Protecting Australian Cyberspace: Are our International Lawyers Ready?

STEPHEN TULLY*

Abstract

Cyberspace is an important element of Australia's critical national infrastructure. Recent policy developments within this field seek to maintain economic opportunity and protect national security. This article discusses four contemporary threats posed to the Australian military and civilian electronic information infrastructure: 'cyber war' conducted by hostile states, 'cyber conflicts' by foreign combatants, attacks committed by 'cyberterrorists' and the commission of 'cybercrimes'. This article reviews the existing international legal paradigms relevant to each and identifies the issues raised from a survey of the existing literature. It concludes that each paradigm is presently inadequate for addressing the nature of these threats and calls for further contributions from Australian government, military and international lawyers to articulate a distinctive national perspective on these questions.

I Introduction

The United States (US) Department of Defense has recently developed an offensive cyber war capability and a coordinated military-civilian strategy to defend against cyber attacks.[1] Cyber experts from the Centre for Strategic Counterterrorism Communications at the US State Department also routinely patrol social media including the internet and recently hacked Yemeni websites to replace al-Qaeda propaganda.[2] In Australia, the Director General of the Australian Security Intelligence Organisation ('ASIO') has predicted that cyber attacks against Australia will increase from both state and non-state actors, including terrorists who use the internet for recruitment and to support operational activities.[3] More than 200 cyber intrusions against the Department of Defence were investigated in 2009.[4] The Department of Foreign Affairs and Trade is also subjected to daily cyber attacks.[5] Australian engineers have since received training at the Idaho National Laboratory, which

* Legal Officer, Migration and Refugee Review Tribunals, to whom all views are personally attributable. Sincere thanks to the anonymous referees who provided very helpful comments on an earlier draft.

1 Trudy Rubin, 'It's Time to Get Serious about Cyber Attack Risk', *Sydney Morning Herald* (Sydney), 29 December 2010, 11.

2 'US Hacked Yemen al-Qaeda Sites: Clinton', *Sydney Morning Herald* (online), 24 May 2012 <http://news.smh.com.au/breaking-news-world/us-hacked-yemen-alqaeda-sites-clinton-20120524-1z6tg.html>.

3 David Irvine, Australian Security Intelligence Organisation, 'Director-General's Speech to The Sydney Institute' (Speech delivered at The Sydney Institute, 24 January 2012) <http://www.asio.gov.au/Publications/Public-Statements/2012/24-Jan-2012-Sydney-Institute.html>.

4 Senator John Faulkner, Department of Defence (Cth), 'Opening of the Cyber Security Operations Centre' (Press Statement, MIN1001155/10, 15 January 2010) <http://www.defence.gov.au/minister/FaulknerTranscripttpl.cfm?CurrentId=9885>.

5 Dylan Welch and Dan Oakes, 'Australia to Defend Itself in Cyber War', *Sydney Morning Herald* (Sydney), 3 June 2011, 1.

designed the Stuxnet worm used to sabotage an Iranian nuclear facility.[6] And finally, 'Anonymous' conducted Operation 'Titstorm' to disable the websites of the Australian Parliamentary House and the Department of Broadband, Communications and the Digital Economy to protest at mandatory internet filtering.[7]

These developments raise a range of questions. What precisely is occurring, and where are cyber threats emanating from? How does cyber activity fit within the paradigms of international law so familiar to us, if at all? Should our international, military and government lawyers respond? If so, how? What are the available legal options and the policy choices relevant to each?

This article addresses several of these questions by surveying the existing literature and contrasting recent policy developments within Australia with that of other states, principally the US and the United Kingdom (UK). Part II will define cyberspace. Part III describes how cyberspace is conceptualised as critical national infrastructure. Parts IV to VII examine four threats to Australian cyberspace: 'cyber war' conducted by states, 'cyber conflicts' between combatants, 'cyberterrorism' targeting civilians, and finally the use of computer technology to commit offences ('cybercrimes'). These parts will situate each threat within the relevant legal framework: international law on the use of force, international humanitarian law, anti-terrorism measures and criminal law enforcement. The adequacy of each regime for protecting Australia's electronic information infrastructure is assessed. Part VIII identifies challenges, risks and possible solutions, considers several cross-cutting themes and calls for further contributions which demonstrate a distinctive Australian perspective on these issues.

II Cyberspace Defined

'Cyberspace' may be defined as the interdependent network of information technology infrastructures. It includes the internet, telecommunications networks, computer processing systems and embedded industrial processors and controllers.[8] It is a domain characterised by electronics and the electromagnetic spectrum in which to store, modify and exchange data via networked systems as well as the associated physical infrastructure.[9] It is an environment within which various information operations occur.

On one view, cyberspace is borderless and transnational. The internet-based information infrastructure can accordingly be analogised to the global commons free from any one state's control and susceptible to appropriation.[10] However, the enabling physical infrastructure is clearly located within the territorial jurisdiction of a state. Thus cyberspace, like any other territorial domain (albeit artificially constructed), is subject to national interests. The UK has indicated that, '[j]ust as in the 19th century we had to secure the seas for our national safety and prosperity, and in the 20th century we had to secure the air, in

---

6 Dylan Welch, 'Engineers Off to US for Secret Cyber School', *Sydney Morning Herald* (online), 9 April 2011 <http://www.smh.com.au/technology/security/engineers-off-to-us-for-secret-cyber-school-20110408-1d7pt.html>.

7 Colin Ho and Benn Grubb, 'Govt Websites Attacked by Titstorm', *ZDNet Australia*, 10 February 2010 <http://www.zdnet.com/govt-websites-attacked-by-titstorm-1339300948/>.

8 Executive Office of the President of the United States, *Cyber Security and Monitoring*, US NSPD54/HSPD23 (8 January 2008). 'Cyber' derives from Greek and means 'governor'.

9 Chairman of the Joint Chiefs of Staff, *National Military Strategy for Cyberspace Operations* (December 2006) ix <www.dod.mil/pubs/foi/joint_staff/jointStaff_jointOperations/07-F-2105doc1.pdf>.

10 Stephen Lukasik, 'Protecting the Global Information Commons' (2000) 24 *Telecommunications Policy* 519, 525.

the 21st century we also have to secure our advantage in cyber space'.[11] For the US, cyberspace is as relevant a field for defence activity as the naturally occurring domains of land, sea, air and space.[12] Like the UK, the US Department of Defense will strategically address cyberspace as an operational domain in which to organise, train and equip itself so as to take full advantage of cyberspace's potential.[13] However, cyberspace is not protected through a passive 'retreat behind a Maginot line of firewalls' but by deploying dynamic 'manoeuvre warfare' where new technology proactively locates and neutralises intrusions.[14]

In addition to protecting a cyber network against intrusions, security requires maintaining the confidentiality, availability and integrity of information, incident response and effective deterrence. Cyberspace threats are believed to pose one of the most serious economic and national security challenges of the 21st century for the US and its allies.[15] Threats particular to Australian cyberspace include lone hackers, online criminals, 'issue motivated groups', industrial espionage and foreign intelligence services. Such threats are real, evolving and continue to test Australian defences.[16] Australia has identified cyber security as a national security priority as government and society become increasingly dependent upon (and correspondingly vulnerable for) integrated information technology.[17] Protecting cyberspace became a top-tier policy objective because of its position within critical national infrastructure.

III Cyberspace as Critical National Infrastructure

'Critical national infrastructure' is made up of those systems and assets so vital to states that incapacity or destruction would debilitate national security, the economy, public health or safety. Attacks can disrupt power, water, traffic control and other critical systems by targeting the electronic mechanisms which control manufacturing plants, power generators, refineries and other infrastructure. For example, malicious activities against electronic systems in the US have crippled electric power stations and caused multi-city power outages.[18]

The international community has proposed establishing a 'global culture of cyber security' to protect critical information infrastructures.[19] National efforts are being

---

11 UK Cabinet Office, *Cyber Security Strategy of the United Kingdom: Safety, Security and Resilience in Cyber Space* (June 2009) 5.

12 US Department of Defense, *Quadrennial Defense Review* (February 2010).

13 US Department of Defense, *Strategy for Operating in Cyberspace* (July 2011) 5–7.

14 William Lynn, US Department of Defense, 'Remarks at the USAF-Tufts Institute for Foreign Policy Analysis Conference' (Speech delievered at the USAF-Tufts-Institute for Foreign Policy Analysis Conference, Ronald Reagan Building, Washington DC, 21 January 2010) <http://www.defense.gov/speeches/speech.aspx?speechid=1410>.

