this broader approach, and a discussion of the merits of difference approaches to defining cyber-terrorism. For a selection of other domestic computer offences that do not amount to computer ‘terrorism’, see Criminal Code Act 1995 (Cth) div 477 (Aus); Computer Misuse Act 1990 (UK) c 18; Criminal Code, RSC 1985, c 46, ss 341.1–341.2 (Can); Crimes Act 1961 (NZ), ss 248–254.

3 The other four pieces of legislation enacted under the SLAT Package were the Suppression of the Financing of Terrorism Act 2002 (Cth), the Criminal Code Amendment (Suppression of Terrorist Bombings) Act 2002 (Cth), the Border Security Legislation Amendment Act 2002 (Cth), and the Telecommunications Intercept Legislation Amendment Act 2002 (Cth).


5 See Criminal Code Act 1995 (Cth), s 101.1(2), which applies Category D (extended geographical) jurisdiction (s 15.4) to the offence of committing a terrorist act.

6 The other possible harms listed in sub-s (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.
The list of enumerated harms in paras (i)-(vi) does nothing to limit this broad potential scope, precisely because the provision is ‘not limited to’ those systems. Subsection (3) does provide an exception for acts of political protest that only intend to cause property damage, although the scope of this exception remains uncertain, and does not apply to acts that satisfy the relatively low threshold of intending to ‘create a serious risk to the … safety of … a section of the public’.7

In a previous article, the author has argued that s 100.1(2)(f) is broad enough to apply politically motivated denial-of-service attacks8 against nonessential websites and email systems which do not deserve the label of ‘cyber-terrorism’.9 This issue was raised in debates in the Australian Senate before the legislation was passed.10 A recent Australian example of such an attack was ‘Operation Titstorm’, in which a group of ‘hacktivists’11 calling themselves ‘Anonymous’ launched a denial-of-service attack against the Australian Federal Parliament House website in order to protest the Rudd Labor Government’s plans to install a mandatory internet filter.12

While the Australian government has not, and most likely will not, prosecute relatively minor cyber-attacks such as Operation Titstorm as terrorist acts, this does not excuse the government for drafting the legislation so broadly as to encompass cyber-attacks that interfere with nonessential infrastructure without causing, or intending to cause, any additional harm. Indeed, the seriousness of this problem was recently brought to light when one of the members of Anonymous pleaded guilty to the lesser charge of inciting unauthorised impairment of electronic communications in Newcastle Local Court. In that case, the presiding magistrate stated that ‘[i]t is a serious offence because of it being able to amount to computer terrorism’.13

Since Operation Titstorm in February 2010, the Anonymous group has also launched Operation Payback: a barrage of transnational denial-of-service attacks against the websites of anti-piracy and intellectual property organisations in Australia, Spain, Portugal, the United Kingdom, and the United States.14 Most recently, Anonymous has also launched denial-of-service attacks against Paypal, Mastercard and Visa to protest against the companies’ refusal to process donations to the infamous WikiLeaks website.15 Of course, the magistrate’s prognostications are not determinative of the breadth of the federal legislation, and one would hope that the Australian government would not pursue these relatively minor denial-of-service attacks as acts of terrorism. Nonetheless, these growing international issues reveal the extraordinary breadth of the Australian anti-terror legislation, which could theoretically apply a maximum penalty of life imprisonment to cyber-attacks against nonessential infrastructure in Australia or any foreign country.

2.2. United Kingdom

The United Kingdom definition of terrorism is contained in s 1 of the Terrorism Act 2000 (UK) c 11 (TA2000). Although the United Kingdom government enacted a range of post-9/11 measures under the Anti-Terrorism, Crime and Security Act 2001 (UK) c 24, it left this earlier definition of terrorism unchanged. As it was in place before 9/11, the UK definition in many ways provided a template for the other Commonwealth jurisdictions,16 which were required to criminalise acts of terrorism under United Nations Security Council Resolution 1373.17 Not surprisingly, then, it displays remarkable similarity to the Australian definition:

(1) In this Act ‘terrorism’ means the use or threat of action where —
   (a) the action falls within subsection (2),