15 Executive Office of the President of the United States, *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure* (2009) 1 <http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf>.

16 Mike Burgess, Cyber and Information Security Defence Signals Directorate (Speech delivered at the National Security Australia 2010 Conference, 26 February 2010) 14.

17 Kevin Rudd, Department of the Prime Minister and Cabinet, 'First National Security Statement to the Commonwealth Parliament' (Speech to the Australian Parliament, Canberra, 4 December 2008).

18 Executive Office of the President of the United States, above n 15.

19 *Creation of a Global Culture of Cybersecurity and the Protection of Critical Information Infrastructures*, GA Res 199, UN GAOR, 58th sess, 78th plen mtg, UN Doc A/Res/58/199 (30 January 2004).

reviewed to this end.[20] For example, the US acknowledges the need to protect computer systems and describes key portions of cyberspace as critical national infrastructure.[21] US financial institutions, credit systems, stock exchanges and the Federal Reserve depend upon functioning information networks.[22]

In 1997, President Clinton established the President's Commission on Critical Infrastructure Protection. The following year, US policy became taking 'all necessary measures to swiftly eliminate any significant vulnerability to both physical and cyber attacks on our critical infrastructures, including especially our cyber systems'.[23] An offensive capability against enemy computer networks became a policy directive under the administration of President George W Bush.[24]

During 2003, a 'National Strategy to Secure Cyberspace' encouraged greater public-private coordination and focused government initiatives on securing critical national infrastructure. The National Strategy presupposed that a healthy and functioning cyberspace was essential to the economy and national security.[25] Additionally, it foreshadowed efforts to formulate defensive strategies within an operational military context.[26] 'Cyberspace' became defined as the interdependent network of information technology infrastructures, and included the internet, telecommunications networks, computer systems and embedded industrial processors.[27] The US government was also called upon to protect privately owned critical infrastructure from attack, intrusion or sabotage by foreign military forces, terrorists and criminals.[28] In 2008, the scope of government concern was extended beyond critical national infrastructure, although the principal focus was protecting government networks.[29] Despite these efforts, in 2009 the cyber security responsibilities of the US Department of Homeland Security were adjudged to remain unsatisfied[30] and a comprehensive review of US cyber strategy was initiated.[31]

This brief review of US policy clearly illustrates the governmental concern to protect critical national infrastructure, albeit with several policy tangents and mixed success. Australian policy has largely followed suit. Australia's infrastructure is considered

---

20 *Creation of a Global Culture of Cybersecurity and Taking Stock of National Efforts to Protect Critical Information Infrastructures,* GA Res 64/211, UN GAOR, 64th sess, UN Doc A/Res/64/211 (17 March 2010).

21 US Department of Homeland Security, *The National Strategy to Secure Cyberspace* (February 2003) <http://www.dhs.gov/xlibrary/assets/National_Cyberspace Strategy.pdf>. See generally, Sean Condron, 'Getting it Right: Protecting American Critical Infrastructure in Cyberspace' (2007) 20 *Harvard Journal of Law and Technology* 403; Eric Jensen, 'Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense' (2002) 38 *Stanford Journal of International Law* 207, 240.

22 US Security Policy Board, *White Paper on Information Infrastructure Assurance* (December 1995).

23 Executive Office of the President of the United States, *Memorandum on Critical Infrastructure Protection*, PDD/NSC-63 (22 May 1998).

24 Executive Office of the President of the United States, *To Develop Guidelines for Offensive Cyber-Warfare*, NSPD 16 (July 2002).

25 Executive Office of the President of the United States, *The National Strategy to Secure Cyberspace* (2003) vii.

26 Executive Office of the President of the United States, *The National Strategy to Secure Cyberspace*, NSPD 38 (7 July 2004).

27 Executive Office of the President of the United States, *Cyber Security and Monitoring,* US NSPD54/HSPD23 (8 January 2008).

28 Executive Office of the President of the United States, *CyberSpace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure* (2009) 28.

29 Executive Office of the President of the United States, *Comprehensive National Cybersecurity Initiative*, NSPD54/HSPD23 (8 January 2008).

30 US Government Accountability Office, *National Cybersecurity Strategy: Key Improvements are Needed to Strengthen the Nation's Posture*, GAO-09-432T (10 March 2009) 4.

31 Executive Office of the President of the United States, *Cyberspace Policy Review* (2009).

vulnerable to criminal activity, natural disaster, terrorism and information warfare against civilian and military systems.[32] Australia's Cyber Security Strategy seeks to maintain a secure, resilient and trusted electronic operating environment with which to support national security and benefit the digital economy.[33] This strategy defines 'systems of national interest' as systems which, if rendered unavailable or compromised, could significantly impact upon Australia's economic prosperity, international competitiveness, public safety, social wellbeing or national security.[34]

In 2008, resilience was identified as an underlying element of critical infrastructure protection arrangements for Australia.[35] A Critical Infrastructure Resilience Strategy was developed.[36] 'Resilience' requires coordinated cross-sectoral planning, responsive, flexible and timely recovery measures, organisational cultures which ensure minimum service levels during interruptions, emergencies or disasters and networks which quickly return to full operation.[37] In other words, the policy focus has shifted from reducing the vulnerability of critical national infrastructure to, say, terrorist threats, to a whole-of-government approach.[38]

Unsurprisingly, the threats to Australian cyberspace have prompted legislative measures.[39] A suite of legislation has been adopted.[40] Several institutions have also been established. Most prominent among them is the Computer Emergency Response Team ('CERT') Australia and the Cyber Security Operations Centre within the Defence Signals Directorate.[41] The Australian Internet Security Initiative collects data concerning compromised computers operating on the Australian internet and informs the Australian Communications and Media Authority and internet service providers. The Trusted Information Sharing Network ('TISN') for Critical Infrastructure Protection is a forum where the owners and operators of critical infrastructure exchange information on common security concerns. Guidance on how to protect communications technology systems is increasingly available.[42]

These developments highlight the policy resolve to protect Australia's critical infrastructure. Like the US, the threat of cyber disruption is not limited to government networks. The financial loss from computer security 'events' committed against Australian businesses during 2006–07 was between A$595 and A$649 million.[43] In 2009, two

---

32 Adam Cobb, 'Thinking about the Unthinkable: Australian Vulnerabilities to High-Tech Risks' (Research Paper No 18, Parliamentary Library, Australian Parliament, Foreign Affairs, Defence and Trade Group, 29 June 1998).

33 Australian Government Attorney-General's Department, *Commonwealth Government Cyber Security Strategy* (2009) 5.

34 Ibid 12.

35 Ric Smith AO, *Homeland and Border Security Review* (27 June 2008).

36 Australian Government, *Critical Infrastructure Resilience Strategy* (30 June 2010) 8.

37 Council of Australian Government's Senior Officers' Meeting Review of National Critical Infrastructure Protection Arrangements, *Final Report* (2009). See also Council of Standards Australia, *Australian/New Zealand Standard for Risk Management*, AS/NZS ISO 31000, 20 November 2009.

38 Australian Government, *Critical Infrastructure Resilience Strategy Supplement*: *An Overview of Activities to Deliver the Strategy* (2010) 6, 11.

39 Australian Government, *Parliamentary Debates*, House of Representatives, 4 December 2008, 12549–61 (Kevin Rudd); 26 September 2001, 31582–4 (Daryl Williams); 27 June 2001, 28641–3 (Daryl Williams).

40 For example, the *Cybercrime Act 2001* (Cth) and the *Spam Act 2003* (Cth).

41 See further Department of Defence (Intelligence and Security), Cyber Security Operation Centre (CERT Australia), *Strategies to Mitigate Targeted Cyber Intrusions* (18 February 2010).

42 Department of Defence (Intellegence and Security), *Australian Government Information Security Manual* (September 2009).

43 Kelly Richards, Australian Institute of Criminology, *The Australian Business Assessment of Computer User Security: A National Survey* (2009).

Australian internet service providers were reportedly subjected to sustained disruption over several weeks which severely inhibited customer service.[44] The resulting question then becomes whether well-established international legal paradigms are adequate for implementing contemporary policy objectives.

IV Cyber Attack and the Use of Force

There is reputedly a 'growing consensus' that future conflicts between states will feature cyber operations which cripple national infrastructure, corrupt military data and hinder financial transactions.[45] Indeed, digital warfare might eclipse traditional kinetic engagements.[46] The UK, for example, identified the threat of cyber attack as one of the biggest security risks for the 21st century.[47] A 'cyber attack' has been defined as 'deliberate actions to alter, disrupt, deceive, degrade, or destroy computer systems or networks or the information and/or programs resident in or transiting these systems or networks'.[48] A cyber attack illustrates 'information warfare', which is the ability of military forces to protect their own information systems while simultaneously attacking those of its adversaries.[49]

Cyber attacks have reportedly been deployed against states. The US suspects attacks by China, which exploits informal relationships with civilians to conduct operations and gather intelligence.[50] 'Titan Rain' is a series of coordinated attacks upon US military computer systems occurring since 2003 whose precise nature (state-sponsored or corporate espionage or random hacker attacks) is unclear. In 2009, cyber attacks presumed to originate from North Korea temporarily jammed South Korean and US government websites during North Korean missile testing. Better known are Russia's alleged cyber attacks against Estonia in 2007.[51] Official websites in Georgia were also temporarily disabled by Russia during 2008, hindering government communication with citizens and creating confusion prior to Russia's invasion.[52] Other claimed instances include Israeli cyber attacks against Syria in 2007 and by the US in Iraq.

Are these precedents contributing to the evolution of customary international law in this field? States might be attempting to balance the use of a new kind of force against

---

44 Trusted Information Sharing Network, *Managing Denial of Service Attacks: Summary Report for CIOs and CSOs* (December 2009) 6.

45 John Chipman, Director-General of the International Institute for Strategic Studies, 'Military Balance 2010' (Press Statement, 3 February 2010) <http://www.iiss.org/publications/military-balance/themilitary-balance-2010/military-balance-2010-press-statement/>.

46 Brian O'Donnell and James Kraska, 'Humanitarian Law: Developing International Rules for the Digital Battlefield' (2003) 8 *Journal of Conflict and Security Law* 133, 160.

47 UK Cabinet Office, *Cyber Security Strategy of the United Kingdom: Safety, Security and Resilience in Cyber Space* (2009) 5.

48 William Owens, Kenneth Dam and Herbert Lin (eds), *Technology, Policy, Law and Ethics Regarding US Acquisition and Use of Cyberattack Capabilities* (National Academies Press, 2009) 1, 3. A 'computer network attack' has been similarly defined: US Department of Defense, *Technical Assurance Standard for Computer Network Attack Capabilities*, US Department of Defense Directive 0-3600.3, 13 May 2005; European Commission, *Commission Proposal for a Council Framework Decision on Attacks against Information Systems*, COM/2002/173 final (2002) 1–3.

49 See, for example, US Joint Chiefs of Staff, *Information Operations*, Joint Pub 3-13 (2006) ix <http://www.fas.org/irp/doddir/dod/jp3_13.pdf>.

50 Daniel Creekman, 'A Helpless America? An Examination of the Legal Options Available to the United States in Response to Various Cyber-attacks from China' (2002) 17 *American University International Law Review* 641.

51 Ian Taylor, 'Russia Accused of Unleashing Cyberwar to Disable Estonia', *The Guardian* (London), 17 May 2007.

52 Lesley Swanson, 'The Era of Cyber Warfare: Applying International Humanitarian Law to the 2008 Russian-Georgian Cyber Conflict' (2010) 32 *Loyola of Los Angeles International and Comparative Law Review* 303.

untested risks.[53] For example, states may wish to launch a cyber attack against another prior to the outbreak of hostilities without intending to provide the other side with a legal basis for regarding its action as having commenced hostilities.[54] Other states may be concerned to maintain their 'cyber neutrality' with all parties to a cyber conflict.[55]

For Australia, cyber warfare is a serious threat. A 2009 Defence White Paper observed that Australia's national security could be compromised by cyber attacks on our defence, governmental, commercial and infrastructure-related information networks.[56] Their potential impact has paradoxically grown with the Defence Department's increasing dependence on networked operations. Irregular opponents such as insurgents and terrorists are exploiting technology in low-risk and effective ways.[57] This circumstance has prompted a more enhanced cyber situational awareness and incident-response capability.[58]

New Zealand has similarly noted that hostile non-state actors seek to exploit whatever advantage they can from their cyber warfare capability.[59] The threat of cyber attack is growing, with potentially crippling consequences. Critical national infrastructure is increasingly reliant upon web-based information and communication networks for effective operations, with New Zealand defence forces and intelligence services being integrated into those networks.[60] States also possess the capability to conduct cyber attacks, and New Zealand may become a weak link in shared efforts to deter hostile cyber intrusions if it does not keep abreast of developments.[61]

The historical evolution of US defence policy concerning cyber attacks is instructive for both Australia and New Zealand. The US has described the scale and importance of information warfare as an offensive weapon and a defensive quagmire.[62] A comprehensive national security strategy which incorporated domestic and international dimensions had to be grafted around cyber security.[63] A host of international legal questions arose with respect to territorial jurisdiction, sovereign responsibility and the use of force.[64] The three US military services then independently developed their own information operations doctrine, cyber operations personnel, and institutions for managing and defending their information networks. The US Army, for example, addressed computer network operations as a subset of information operations.[65] The US Navy, by contrast, focused on

---

53 Greg Grove, 'Cyber-attacks and International Law' (2000) 42(3) *Survival* 89.

54 Office of General Counsel, US Department of Defense, *An Assessment of International Legal Issues in Information Operations* (1999) 5, reprinted in (2002) 76 *International Legal Studies* 459 <http://www.nwc.navy.mil/cnws/ild/studiesseries.aspx>.

55 Joshua Kastenberg, 'Non-intervention and Neutrality in Cyberspace: An Emerging Principle in the National Practice of International Law' (2009) 64 *Air Force Law Review* 43.

56 Australian Department of Defence, *Defending Australia in the Asia-Pacific Century: Force 2030* (2009) [9.85].

57 Ibid [2.25].

58 Ibid [9.87].

59 New Zealand Ministry of Defence, *Defence White Paper* (2010) [3.20].

60 Ibid [3.14].

61 Ibid [3.15].

62 US President's Commission on Critical Infrastructure Protection, *Critical Foundations: Protecting America's Infrastructure* (1997) 9.

63 Center for Strategic and International Studies Commission on Cybersecurity, *Securing Cyberspace for the 44th Presidency* (2008) 1.

64 Executive Office of the President of the United States, *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure* (2009).

65 US Army, *US Army Information Operations: Doctrine, Tactics, Techniques, and Procedures*, Field Manual 3-13 (November 2003).

accessing foreign information networks and defending its own networks from penetration.[66] The US Air Force formulated a network warfare policy 'across the interconnected analog and digital network portion of the battlespace'.[67] In 2006, the profile of cyberspace operations was elevated by assigning the 8th Air Force as the 'Air Force Cyberspace Command'.

The US military commenced preparations for persistent, asymmetrical threats to computer operations including 'adversary exploitation and attack of [its] computer networks on the global information grid'.[68] The Computer Network Defence is a program designed to protect military information, computers and networks from disruption or destruction. However, the absence of a unified or coherent government-wide cyber doctrine created the prospect of inadequate and ineffective responses to cyber threats.[69] Military strategy also began to shift from a 'one size fits all' deterrence model to a version tailored towards rogue states and terrorist groups. A national cyber doctrine which drew together the approaches of each of the military services was formulated. In 2009, the US established US Cyber Command to coordinate military operations within cyberspace.[70] The US Congress has also been called upon to establish a fourth military branch entitled 'Cyber Force'.[71]

Using computer technology within combat situations has now been comprehensively conceptualised within US military doctrine.[72] 'Cyber operations', for example, involve 'the employment of cyber capabilities where the primary purpose is to achieve military objectives or effects in or through cyberspace'.[73] 'Information warfare' includes attacks that alter information contained within systems such as servers, without visibly altering physical attributes.[74] Other key concepts include 'information operations', 'information system' and 'computer network attack'.[75]

The primary question is whether a cyber attack could qualify as an 'armed attack' within the use of force paradigm proscribed by art 2(4) of the Charter of the United Nations ('UN Charter'). The issue has received considerable attention by international lawyers.[76] The orthodox analysis for a use of force considers kinetic impacts such as explosions or

---

66 US Naval Network Warfare Command, *Navy NetwarCom Strategic Plan 2009-2013: A Framework for Decision-making* (2009) 6 <http://www.netwarcom.navy.millabout-us/StrategicPlan.pdf>.