8 A denial-of-service attack involves a number of individuals (or a controlled ‘botnet’) making a significant number of simultaneous requests to a website or email server. The server becomes overloaded with these simultaneous requests for information, and slows down to the point where its content is effectively inaccessible. For a more detailed explanation of denial-of-service attacks, see United States Computer Emergency Readiness Team (CERT), Understanding Denial-of-Service Attacks (4 November 2009) US CERT, available at http://www.us-cert.gov/cas/tips/ST04-015.html; Felix Lau et al., Distributed Denial of Service Attacks (28 February 2001), available at http://www.eecs.berkeley.edu/~jlijia/papers/smco00.edited.pdf.
9 See Hardy, above no. 7, 485–488.
11 A portmanteau of ‘hacking’ and ‘activism’.
15 See ‘European Amazon websites down after attack by WikiLeaks supporters’, The Australian (Sydney), 13 December 2010.
17 SC Res 1373, UN SCOR, 55th sess, 4385th mtg, UN Doc S/RES/1373 (28 September 2001). Resolution 1373 provided no definition of terrorism for states to implement in their domestic legislation.
(b) the use or threat is designed to influence the government or an international governmental organisation or to intimidate the public or a section of the public, and
(c) the use or threat is made for the purpose of advancing a political, religious, racial or ideological cause.

As in the Australian definition, sub-s (2) lists the possible harm requirements of a terrorist act.\(^{18}\) If a cyber-attack were to be prosecuted as a terrorist act in the United Kingdom, it would likely fall under sub-s (2)(e), which similarly criminalises acts of terrorism against electronic systems:

(2) Action falls within this subsection if it –

... (e) is designed seriously to interfere with or seriously to disrupt an electronic system

This UK provision displays some similarities to the Australian provision, but generally sets a lower burden of proof. Like the Australian Criminal Code, the UK legislation provides a maximum penalty of life imprisonment\(^{19}\) for politically motivated action that is designed to influence any government\(^{20}\) by interfering with any electronic system in any jurisdiction,\(^{21}\) including nonessential infrastructure. Unlike the Australian definition, however, the UK definition increases the range of possible targets to include ‘international governmental organisations’.\(^{22}\) This is broader than the Australian provision, which only criminalises acts of terrorism directed at governments and civilian populations. It would include politically motivated cyber-attacks directed at bodies such as NATO, the World Bank and the United Nations.

Unlike the Australian definition, the UK definition also requires that the offender intend to but not actually interfere with the system. This is a higher standard than the Australian provision in terms of the fault element of the offence, but a lower standard in terms of the physical element. While the Australian provision could theoretically apply to offenders who are reckless as to whether their actions are likely to seriously disrupt or destroy an electronic system,\(^{23}\) the UK provi-
d requires that the offenders actually intend such interference. On the other hand, the UK definition could theoretically apply to offenders who intended to launch a serious denial-of-service attack against a government but were not successful, whereas the Australian provision would require that the offenders actually interfered with the system.\(^{24}\)

The UK legislation also sets a lower standard of intimidation than the Australian legislation, by requiring that an act merely intend to ‘influence’ a government or international organisation (as opposed to influencing a government ‘by intimidation’). It also does not include a political protest exception comparable to the Australian’s 100.1(3). These factors tend to suggest that a politically motivated denial-of-service attack such as Operation Titstorm would be even more likely to fall within the UK legislation.

When sub-s (2)(e) was introduced in the UK Parliament, there was much emphasis on the potential for great harm to be caused by acts of ‘cyber-terrorism’. In the House of Lords, for example, Lord Cope of Berkeley emphasised that great damage could be caused to the public by offenders who use the techniques of computer hacking to destroy electronic systems:

The amendment...extends the definition to cover what is known in the jargon as cyber-terrorism – the destruction of electronic systems. That is very important, because great damage can be caused to public life and the public can be held to ransom by computer hacking of one kind or another.\(^{25}\)

Similarly, Lord Carlile in his independent review of the UK definition of terrorism recommended that sub-s (2)(e) be retained in order to cover the broad range of possible consequences stemming from a cyber-attack:

Section 1(2)(e) deals with the design seriously to interfere with or seriously to disrupt an electronic system. This has the potential to include internet service providers, financial exchanges, computer systems, controls of national power and water, etc. The huge damage to the economy of the nation, and the potential for injury as a result, are self-evident. This category too should be included in the definition. I have concluded that the provision remains justified.\(^{26}\)

 Most recently, the United Kingdom government has announced in its National Security Strategy that cyber-attacks by state and non-state actors are one of four, Tier-1, ‘highest priority risks’ to national security.\(^{27}\) While all of these comments tend to support the inclusion of a ‘cyber-terrorism’ provision in domestic legislation, they also reveal the extraordinary overbreadth of the current UK definition.

---

\(^{18}\) Similar to Australia, the other possible harms listed in s 1(2) are:

(a) involves serious violence to a person;
(b) involves serious damage to property;
(c) endangers a person’s life, other than that of the person committing the action;
(d) creates a serious risk to the health or safety of the public or a section of the public.