67 US Air Force, *Doctrine Document 2.5.5* (2005) <http://www.dtic.mildoctrine/jelservice-pubs/afdd2_5.pdf>.

68 US Department of Defense, Joint Chiefs of Staff, *Joint Operation Planning*, Joint Publication JP 5-0 (26 December 2006) 1.

69 Mark Young, 'National Cyber Doctrine: The Missing Link in the Application of American Cyber Power' (2010) 4 *Journal of National Security Law and Policy* 173, 180.

70 Robert Gates, US Secretary of Defense, *Memorandum to the Secretaries of the Military Departments Concerning the Establishment of a Subordinate Unified US Cyber Command Under US Strategic Command for Military Cyberspace Operations* (2009) <http://online.wsj.com/public/resources/documents/OSD05914.pdf>.

71 Natasha Solce, 'The Battlefield of Cyberspace: The Inevitable New Military Branch: The Cyber Force' (2008) 18 *Albany Law Journal of Science and Technology* 293.

72 Joint Chiefs of Staff, US Department of Defense, *Joint Doctrine for Information Operations GL-2*, Joint Publication 3-13 (2006) <http://www.dtic.mil/doctrine/jel/new pubs/jp3 13.pdf>.

73 Joint Chiefs of Staff, US Department of Defense, *Dictionary of Military and Associated Terms*, Joint Publication 1-02 (2009) <http://www.dtic.mil/doctrine/jel/newoubs/jp102.pdf>.

74 Office of the Judge Advocate General, US Air Force, *Primer on Legal Issues in Information Operations* (1997) 13.

75 Clay Wilson, 'Electronic Warfare and Cyberwar: Capabilities and Related Policy Issues' (RL31787, US Congressional Research Service, 5 June 2007) 5.

76 See, for example, Marco Benatar, 'The Use of Cyber Force: Need for Legal Justification?' (2009) 3 *Goettingen Journal of International Law* 375; Daniel Silver, 'Computer Network Attack as a Use of Force under Article 2(4) of the United Nations Charter' (2002) 76 *International Legal Studies* 73.

physical force. One initial difficulty is identifying the threshold at which a cyber attack amounts to an 'armed attack'. Under customary international law a situation of 'armed conflict', for example, depends upon the existence of organised armed groups engaged in fighting of some intensity.[77] However, electronic attack is an atypical form of military combat.[78] Mere 'annoyances' must also be differentiated from those cyber activities intended to destroy infrastructure or human life.[79]

Attacks using conventional weapons clearly fall within art 2(4) of the UN Charter. However, the relevant provisions under that instrument 'do not refer to specific weapons. They apply to any use of force, regardless of the weapons employed.'[80] Supplying arms and logistics might be an unlawful use of force but would not qualify as an 'armed attack'.[81] Only the 'most grave' forms of force constitute an 'armed attack'.[82]

There are arguments that could support a conclusion that a cyber attack is an 'armed attack'. Several criteria derived from kinetic encounters — severity, immediacy, directness, invasiveness, measurability and presumptive legitimacy — have been applied to cyber attacks.[83] Thus the *jus ad bellum* would be sufficiently flexible to accommodate cyber attacks which do not cause physical damage such as disrupting online financial services or disabling military defence networks. A 'strict liability' approach, by contrast, automatically deems a cyber attack as an armed attack given the consequences to victim states. [84] Third, a 'consequentiality' or 'results-orientated' argument posits that an armed attack occurs whenever cyber activities directly occasion the same effects as are produced by kinetic force (that is, physical injury, death or property destruction).[85] In this respect, electronic systems control elements of the national electric power grid, air traffic control networks and nuclear power plant safety systems.

The prevailing consensus among scholars is that the paradigm on the use of force does not apply to cyber attacks which produce non-physical damage. Article 2(4) only captures physical damage. On this standard, only the damages caused by Stuxnet in Iran, and not Russia's cyber attacks against Estonia or Georgia, would qualify as a 'use of force'. Other action could instead qualify as a violation of the principle of non-intervention under customary international law,[86] thereby not leaving states as vulnerable as some may suggest. In any event, a cyber attack which intentionally causes destructive effects within state territory will more clearly constitute an unlawful use of force under art 2(4).[87] The

---

77 International Law Association, *Report of the International Committee on the Use of Force* (2010) 30, 32.

78 Wesley Clark and Peter Levin, 'Securing the Information Highway: How to Enhance the United States Electronic Defenses' (2009) *Foreign Affairs* 2.

79 Wolfgang McGavran, 'Intended Consequences: Regulating Cyber Attacks' (2009) 12 *Tulane Journal of Technology and Intellectual Property* 259, 275.

80 *Legality of the Threat or Use of Nuclear Weapons (Advisory Opinion)* [1996] ICJ Rep 244, [38].

81 *Case concerning Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America) (Merits)* [1986] ICJ Rep 14, [191], [195].

82 *Case concerning Oil Platforms (Islamic Republic of Iran v United States of America) (Merits)* [2003] ICJ Rep 161, [51], [63], [64], [72].

83 Michael Schmitt, 'Computer Network Attacks and the Use of Force in International Law: Thoughts on a Normative Framework' (1999) 37 *Columbia Journal of Transnational Law* 885, 913–15.

84 David Graham, 'Cyber Threats and the Law of War' (2010) 4 *Journal of National Security Law and Policy* 87, 91.

85 Ian Brownlie, *International Law and the Use of Force by States* (Clarendon Press, 1963) 362.

86 Russell Buchan, 'Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?' (2012) 17 *Journal of Conflict and Security Law* 212.

87 Walter Sharp, *Cyberspace and the Use of Force* (Aegis Research Corp, 1999) 140.

effects-based analysis has been adopted by, for example, the US Department of Defense.[88] A cyber attack could be an 'act of war' sufficient to trigger a military response.[89] A former UK national security adviser has similarly concluded that a cyber attack could be an 'act of war' while conceding that novel 'laws of war' were necessary.[90]

The characterisation of a cyber attack as an 'armed attack' raises many questions. First, could a cyber attack be a threat to international peace and security or perhaps a breach of the peace so as to precipitate UN Security Council action under ch VII of the UN Charter? The US considers that computer network attacks which cause widespread damage, economic disruption and lost life could do so.[91] A UN expert body concluded that information security threats present risks to 'the stability of a globally-linked international community'.[92] The Council could authorise 'cyber sanctions' inasmuch as one measure 'not involving the use of armed force' is the 'complete or partial interruption of economic relations and of rail, sea, air, postal, telegraphic, radio, and other means of communication'.[93]

Second, even assuming *arguendo* that a cyber attack is an 'armed attack', could a cyber attack be an 'act of aggression'? 'Aggression' is the use of armed force by a state against the sovereignty, territorial integrity or political independence of another, or in any manner inconsistent with the UN Charter.[94] The well-recognised acts of aggression, such as invasion by armed forces, bombardment and blocking ports or coasts, suggest that such acts are essentially physical and armed in nature. The views of states have been solicited.[95] Mali, for example, considers that using 'information weapons' could be an 'act of aggression' where a victim state believed that the attack was executed by the armed forces of another and directed towards disrupting military facilities, destroying defensive and economic capacity or violating sovereignty.[96] Characterising a cyber attack as an act of aggression triggers additional questions, including potential intervention from the International Criminal Court.[97]

---

88 US Department of Defense, Office of General Counsel, *An Assessment of International Legal Issues in Information Operations* (1999).

89 John Garnaut and Sanghee Liu, 'China Denies Mass Hacking of Gmail Accounts', *Sydney Morning Herald* (Sydney), 3 June 2011, 7.

90 Brian Wheeler, 'Cyber Attacks 'Acts of War' — Sir Richard Mottram', *BBC News* (online), 16 February 2011 <http://www.bbc.co.uk/news/uk-politics-12485147>.