\(^{19}\) See Terrorism Act 2000 (UK) c 11, s 56 (offence of directing activities of an organisation which is concerned with the commission of acts of terrorism).

\(^{20}\) Terrorism Act 2000 (UK) c 11, s 14(4); “the government” means the government of the United Kingdom, of a Part of the United Kingdom or of a country other than the United Kingdom’. For discussion see R v F [2007] EWCA Crim 243.

\(^{21}\) See Terrorism Act 2000 (UK) c 11, ss 63A-63D.

\(^{22}\) This was added by s 34 of the Terrorism Act 2006 (UK) c 11.

\(^{23}\) See Hardy, above no. 7, 484.

\(^{24}\) However, both definitions also include the ‘threat’ of action. In such a case, there would be no need to show under the Australian legislation that an offender actually followed through with the attack.


\(^{26}\) Lord Carlile of Berriew QC, The Definition of Terrorism: A Report by Lord Carlile of Berriew QC, Independent Reviewer of Terrorism Legislation (Cm 7052, March 2007) 40 [71].

\(^{27}\) See United Kingdom Government, A Strong Britain in an Age of Uncertainty: The National Security Strategy (October 2010) [0. 18], [3.27]–[3.31].
Subsection (2)(e) does not merely criminalise cyber-attacks that destroy electronic systems, interfere with national power and water supplies, cause major economic harm, physically injure civilians, or create a national public emergency, as the UK government (understandably) wants to deter and prosecute; it also extends to offenders who merely intend to seriously interfere with or disrupt nonessential electronic systems.

Of course, cyber-attacks in both Australia and the United Kingdom would need to satisfy other requirements to qualify as terrorist acts (namely, that they be politically motivated and intend to influence a government or intimidate a civilian population). Nonetheless, in both Australia and the UK, seriously interfering with or disrupting any electronic system in any country is one of several independent harm requirements of a terrorist act. A cyber-attack in either jurisdiction need not cause any greater harm to a government or civilian population in order to qualify as an act of terrorism.

2.3. Canada

The Canadian definition of terrorism is contained within s 83.01 of the Canadian Criminal Code as amended by the Anti-Terrorism Act 2001 (‘ATA’). It defines ‘terrorist activity’ as either an act against a number of specified terrorism conventions, or as:

(b) an act or omission, in or outside Canada,
   (i) that is committed
      (A) in whole or in part for a political, religious or ideological purpose, objective or cause, and
      (B) in whole or in part with the intention of intimidating the public, or a segment of the public, with regard to its security, including its economic security, or compelling a person, a government or a domestic or an international organization to do or to refrain from doing any act, whether the public or the person, government or organization is inside or outside Canada, and
   (ii) that intentionally
      (A) causes death or serious bodily harm to a person by the use of violence,
      (B) endangers a person’s life,
      (C) causes a serious risk to the health or safety of the public or any segment of the public,
      ... 
   (E) causes serious interference with or serious disruption of an essential service, facility or system, whether public or private, other than as a result of advocacy, protest, dissent or stoppage of work that is not intended to result in the conduct of harm referred to in any of clauses (A) to (C).

The Canadian legislation provides a maximum penalty of life imprisonment for anyone who commits an indictable offence for the benefit of, at the direction of, or in association with a group that engages in terrorist activity. Under sub-s (b)(ii)(E), this would include cyber-attacks in Canada or any foreign country that intentionally cause serious interference with or disruption to essential services, facilities or systems, whether publicly or privately owned. In these respects, the Canadian definition is an improvement on the Australian and UK definitions: firstly, because it requires that an attack both intend to and actually interfere with infrastructure; and secondly, because it would not extend to cyber-attacks against nonessential electronic systems, such as websites and email servers. Like the Australian definition, sub-s (b)(ii)(E) also includes a political protest exception, which requires protestors to intend to cause, at a minimum, a ‘serious risk to the ... safety of ... any segment of the public’.

On the other hand, however, the Canadian definition includes a broader range of possible infrastructure targets than both the UK and Australian definitions, as it would extend to politically motivated cyber-attacks against ‘services’ and ‘facilities’, and not merely ‘systems’. It also expands the intimidation requirement to include acts designed to compel ‘persons’ and ‘domestic’ organisations to act in a particular way. This could include cyber-attacks designed to compel individual Members of Parliament to withdraw proposals, or those designed to change the anti-piracy policies of domestic copyright organisations (such as those targeted under Operation Payback).

When the ATA was being debated in the Canadian Parliament, there was a greater focus on sub-s (b)(ii)(e) applying to the disruption of services and facilities in the ‘real’ – as opposed to ‘cyber’ – world. This contrasts with the debates in Australia and the UK, which focused more heavily on sub-s (2)(f) and (2)(e) applying to the threat of cyber-attacks. It may also explain why Canada has not made explicit reference to ‘electronic’ systems in their definition. In the Canadian House of Commons, for example, Member for Argenteui-Papineau-Mirabel Mario Laframboise asked: ‘could some nurses who decide to defy regulations or legislation for the purpose of making union demands be charged with terrorist activities, since they are causing interference with or disruption of essential services? This is what the bill before us implies.’ Member for Burnaby-Douglas Svend Robinson also argued that the provision was wide enough to include legitimate acts of political dissent, such as those that put Nelson Mandela in power:

"The definition of terrorist activity I believe goes too far... It talks about causing serious interference with or serious disruption of an essential service, facility or system, whether public or private, other than as a result of lawful advocacy. Consider for a moment the possible risks of this and what this could be applied to. There are many examples of this, some historic, some current... The African National... "

---

28 RSC 1985, c 46.
29 SC 2001, c 41.
30 Criminal Code, RSC 1985, c 46, s 83.01(a).
31 The remaining harm requirement in s 83.01(b)(ii) is: ‘causes substantial property damage, whether to public or private property, if causing such damage is likely to result in the conduct or harm referred to in any of clauses (A) to (C)’. 32 Criminal Code, RSC 1985, c 46, s 83.2. See also ss 83.21 and 83.22 (penalty of life imprisonment for instructing a person to carry out activity for a terrorist group).
Congress in its fight against the brutal and racist apartheid regime in South Africa would clearly have been caught by this legislation, as would any Canadian who supported the African National Congress in its fight against apartheid.34

These arguments are similar to those made by the Greens and Democrats in the Australian Senate when debating the political protest exception in s 100.1(3).35 Their focus is on protests in the ‘real’ rather than ‘cyber’ world, but their logic could equally apply to cyber-protests such as Operation Tit-storm, Operation Payback, and the recent cyber-attacks launched by Anonymous during the WikiLeaks saga, which were designed to intimidate governments and organisations into changing their policies on censorship, piracy, and confidentiality issues. They suggest that, while the Canadian definition generally sets a higher standard than its Australian and UK counterparts, and while an effort has been made to exclude legitimate forms of political protest from the legislation, serious and unanswered questions still remain about the possible scope of Canada’s definition of terrorism if it were to be applied to cyber-attacks against infrastructure, including acts of political protest that use the techniques of hacking computer systems.

2.4. New Zealand

New Zealand’s definition of terrorism is contained in s 5 of the Terrorism Suppression Act 2002 (NZ) (‘TSA’). Insofar as it could apply to cyber-attacks against infrastructure, it provides a maximum penalty of life imprisonment for ‘terrorist acts’,36 which are defined as follows:

(1) An act is a terrorist act for the purposes of this Act if –
   (a) the act falls within subsection (2)

   ...

(2) An act falls within this subsection if it is intended to cause, in any 1 or more countries, 1 or more of the outcomes specified in subsection (3), and is carried out for the purpose of advancing an ideological, political, or religious cause, and with the following intention:
   (a) to induce terror in a civilian population
   (b) to unduly compel or to force a government or an international organisation to do or abstain from doing any act

Subsection (3) then lists the possible harm requirements of a terrorist act:

(3) The outcomes referred to in subsection (2) are –
   ...

(d) serious interference with, or serious disruption to, an infrastructure facility, if likely to endanger life

Subsection (5) provides an exception for acts of political protest similar to the Australian and Canadian definitions, although it does not strictly require a protestor to intend to create a serious risk to safety of a section of the public:

(5) To avoid doubt, the fact that a person engages in any protest, advocacy, or dissent, or engages in any strike, lockout, or other industrial action, is not, by itself, a sufficient basis for inferring that the person –
   (a) is carrying out an act for a purpose, or with an intention, specified in subsection (2); or
   (b) intends to cause an outcome specified in subsection (3).

Out of all four Commonwealth definitions, the New Zealand definition sets the highest standard for attacks against infrastructure by requiring that they also be ‘likely to endanger life’. This might include, for example, cyber-attacks that interfere with air traffic control systems, those that interfere with the valves and pressure settings in gas lines, those that interfere with safeguards in nuclear power stations, or those that alter patient information in hospital databases,37 but it would not ordinarily include cyber-attacks against websites, email systems, financial institutions, or telecommunications providers. Indeed, in being limited to ‘infrastructure facilities’, the New Zealand legislation would not likely extend to cyber-attacks against any such ‘services’ or ‘systems’. One downside, however, is that the infrastructure facility need not be ‘essential’ to the country, as is required by the Canadian definition. Like the other Commonwealth definitions, the New Zealand definition is also not limited to domestic cyber-attacks, and could extend to cyber-attacks against infrastructure facilities in any 1 or more countries.