91 US Department of Defense, Office of General Counsel, *An Assessment of International Legal Issues in Information Operations* (1999) 15; Executive Office of the President of the United States, *The National Strategy to Secure Cyberspace* (2003) 49–52 <http://www.dhs.gov/xlibrary/assets/NationalCyberspace-Strategy.pdf>.

92 *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, UN GAOR, 65th sess, Agenda item 94, UN Doc A/65/201 (30 July 2010) 2.

93 *Charter of the United Nations* art 41.

94 *Resolution on the Definition of Aggression*, GA Res 3314, UN GAOR, 34th sess, 2319th plen mtg, UN Doc A/Res/3314 (14 December 1974) annex art 1. Article 3 lists seven acts which qualify as acts of aggression and art 4 notes that these enumerated acts are 'not exhaustive.'

95 *Report on Developments in the Field of Information and Telecommunications in the Context of International Security — Report of the Secretary General*, UN GAOR, 64th sess, UN Doc A/64/129 (8 July 2009) and *Developments in the Field of Information and Telecommunications in the Context of International Security — Report of the Secretary General*, UN GAOR, 64th sess, Agenda Item 91, UN Doc A/64/129/Add. 1 (9 September 2009).

96 Ibid [22]. For comment, see Sean Kanuck, 'Sovereign Discourse on Cyber Conflict Under International Law' (2010) 88 *Texas Law Review* 1571, 1585–7.

97 Jonathan Ophardt, 'Cyber Warfare and the Crime of Aggression: The Need for Individual Accountability on Tomorrow's Battlefield' (2010) 3 *Duke Law and Technology Review* 1.

A third question is whether a state may adopt measures in the exercise of its inherent right to self-defence and, if so, which ones.[98] In 2007, the North Atlantic Treaty Organisation indicated that a cyber attack would not trigger the collective self-defence provisions of the constituent treaty.[99] However, Australia and the US have since agreed that a 'substantial cyber attack' against either state would activate the Australia/New Zealand/United States ('ANZUS') military alliance.[100] The ANZUS Treaty[101] was duly amended so that 'in the event of a cyber attack that threatens the territorial integrity, political independence or security of either of our nations, Australia and the United States would consult together and determine appropriate options to address the threat.'[102] This step reflects their mutual intention to deepen cyber security cooperation.[103] The US has indicated that, if attacked in cyberspace, it would 'respond in an appropriate manner', including deploying cyber weapons.[104] The US is also a proponent of defensive strategies which contemplate proactively seeking out and neutralising cyber threats before they eventuate. In Europe, exercises are regularly conducted to test security incident responses to cyber attacks against large-scale networks.[105] CERTs — a model which Australia adopted — are a responsive measure against cyber attack.[106]

The prevailing academic view is that a cyber attack upon critical national infrastructure which amounts to a 'use of force' gives rise to a good faith response by states. A cyber attack would be grave enough to engage art 51 of the UN Charter if, for example, corrupting the computer systems of civil aviation networks caused loss of life and property destruction on a sufficient scale. The nature of that response is not restrained by 'outdated' interpretations of the right to self-defence.[107] The classic requirements of self-defence — necessity and proportionality — have been applied to a cyber response.[108] Furthermore, conventional military force could also be used to respond to a cyber attack provided states comply with the applicable legal requirements including reporting to the Security Council.[109] These conclusions will be revisited in Part VII below; suffice it to say that,

---

98 See, for example, Horace Robertson, 'Self-Defense Against Computer Network Attack Under International Law' (2002) 76 *International Legal Studies* 121.

99 Johnny Ryan, 'Growing Dangers: Emerging and Developing Security Threats' (Winter 2007) *NATO Review* <http://www.nato.int/docu/review/2007/issue4/english/analysis2.html>.

100 'Cyber War Added to ANZUS Pact', *Sydney Morning Herald* (Sydney), 16 September 2011.

101 No 2 Security Treaty between Australia, New Zealand and the USA [ANZUS], opened for signature 1 September 1951, [1952] ATS 2 (entered into force 29 April 1952).

102 'All the Way with the US in the Fifth Domain of Warfare', *Sydney Morning Herald* (Sydney), 20 September 2011, 11.

103 Paul Maley, "'Battleground of the Future" the Focus of New Agreement with US', *The Australian* (Sydney), 18 May 2012.

104 US Department of Homeland Security, *The National Strategy to Secure Cyberspace* (2003), 50 <http://www.uscert.gov/reading-room/cyberspace-strategy.pdf>.

105 *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection, Protecting Europe from Large Scale Cyber-attacks and Disruptions: Enhancing Preparedness, Security and Resilience*, SEC/2009 [2009] 149.

106 UK House of Lords, European Union Committee, *Protecting Europe against Large-scale Cyber-attacks*, House of Lords Paper No 68, Session 2009-2010 (2010) 21–3.

107 See, for example, Matthew Hoisington, 'Cyberwarfare and the Use of Force Giving Rise to the Right of Self-Defence' (2009) 32 *Boston College International and Comparative Law Review* 439, 453–4.

108 Thomas Wingfield, *The Law of Information Conflict: National Security Law in Cyberspace* (Aegis Research, 2000) 41–4. See generally Nicholas Tsagourias, 'Cyber Attacks, Self-defence and the Problem of Attribution' (2012) 17 *Journal of Conflict and Security Law* 229.

109 Christopher Petras, 'The Use of Force in Response to Cyber-Attack on Commercial Space Systems — Re-examining 'Self-Defence' in Outer Space in Light of the Convergence of US Military and Commercial Space Activities' (2002) 67 *Journal of Air Law and Commerce* 1213, 1260.

where damage is minimal, identifying a permissible retaliatory response to a cyber attack becomes difficult.[110] And in order to be an effective deterrent, any threatened response must be consequential. However, just as threatened military retaliation may have little impact upon those groups lacking identifiable assets, cyber responses have little effect upon adversaries who are not 'cyber dependent'.[111] Existing international law is already unsettled on whether self-defensive measures can be taken against non-state actors.[112] In sum, the paradigm of international law on the use of force raises more questions than answers. Is the position under international humanitarian law any clearer?

V Cyber Conflict and International Humanitarian Law

Cyber conflict has been assessed against the key principles of international humanitarian law.[113] For example, cyber conflict may blur the principle of distinction between military objectives and civilian infrastructure.[114] Virtually all US government communications travel through civilian owned and operated networks, and there is complete government dependence on civilian providers of computer software, hardware, services and maintenance.[115] The intermingling of civilian and military computer infrastructure thereby renders civilian objects susceptible to targeting. Nevertheless, it is considered possible — and necessary — to distinguish between civilian and military computer networks.[116] The principle of distinction can, on one view, apply to computer network attacks as any other attack.[117]

The tendency of developed, Western armed forces to outsource technical specialist functions to civilians is also difficult to reconcile with the notion of direct participation in hostilities.[118] Does direct participation in hostilities include the programming, operation or maintenance of computer systems? The International Committee of the Red Cross ('ICRC') considers that, if the test is whether a person carries out acts which aim to support one party to a conflict by directly causing harm to another, either by directly inflicting death, injury and destruction or directly harming the enemy's military operations

---

110 Bryan Ellis, *The International Legal Implications and Limitations of Information Warfare: What are our Options?* (USAWC, 2001) 9.

111 K Taipale, '"Cyber-deterrence", Law, Policy and Technology: Cyberterrorism, Information Warfare, Digital and Internet Immobilization' (2010) <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1336045>.

112 *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory (Advisory Opinion)* [2004] ICJ Rep 136, [139]; *Armed Activities on the Territory of the Congo (Congo v Uganda)* [2005] ICJ Rep 4, [146]. See further Brent Michael, 'Responding to Attacks by Non-State Actors: The Attribution Requirement of Self-Defence' (2009) 16 *Australian International Law Journal* 133.

113 See, eg, Ruth Wedgwood, 'Proportionality, Cyberwar and the Law of War' (2000) 76 *International Legal Studies* 219; Michael Schmitt, Heather Harrison and Thomas Wingfield, *Computers and War: The Legal Battlespace* (2004) <http://www.ihlresearch.org/ihl/pdfs/schmittetal.pdf>.

114 Jeffrey Kelsey, 'Hacking Into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare' (2008) 106 *Michigan Law Review* 1427, 1446–7.