Despite this relatively high standard, minority parties in the New Zealand Parliament were still highly critical of the potential scope of sub-s (3)(d). When the Counter-Terrorism Bill 2003 (NZ)38 was being debated, for example, Greens MP Keith Locke

34 Canada, Parliamentary Debates, House of Representatives, 16 October 2001, 2135.
35 See, e.g., Commonwealth, Parliamentary Debates, Senate, 24 June 2002, 2405–6 (Natasha Stott Despoja); 2481, 2486 (Bob Brown).
36 Terrorism Suppression Act 2002 (NZ) s 6A.
37 The remaining harm requirements in s 5(3) are:
   (a) the death of, or other serious bodily injury to, 1 or more persons (other than a person carrying out the act);
   (b) a serious risk to the health or safety of a population
   (c) destruction of, or serious damage to, property of great value or importance, or major economic loss, or major environmental damage, if likely to result in 1 or more outcomes specified in paragraphs (a), (b), and (d);
   (c) introduction or release of a disease-bearing organism, if likely to devastate the national economy of a country.
argued that the other limbs of the TSA’s definition were not enough to save sub-s (3)(d) from its extraordinary breadth:

[T]he definition of terrorism in the Terrorism Suppression Act is much too broad. It does not target only people who support those who use violence against and create terror amongst civilians; it also covers, within the very broad definition of terrorism in that Act, people who seriously disrupt an infrastructure facility in a way likely to endanger human life. One does not even need to intend to endanger human life to be covered under that definition. All that one needs to do is to fulfil two other criteria: first, to unduly compel a Government to do something – which many politicians are accused of – and, second, the motive has to be political, religious or ideological.  

The same argument could equally apply to the other three Commonwealth definitions above, which only require the low and uncertain thresholds of (1) intending to advance a political, religious or ideological cause, and (2) intending to intimidate a government or a section of the public, for an act to fall within the broad scope of the infrastructure provisions.

In 2007, when debating amendments to the TSA, Locke reiterated these earlier arguments, arguing that sub-s (3)(d) was broad enough to include legitimate acts of political protest, and should therefore include a requirement that an offender intend to endanger life:

As things stand, if this bill passes, those organising a hospital strike or a disruptive protest on the scale of the 1981 Springbok Tour demonstrations could be up for a life sentence for serious disruption of an infrastructure facility, in a way likely to endanger human life, even if they in no way intended to endanger human life.

These arguments display obvious similarities to those made against the ATA in the Canadian Parliament. While anti-apartheid rugby protests may appear to be an extreme example that would not be prosecuted under the legislation, the 1981 Springbok Tour certainly involved hostilities that were ‘likely to endanger life’, and which could easily spark fears of terrorism in today’s post-9/11 climate. Not only did thousands of protestors clash violently with police in the streets, but rugby supporters also pelted protestors with blocks of concrete and full bottles of beer, the grandstand at Rugby Park was burned down, and television cables were cut at a transmitter facility north of Auckland. Most frighteningly in a post-9/11 world, one protestor stole a Cessna aircraft, and then flew the plane at dangerously low altitudes over Eden Park during the third test in Auckland, dropping flour and smoke bombs on the field, at the players, and in the crowds.

We can, of course, look back today and say that the pilot did not intend anything so serious as a ‘terrorist act’; but when one watches the video from the third test42 – and hears the buzz of a low-flying plane drown out the sound of crowd and commentary, dropping unknown exploding objects on players and spectators – one gets a sense of the level of panic that would be caused by a similar act in today’s post-9/11 climate. Indeed, writing in 1990, Holcroft has looked back on that day, recalling that he did not see ‘terrorism’, but that he ‘certainly saw in action a fanaticism very close to the mentality that breeds it.45

Perhaps because of this political and historical background, and similar to the Canadian approach, opposition parties in New Zealand have been more concerned with protecting ‘real world’ protests from being criminalised under anti-terror legislation; but the legislation, and its counter-arguments, could equally apply to contemporary attacks and protests that use the techniques of hacking computer systems. While one might argue that extreme examples are not helpful in advancing debate on the issue, there is much strength to the Greens’ argument that a politically motivated act should not necessarily attract a maximum penalty of life imprisonment simply because it intends to intimidate a government or a section of the public and is ‘likely’ to endanger life.46 And if this higher New Zealand standard remains problematic, then it puts into sharp relief the extraordinary reach of the other three Commonwealth definitions. The next section compares these Commonwealth definitions with the more measured approach taken by the United States after 9/11, which does in fact reserve the most serious penalties for those acts of cyber-terrorism that attempt to cause death, as the New Zealand Greens would have preferred.

3. Cyber-terrorism in United States legislation

In contrast to the broad-brush approach of the Commonwealth anti-terror legislation, the United States post-9/11 response takes a more nuanced approach to criminalising acts

---

40 New Zealand, Parliamentary Debates, 21 October 2003, 9341.
43 See Holcroft, above no. 42, 58; New Zealand History Online, ‘Film: the third test – 1981 Springbok ‘Tour’, available at http://www.nzhistory.net.nz/media/video/the-third-test-auckland. These two reports differ on whether it was 1 or 2 protestors, and whether the plane was stolen or hired and then taken off course, but these discrepancies would not have changed the impact on those at the stadium at the time of the attack.
45 Holcroft, above no. 42, 60.
46 See also Alex Conte, above no. 39, 372, who has argued that sub-s (3)(d) should be ‘confined to conduct that is likely to cause death or serious bodily injury’.
of cyber-terrorism. The USA PATRIOT Act of 2001 and the Cyber Security Enhancement Act of 2002 finely calibrate the penalties for cyber-attacks against infrastructure according to the level of harm caused, and reserve the maximum penalty of life imprisonment for only those acts of cyber-terrorism that cause or attempt to cause death.

3.1 USA Patriot Act 2001 and Cyber Security Enhancement Act 2002

Passed only six weeks after the September 11 attacks, the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001 has certainly been the subject of much fear and criticism. Much of its pernicious scope stems from the definitions of ‘international’ and ‘domestic terrorism’ in Title 18 of the United States Code, the latter being added by §802 of the 2001 Act. Both definitions now read in tandem as follows:

(1) the term ‘international terrorism’ means activities that—
   (A) involve violent acts or acts dangerous to human life that are a violation of the criminal laws of the United States or of any State, or that would be a criminal violation if committed within the jurisdiction of the United States or of any State;
   (B) appear to be intended—
      (i) to intimidate or coerce a civilian population;
      (ii) to influence the policy of a government by intimidation or coercion; or
      (iii) to affect the conduct of a government by mass destruction, assassination, or kidnapping; and
   (C) occur primarily outside the territorial jurisdiction of the United States, or transcend national boundaries in terms of the means by which they are accomplished, the persons they appear intended to intimidate or coerce, or the locale in which their perpetrators operate or seek asylum

...the term ‘domestic terrorism’ means activities that—
   (A) involve acts dangerous to human life that are a violation of the criminal laws of the United States or of any State;
   (B) appear to be intended—
      (i) to intimidate or coerce a civilian population;
      (ii) to influence the policy of a government by intimidation or coercion; or
      (iii) to affect the conduct of a government by mass destruction, assassination, or kidnapping; and
   (C) occur primarily within the territorial jurisdiction of the United States.

These broad definitions of terrorism are strikingly similar to the Commonwealth definitions, although they do not enumerate specific harms, such as attacks against electronic systems. More importantly, however, they are unlike the Commonwealth definitions in that they do not provide a basis for prosecuting acts of terrorism in US courts. Instead, they were enacted for the ‘limited’ purpose of seeking court orders and search warrants against individuals suspected of engaging in terrorist activity. Section 219 of the Patriot Act, for example, gives Federal magistrates in any district the power to issue a nation-wide search warrant for individuals suspected of domestic or international terrorism.

While criticism of the Patriot Act on these and other grounds is understandable, the specific terrorism offences it implemented are more sensible and finely calibrated than those in comparable Commonwealth legislation. This is first made clear by §808 of the Patriot Act, which amends the federal crimes of terrorism in §2332b of Title 18. Section 2332b defines the crime of ‘acts of terrorism transcending national boundaries’ as conduct that occurs across national borders which results in a range of serious harm to persons and property. While this definition of transnational terrorism is still quite broad, and could include cyber-attacks directed against United States government property, §2332b(c) provides a finely calibrated scale of punishments according to the amount of harm that each act of terrorism causes. It only provides a maximum penalty of death or life imprisonment for those acts resulting in death to others, and a maximum penalty of life imprisonment for acts involving kidnapping.

All other acts of terrorism receive lesser maximum penalties: from 35 years for maiming, to 25 years for property damage, to 10 years for the threat of an attack.