115 Eric Jensen, 'Cyber Warfare and Precautions against the Effects of Attacks' (2009–10) 88 *Texas Law Review* 1533.

116 James Terry, 'The Lawfulness of Attacking Computer Networks in Armed Conflict and in Self-Defense in Periods Short of Armed Conflict: What Are the Targeting Constraints?' (2001) 169 *Military Law Review* 70, 90–1.

117 Yoram Dinstein, 'The Principle of Distinction and Cyber War in International Armed Conflicts' (2012) 17 *Journal of Conflict and Security Law* 261.

118 David Turns, 'Cyber Warfare and the Notion of Direct Participation in Hostilities' (2012) 17 *Journal of Conflict and Security Law* 279.

or capacity, then electronic interference with military computer networks by civilians is one example.[119]

Cyber conflicts give rise to an initial difficulty of classification. It is argued that cyber operations are an 'international armed conflict' between states when they injure individuals or damage objects.[120] Such an activity is a 'non-international armed conflict' when hostilities between a state and an 'organised' armed group are sufficiently intense, protracted, non-isolated and reach a certain level of violence. A low-intensity cyber conflict could also be analogised to an insurgency.[121]

Applying international humanitarian law to a cyber conflict proves elusive in other respects. Balancing military advantage against the extent of civilian harm — the principle of proportionality — is challenging. Furthermore, an 'attack' involves '*acts of violence* against the adversary, whether in offence or in defence'.[122] That definition would be difficult to reconcile with that of a 'cyber attack' as 'the premeditated use of disruptive activities, *or the threat thereof*, against computers and/or networks, *with the intention to cause harm* or to further social, ideological, religious, political or similar objectives or to *intimidate* any person in furtherance of such objectives'.[123]

Cyber weapons are many and varied.[124] They include 'sniffers',[125] 'trojan horses', 'rootkits' or 'trap doors',[126] 'logic bombs',[127] 'video-morphing',[128] 'distributed denial of service attacks',[129] 'malware' including 'worms' or 'viruses',[130] 'infoblockades',[131] 'spamming',[132] 'zombies' or 'bots'[133] and 'IP spoofing'.[134] 'Hacking' is breaking into a computer's operating system, whereas 'brute-force intrusion' attempts all possible code combinations. Such techniques can be executed with limited resources against large and

---

119 International Committee of the Red Cross, *Interpretative Guidance on the Notion of Direct Participation in Hostilities Under International Humanitarian Law* (2009).

120 Michael Schmitt, 'Classification of Cyber Conflict' (2012) 17 *Journal of Conflict and Security Law* 245.

121 Samuel Liles, 'Cyber Warfare as a Form of Low-intensity Conflict and Insurgency' (Paper presented at the Conference on Cyber Conflict Proceedings, 2010).

122 *Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I)*, signed 12 December 1997, 1125 UNTS 3 (entered into force 7 December 1977) art 49 ('*Additional Protocol 1*') (emphasis added).

123 US Army Training and Doctrine Command, *Critical Infrastructure Threats and Terrorism*, DCS Int Handbook No 1.02 (2006) VII-2.

124 Christopher Joyner and Catherine Lotrionte, 'Information Warfare as International Coercion: Elements of a Legal Framework' (2001) 12 *European Journal of International Law* 825, 836–9.

125 Programs executed from remote sites for retrieving user identifications, passwords and other information.

126 Programs used to gain unauthorised access to secured networks.

127 Malicious coding which lies dormant until a trigger condition (either a specific event or predetermined time) causes it to activate and destroy the host computer's files.

128 Rendering broadcasts indistinguishable from normal transborder data flows.

129 Multiple data requests flood an internet site, server, or router to slow or impede regular traffic until functional capacity becomes overwhelmed.

130 These travel from computer to computer across a host's network to damage files and corrupt or destroy data.

131 This blocks electronic information from entering or leaving national borders.

132 Email systems are flooded with frivolous messages to overload servers and prevent communication.

133 Automated tools which contaminate other computers and launch coordinated attacks in the nature of a 'distributed denial of service attack'.

134 Also known as 'IP address forgery' or a 'host file hijack', this occurs when hijackers masquerade as trusted hosts to fabricate messages or copy websites in order to capture browsers or gain network access.

technologically sophisticated computers or networks. Cyber weapons target a computer's operating system through malicious codes, misinformation and data retrieval.[135]

On one view, it is 'perfectly reasonable' that cyber weapons are subject to international humanitarian law as is any other new weapon system.[136] The ICRC takes this position.[137] Identical questions have arisen with respect to, for example, the deployment of drones and automated weapons. The use of electro-magnetic pulse weapons, directed energy lasers, microwave devices, high-energy radio frequency guns and other electronic weapons are subject to international humanitarian law. States which develop 'a new weapon, means or method of warfare' must determine whether its deployment is prohibited by *Additional Protocol 1* or another international legal rule.[138] The US Air Force, for example, considers that computer networks are not weapons systems.[139] Other states including Australia may have yet to assess cyber weapons. In the contemporary security environment another form of cyber activity has dominated attention: cyberterrorism.[140]

VI Cyberterrorism

'Terrorism' is variously defined.[141] So too is 'cyberterrorism'. Cyberterrorism has been defined as 'the politically-motivated use of computers as weapons or as targets, by sub-national groups or clandestine agents intent on violence, to influence an audience or cause a government to change its policies'.[142] The activity generally means unlawful attacks, and the threat thereof, against computers, networks and information.[143]

Cyber operations are ideal for terrorists. Offensive operations may be conducted over the internet to complement orthodox tactics.[144] Hezbollah's strategy, for example, includes disrupting Israel's economy by targeting official and financial websites, knocking out internet servers and crippling e-commerce.[145] The internet enables terrorists to research and coordinate attacks.[146] Terrorists may use it for psychological warfare, publicity or

---

135 Vida Antolin-Jenkins, 'Defining the Parameters of Cyberwar Operations: Looking for Law in All the Wrong Places?' (2005) 51 *Naval Law Review* 132, 144.

136 Louise Doswald-Beck, 'Some Thoughts on Computer Network Attack and the International Law of Armed Conflict' (2002) 76 *International Legal Studies* 163, 164.

137 Knut Dormann, *Applicability of the Additional Protocols to Computer Network Attacks* (2004) <http://ww.icrc.org/Web/Eng/siteeng).nsf/html/68LG92>.

138 *Additional Protocol 1* art 36(1).

139 Memorandum from US Air Force Operations and International Law Division to Staff Judge Advocate, US Air Force Command Agency, *Legal Issues Related to 'Network as a Weapon System* (13 May 2005).

140 See, for example, Richard Garnett and Paul Clarke, 'Cyberterrorism: 'A New Challenge for International Law', in Andrea Bianchi and Yasmin Naqvi, *Enforcing International Law Norms against Terrorism* (Hart Publishing, 2004) 454; David Gray and Albon Head, 'The Importance of the Internet to the Post-Modern Terrorist and its Role as a Form of Safe Haven' (2009) 25 *European Journal of Scientific Research* 396; Elizabeth Renieris, 'Combating Incitement to Terrorism on the Internet: Comparative Approaches in the United States and United Kingdom and the Need for an International Solution' (2009) 1 *Vanderbilt Journal of Entertainment and Technology Law* 673; Indira Carr, *Cyber Security and Cyberterrorism* (Ashgate, 2010).

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

142 Mohammad Iqbal, 'Defining Cyberterrorism' (2004) 22 *John Marshall Journal of Computer and Information Law* 397. Compare Maura Conway, 'What is Cyberterrorism?' (2002) 101(659) *Current History* 436.

143 Dorothy Denning, 'Activism, Hactivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy', in John Arquilla and David Ronfeldt (eds), *Networks and Netwars* (Rand Corporation, 2001) 241.