More likely, however, an act of cyber-terrorism would fall under §1030 of Title 18, as amended by the ‘deterrence and prevention of cyber-terrorism’ provision in §814 of the Patriot Act. Section 1030 is defined as a ‘federal crime of terrorism’ under §2332b(g)(5) for the purposes of investigating authorities where such an act is ‘calculated to influence or affect the conduct of government by intimidation or coercion, or to retaliate against government conduct.’ Insofar as it is relevant to this definition of a ‘federal crime of terrorism’, §1030 criminalises conduct against protected computer systems as follows:

(a) Whoever—
   (1) having knowingly accessed a computer without authorization or exceeding authorized access, and by means of such conduct having obtained information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations [; or]

... §1030(A)(i) knowingly causes the transmission of a program, information, code, or command, and as a result of

---

48 18 USC 2331.
such conduct, intentionally causes damage without authorization, to a protected computer; [and]

(B) by conduct described in clause (i) ... caused (or, in the case of an attempted offense, would, if completed, have caused) —

... (ii) the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals;

(iii) physical injury to any person;

(iv) a threat to public health or safety; or

(v) damage affecting a computer system used by or for a government entity in furtherance of the administration of justice, national defense, or national security

shall be punished as provided in subsection (c) of this section

While the definition of 'federal crime of terrorism' is only relevant for the purposes of investigating authorities, sub-s (c) of §1030 provides a range of independent penalties for the federal crime of interfering with computer systems. As in §2332b, this range of penalties is finely calibrated according to the level of harm caused by each cyber-attack. Subsection (c) of §1030 provides this range of penalties for offences under sub-s (a)(i) and (5)(A)(i) as follows:

(c) The punishment for an offense under subsection (a) ... of this section is —

(1)(A) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(1) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and

(B) a fine under this title or imprisonment for not more than twenty years, or both, in the case of an offense under subsection (a)(1) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;

... (4)(A) except as provided in paragraph (5), a fine under this title, imprisonment for not more than 10 years, or both, in the case of an offense under subsection (a) (5)(A)(i), or an attempt to commit an offense punishable under that subsection;

... (C) except as provided in paragraph (5), a fine under this title, imprisonment for not more than 20 years, or both, in the case of an offense under subsection (a) (5)(A)(i) ... or an attempt to commit an offense punishable under [that] subsection, that occurs after a conviction for another offense under this section; and

(5)(A) if the offender knowingly or recklessly causes or attempts to cause serious bodily injury from conduct in violation of subsection (a)(5)(A)(i), a fine under this title or imprisonment for not more than 20 years, or both; and (B) if the offender knowingly or recklessly causes or attempts to cause death from conduct in violation of subsection (a)(5)(A)(i), a fine under this title or imprisonment for any term or years or for life, or both.

Subsection (5)(B) was added by the Cyber Security Enhancement Act of 2002, which was implemented under the better-known Homeland Security Act of 2002. It makes clear that only those offences under sub-s (a)(5)(A)(i) (that is, only those cyber-attacks that cause unauthorised damage to a protected computer by inserting code, a program or other information) which knowingly or recklessly cause or attempt to cause death will attract a maximum penalty of life imprisonment. Cyber-attacks under sub-s (a)(5)(A)(i) that cause or attempt to cause serious bodily injury will only attract a maximum penalty of 20 years imprisonment, and other breaches of sub-ss (a)(1) and (a)(5)(A)(i) will attract a maximum of either 10 or 20 years, depending on whether they follow another offence under §1030.

The US government has taken a similar approach to other terrorism offences introduced by the Patriot Act. The offences of destroying an energy facility and destroying national-defense materials, for example, are broad enough to cover both cyber and physical attacks against infrastructure, yet they only provide a maximum penalty of life imprisonment for attacks that result in death. By contrast, the above Commonwealth provisions are broad enough to encompass both cyber and physical attacks against infrastructure, yet none makes similar distinctions between acts causing death, and those causing lesser levels of harm. Instead, the Commonwealth terrorism offences are blunt instruments, providing a maximum penalty of life imprisonment for all politically motivated acts of intimidation (or even 'influence' in the UK) that interfere with electronic systems and infrastructure, regardless of an offender's intention to cause a greater level of harm, injury or death.

When the Homeland Security Act was being debated in Congress, the US government expressed similar fears to the United Kingdom of a devastating cyber-attack against infrastructure. Senator Hatch, for example, introduced the sub-s (5) (B) amendment by arguing that the threat of a devastating cyber-attack warranted introducing a maximum penalty of life imprisonment:

Terrorists and others who wish to harm our country recognize that cyber attacks on our vital computer and related technological systems can have a devastating impact on our country, our economy and the lives of our people ... Since September 11, there has been growing fear that a terrorist could launch a devastating cyber-attack, which could cripple our financial system, our critical infrastructures, our medical systems, and our entire way of life.

concern about the risk to our country of a serious cyber attack, particularly one against our infrastructure which could have devastating consequences.  