144 Michael Hummel, 'Internet Terrorism' (2008) 2 *Homeland Security Review* 117, 126.

145 Timothy Thomas, *Cyber Silhouettes: Shadows over Information Operations* (Foreign Military Studies Office, 2005) 42.

146 Todd Hinnen, 'The Cyber-Front in the War on Terrorism: Curbing Terrorist Use of the Internet' (2004) 5 *Columbia Science and Technology Law Review* 3, 4.

propaganda, data mining, fundraising, recruitment or mobilisation, networking, information sharing, and planning or coordination.[147] All active terrorist groups have an internet presence and employ social networking or video-sharing sites and online communities.[148] The interactive capacity of YouTube and Facebook enables terrorists to recruit personnel.[149] Blogging services including Twitter can become a coordination tool for launching attacks.[150] Communication occurs over the internet[151] as well as through chatrooms, message boards or email, which impose minimal disclosure requirements and are simply and inexpensively established.[152] Digital currency facilitates money transfers, avoids financial institutions, is difficult to trace, does not require customer identification and is free from oversight.[153] Virtual worlds for transferring funds or information offer similar advantages.[154]

Existing international law concerning terrorism can be applied to cyberterrorism. For example, an attack against infrastructure is 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'.[155] However, cyberterrorism is distinguishable from other forms of terrorism.[156] Cyber terrorists typically target military defence or government networks, privately or publicly operated systems which control utility services (including electricity or water) and networks used by individuals, businesses and others for communication or other purposes.[157] Cyber terrorists may prefer to undermine electronic commerce rather than attack critical national infrastructure.[158] States which are highly dependent on electronic communication and information processing networks are accordingly more vulnerable to cyberterrorism.[159]

---

147 See generally Maura Conway, 'Terrorist "Use" of the Internet and Fighting Back' (Paper prepared for presentation at Cybersafety: Safety and Security in a Networked World — Balancing Cyber-Rights and Responsibilities, Oxford Internet Institute, 8–10 September 2005).

148 Gabriel Weimann, 'Terror on Facebook, Twitter and Youtube' (2009–10) 16 *Brown Journal of World Affairs* 45.

149 Andrew Liepman, Deputy Director for Intelligence at the National Counterterrorism Center, 'Violent Islamist Extremism: Al-Shabaab Recruitment in America', Hearing before the Senate Homeland Security and Governmental Affairs Committee (11 March 2009).

150 US Army 304 (Military Intelligence) Battalion, *Intelligence Report, Potential for Terrorist Use of Twitter* (2008), reported in 'US Army Says Blogging Site "Twitter" Could Become Terrorist Tool', *FoxNews* (online), 27 October 2008 <http://www.foxnews.com/story/0,2933,444089,00.html>.

151 *Terrorist/Jihadist Use of the Internet for Strategic Communications: Hearing Before the House Permanent Select Committee on Intelligence*, 109th US Congress (4 May 2006).

152 Benjamin Davis, 'Ending the Cyber Jihad: Combating Terrorist Exploitation of the Internet with the Rule of Law and Improved Tools for Cyber Governance' (2006) 15 *Communications Law Conspectus* 119, 129.

153 William Hett, 'Digital Currencies and the Financing of Terrorism' (2008–09) 15 *Richmond Journal of Law and Technology* 1.

154 Stephen Landman, 'Funding Bin Laden's Avatar: A Proposal for the Regulation of Virtual Hawalas' (2008–09) 35 *William Mitchell Law Review* 5159.

155 *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).

156 Susan Brenner and Marc Goodman, 'In Defense of Cyberterrorism: An Argument for Anticipating Cyber-Attacks' (2002) *Journal of Technology and Policy* 1, 12.

157 Joel Trachtman, 'Global Cyberterrorism, Jurisdiction, and International Organization' in Mark Grady and Francesco Parisi (eds), *The Law and Economics of Cybersecurity* (Cambridge University Press, 2006) 259.

158 Lorenzo Valeri and Michael Knights, 'Affecting Trust: Terrorism, Internet and Offensive Information Warfare' (2000) 12(1) *Terrorism and Political Violence* 15.

159 Richard Clarke, 'Threats to US National Security: Proposed Partnership Initiatives Towards Preventing Cyber Terrorist Attacks' (1999–2000) 12 *DePaul Business Law Journal* 33, 37.

There is no treaty specifically addressing cyberterrorism. A draft International Convention on Cybercrime and Terrorism proposes to criminalise the use of cyber systems to commit those offences specified under existing anti-terrorism treaties which target critical national infrastructure.[160] The UN has just begun to address the topic. Member states were called upon to 'note the risk of terrorists using electronic or wire communications systems and networks to carry out criminal acts and to find means to prevent such criminality'.[161] The Security Council has called for information exchange concerning the 'use of communications technology by terrorist groups'.[162] States are already obliged to prevent and suppress terrorist financing, to criminalise terrorism-related activities such as providing assistance and to deny funding or safe haven to terrorists.[163] Such measures could also be applied to cyberterrorism.[164]

These circumstances give rise to several challenging questions of state responsibility. The first is the responsibility of states to prevent their territory from being used by cyber terrorists.[165] Victim states must determine the source of a cyber attack and whether the state from which attacks were launched was a sanctuary state.[166] Although cyber attacks are commonly committed remotely by anonymous perpetrators, it is technically possible to attribute that conduct to a particular state.[167] The UN General Assembly has called upon states to prevent their territories from being used as safe havens from which to launch cyber attacks against other states.[168] This approach is consistent with holding the Taliban government of Afghanistan responsible for al-Qaeda's actions on September 11. A duty of prevention has been proposed which requires states to prevent cyber terrorist acts, prevent their territories from harbouring cyber terrorists or being used as launch pads for cyberterrorism, and to ensure that national law criminalises and punishes cyberterrorism. Cyberterrorism raises additional questions of state attribution; for example, whether such an action is imputable to states which allow it to occur or support it in other ways. The degree of control exercised by a state over a non-state actor also falls for consideration.[169]

It is difficult to assess the capabilities of terrorists to launch cyber attacks. Cyber attacks may be used to supplement conventional physical attacks which inflict human casualties, cause immediate drama and offer greater psychological impacts. However, stringent physical security measures could encourage terrorists to explore other means of lowering

---

160 Abraham Sofaer et al, *A Proposal for an International Convention on Cyber Crime and Terrorism* (2000).

161 *Measures to Eliminate International Terrorism*, GA Res 51/210, UN GAOR, 51st sess, UN Doc A/RES/51/254 (16 January 1997).

162 *Security Council Resolution 1373*, 4385th mtg, UN Doc S/Res/1373 (2001).

163 Ibid.

164 Christopher Lentz, 'A State's Duty to Prevent and Respond to Cyberterrorist Acts' (2009-2010) 10 *Chicago Journal of International Law* 799, 818.

165 Tal Becker, *Terrorism and the State: Rethinking the Rules of State Responsibility* (Hart Publishing, 2006) 3.

166 David Wheeler and Gregory Larsen, *Techniques for Cyber Attack Attribution, Institute of Defence Analysis* (2003), 23–4 <http://www.dtic.mil/cgi-bin/GetTRDoc?AD-ADA468859&Location=U2&doc=GetTRDoc.pdf>.

167 Susan Brenner, "'At Light Speed": Attribution and Response to Cybercrime/Terrorism/Warfare' (2007) 97 *Journal of Criminal Law and Criminology* 376.

168 *Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders*, GA Res 45/121, UN GAOR, 45th sess, 68th plen mtg, UN Doc A/Res/45/121 (1990); *Combating the Criminal Misuse of Information Technologies*, GA Res 55/63, UN GAOR, 55th sess, 3rd plen mtg, UN Doc A/Res/55/63 (2001).

169 *Military and Paramilitary Activities In and Against Nicaragua (Nicaragua v US)* [1986] ICJ Rep 14, [110] (a state must exercise 'effective control' over non-state actors who are in 'complete dependence' upon the state), confirmed in *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v Serbia and Montenegro) (Judgment)* [2007] ICJ Rep 2, [400], with *Prosecutor v Tadic* (International Criminal Tribunal for the Former Yugoslavia, Case No. IT-94-1-A ICTY App Ch, 15 July 1995) 49 ('overall control').

detection risks. Once a successful cyber attack has won media attention, other terrorists could replicate similar strategies.

US intelligence agencies have warned that terrorist groups intend to employ cyber attacks.[170] President Obama has indicated that terrorism could emanate from computer keystrokes which release weapons of 'mass disruption'.[171] The US National Security Strategy includes preventing terrorist attacks, denying financial and other support and targeting sanctuary states.[172] Terrorist websites are taken offline through countermeasures. For example, the US Department of Defense electronically dismantled an online forum used by terrorists to exchange operational information for intended attacks against US soldiers.[173] Internet service providers incorporated within US jurisdiction are prohibited from conducting business with designated terrorist organisations through shaming techniques, denied commercial opportunities and threatened criminal sanctions.[174]

In Europe during 2008, three offences were adopted to address online terrorist activity: public provocation to commit terrorist offences; recruitment for terrorism; and training for terrorism.[175] Courts can require internet service providers to remove information and shut down websites. European states are directed to retain certain data generated or processed following a communication or use of a communication service.[176] Internet service providers must retain user identification, telephone numbers and IP addresses for both senders and recipients.