The Senator was concerned that the existing maximum penalty of 10 years was not sufficient to cover the potential level of harm covered by a devastating cyber-attack.  

While the US government faces similar fears of cyber-terrorism to the UK and other Commonwealth nations – and probably has even greater reason to enact sweeping, draconian terrorism offences in the wake of 9/11 – it has not allowed these fears to influence the breadth of its federal terrorism offences. And while the US government was keen to introduce a maximum penalty of life imprisonment for acts of cyber- and real-world terrorism against infrastructure, it was careful to restrict these maximum penalties to only the most serious acts of terrorism resulting in death, and carefully calibrate the penalties for attacks causing lesser levels of harm. By contrast, each of the above four Commonwealth nations have enacted sweeping terrorism provisions which provide maximum penalties of life imprisonment for any acts of terrorism directed at electronic systems and other infrastructure.

4. Conclusions

As we move further into the 21st century, questions about the boundaries between cyber-crime, cyber-warfare and cyber-terrorism are likely to be hotly debated, especially as the technology needed to launch electronic protests against governments and private organisations becomes more widely available. This paper has not attempted to decide these boundaries once and for all, but it has provided a foundation for future debate by providing an outline and critique of the current legislation in five western democracies that would be used to prosecute acts of cyber-terrorism. In this narrow legal sense, it has asked the question: at what point does an act of electronic interference become an act of cyberterrorism?  

In political discourse this question may be debated for some time to come, but the current answer in Commonwealth domestic anti-terror law is relatively clear: an act of cyber-terrorism is a cyber-attack that is (1) motivated by a political, religious or ideological cause, (2) designed to influence a person, government or international organisation by intimidation, and (3) seriously interferes with, disrupts or destroys a service, facility, or electronic system. As detailed above, each of the four Commonwealth jurisdictions makes its own particular additions and subtractions to this catch-all definition, but the essence of each legislative regime is the same: a cyber-attack need not cause death, serious bodily harm, or devastating economic damage to qualify as an act of terrorism, so long as it seriously interferes with some form of infrastructure. Only Canada requires that the infrastructure be ‘essential’ to the country, and only New Zealand requires that the interference be ‘likely to endanger life’. Each of the four Commonwealth jurisdictions – Australia, the UK, Canada and New Zealand – provides a maximum penalty of life imprisonment for politically motivated acts of intimidation that interfere with infrastructure, regardless of the particular level of harm caused by the attack. This does not mean that every cyber-attack that qualifies under the legislation will be prosecuted and attract the maximum penalty, but it does have serious implications for the level of discretion available to executive governments, and for the right to freedom of speech if online protestors become concerned that their actions will be targeted under criminal legislation.

For some, this answer may appear extraordinarily broad, and it may suggest that anti-terror legislation extends too far into the realm of legitimate online activity. For others who are more trusting of government, it may be a necessary evil so that domestic authorities have the power to ensure that no devastating act of cyber-terrorism goes unpunished. It is unlikely that these two positions will be reconciled any time soon, but one thing is clear: the Commonwealth anti-terror legislation takes a significantly broader brush to criminalising acts of cyber-terrorism than comparable legislation in the United States, despite similar fears in each jurisdiction about the possible risks of cyber-terrorism to national infrastructure.

As amended by the Patriot Act of 2001 and the Cyber Security Enhancement Act of 2002, the United States cyber-terrorism regime reveals a sensible, measured approach to criminalising acts of cyber-terrorism. An offence under §1030 of the United States Code is defined as a federal crime of terrorism for the purposes of investigating authorities, but will only attract a maximum penalty of life imprisonment if it causes or attempts to cause death. Similarly, attacks against energy facilities and national-defense materials will only attract the maximum penalty of life imprisonment where they result in death. By contrast, each of the four Commonwealth definitions provides a maximum penalty of life imprisonment for all politically motivated acts of electronic intimidation that seriously interfere with infrastructure. While debates about what should and should not be considered an act of cyber-terrorism will likely continue for some time, this discrepancy should encourage further debate about the appropriateness of definitions of cyber-terrorism in domestic legislation, especially in countries dedicated to upholding the rule of law and the right to freedom of online expression.

Keiran Hardy (k.a.hardy@unsw.edu.au) Research Assistant, Australian Research Council Laureate Fellowship on Anti-Terrorism Law, Gilbert + Tobin Centre of Public Law, Faculty of Law, University of New South Wales (Sydney, Australia).

The author would like to thank Alana Maurushat (Deputy Director, Cyberspace Law and Policy Centre, University of New South Wales).