Non-conventional security challenges, including the threat of cyberterrorism, pose similar challenges for the national security of New Zealand.[177] The threat to New Zealand and its economy from cyber intrusions is considered real and growing.[178]

Nevertheless, there is little available empirical data which clarifies the extent or magnitude of cyberterrorism. Is the threat overstated?[179] Promoting the theme of a constant threat perpetuates the self-serving agendas of military, intelligence and security agencies. There are significant gaps between the cyber threat presumed within the literature and the empirical reality of known terrorist behaviour.[180] Although the threat may be 'real' such that affected actors must 'comprehend the risk', it is admittedly difficult to measure 'success' in ensuring security.[181]

---

170 US Government Accountability Office, *House of Representatives on Cybersecurity: Continued Federal Efforts are Needed to Protect Critical Systems and Information*, GAO-09-835T (2009) 2, n 2, citing Director of National Intelligence, *Statement before the Senate Select Committee on Intelligence, Annual Threat Assessment of the Intelligence Community for the Senate Select Committee on Intelligence* (2009).

171 US President Barack Obama, 'Remarks on Securing Our Nation's Cyber Infrastructure' (Press Statement, 29 May 2009).

172 Executive Office of the President of the United States, *The National Security Strategy of the United States* (2006).

173 Paul Walker, 'Traditional Military Activities in Cyberspace: Preparing for 'Netwar'' (2010) 22 *Florida Journal of International Law* 333.

174 Gregory McNeal, 'Cyber Embargo: Countering the Internet Jihad' (2006–08) 39 *Case Western Reserve Journal of International Law* 789.

175 *European Council Framework Decision 2008/919* [2008] OJEC L330, 21, 21.

176 *European Parliament and Council Directive 2006/24* [2006] OJEC L105, 54.

177 New Zealand Defence Force, *Statement of Intent 2011–2014*, G55 SOI (2011) 12.

178 New Zealand Government, *Cyber Security Strategy* (2011) 4, 5.

179 Mark Pollitt, 'Cyberterrorism — Fact or Fancy?' (2009) <http://www.cs.georgetown.edu/~denning/infosec/pollitt.html>.

180 Michael Stohl, 'Cyberterrorism: a Clear and Present Danger, the Sum of All Fears, Breaking Point or Patriot Games?' (2006) 46(4) *Journal of Crime, Law and Social Change* 223.

181 Defence Signals Directorate, 'Cyber Security — Beyond the Firewall' (Speech delievered at the Security in Government Conference, 27 July 2011) 2, 14.

Australia also recognises cyberterrorism as a threat but to date has acquired little practical experience with it. The 2010 Counter-Terrorism White Paper observes that, although terrorists have not demonstrated a strong interest in cyber attacks, Australia has nevertheless implemented measures to reduce the risk and consequences of such an attack upon Australian interests.[182] The terrorist threat is considered real, enduring and a persistent and permanent feature of Australia's security environment.[183] The defence services are expected to support civilian authorities through domestic security arrangements and emergency response efforts.[184]

Australia has also strengthened law enforcement powers. For example, the *Cybercrime Act 2001* (Cth) sch 2 enables federal authorities to search and seize electronically stored data, thereby facilitating the investigation and prosecution of groups using the internet to plan and launch attacks which could seriously interfere with the functioning of government or industry.[185] The *Crimes Legislation Amendment (Telecommunications Offences and other Measures) Act 2004* (Cth) sch 1, which introduced offences into the *Criminal Code Act 1995* (Cth), including 'using a telecommunications network with intention to commit a serious offence' (s 474.14), 'using a carriage service to make a threat' (s 474.15) and 'using a carriage service for a hoax threat' (s 474.16), is potentially applicable to cyberterrorism. More controversially, terrorist organisations can be proscribed such that individual members or supporters are liable for criminal prosecution.[186] Finally, the *Suppression of the Financing of Terrorism Act 2002* (Cth) inserted div 103 into the *Criminal Code Act 1995* (Cth) to address terrorist financing.

Australian law can address cyberterrorism. A 'terrorist act' is defined as an action or threat thereof intended to advance political, religious or ideological causes with a view to coercing or influencing by intimidation a government or the public.[187] Harm includes serious interference, disruption or destruction of electronic systems including those used for information, telecommunications, finance, essential government service delivery, public utilities or transport.[188] These offences have a broad extraterritorial application.[189]

However, there has not to date been any prosecution for a cyber attack under these provisions. The few prosecutions within Australia have principally addressed internet fraud or child pornography.[190] The closest case involved an accused allegedly downloading images of Australian military facilities from the internet in connection with the intended commission of terrorist acts.[191] In another matter, a book entitled *Provisions on the Rules of*

---

182 Australian Government, *Counter-Terrorism White Paper: Securing Australia, Protecting Our Community* (2010) 45.

183 Ibid 7.

184 Ibid 62.

185 Commonwealth, *Parliamentary Debates*, House of Representatives, 27 June 2001, 28641 (Daryl Williams).

186 Parliamentary Joint Committee on Intelligence and Security, Australian Parliament, *Inquiry into the Proscription of 'Terrorist Organisations' under the Australian Criminal Code* (2007).

187 *Criminal Code Act 1995* (Cth) s 100.1. For comment, see Greg Carne, 'Terror and the Ambit Claim: Security *Legislation Amendment (Terrorism) Act 2002* (Cth)' (2003) 14 *Public Law Review* 13.

188 *Criminal Code Act 1995* (Cth) s 100.2.

189 Designated 'Category D' offences by *Criminal Code Act 1995* (Cth) s 102.9.

190 Gregor Urbas, 'Cyberterrorism and Australian law' (2005) 8(1) *Internet Law Bulletin* 1, 7.

191 In *R v Lodhi* (2006) 199 FLR 364, the accused was charged under s 101 of the *Criminal Code Act 1995* (Cth) with possessing a thing connected with preparation for a terrorist act (a document concerning bomb-making), collecting documents connected with preparation for a terrorist act (two maps of Sydney's electrical supply system), making a document connected with the preparation for a terrorist act (aerial photos of Australian Defence Force establishments) and doing an act in preparation for a terrorist act (seeking information about the availability of bomb-making materials). He was found guilty of all but the third.

Jihad — Short Wise Rules and Organisational Structures that Concern Every Fighter and Mujahid Fighting against the Infidels was published online. Belal Khazaal was subsequently found guilty of knowingly making a document in preparation for a terrorist act, but the jury failed to reach a verdict with respect to attempting to incite others to commit terrorist acts.[192] One final matter involved a disgruntled engineer who remotely interfered with sewage control systems but lacked any political motivation.[193]

It is nonetheless 'certain' that Australian courts will experience difficulty when applying this legislation.[194] The terrorism offences under the *Criminal Code* are 'unprincipled and chaotic'.[195] In addition to capturing attacks deserving of the cyberterrorism label, the regime will also encompass acts of online political protest ('hacktivism') which do not warrant such severe sanctions.[196] Cyberterrorism is more than mere prankish hacking, mischievously disrupting nonessential services, or costly nuisances.[197] Cyberterrorism should therefore exclude activities which are incapable of occasioning death or bodily harm, significant infrastructure damage, severe property destruction, fear or serious economic loss.[198] Similar criticisms may be levelled at contemporary efforts to address cybercrime.

VII Cybercrime

'Cybercrime' or transnational computer crime is an unauthorised activity whereby any information and communications technology (computers, digital technology, the internet, communications systems or networks) is used to commit offences.[199] Cybercrime includes offences committed against computers or computer systems as well as technology enabled crime.[200] Targets include information brokers (such as credit reporting agencies or data aggregators), digital media manufacturers and distributors (such as the motion picture, recording and software industries) and online businesses.[201]

The preferred means for addressing cybercrime is international and national criminal law enforcement. In particular, the Council of Europe's *Convention on Cybercrime* establishes offences concerning the confidentiality, integrity and availability of computer data and systems ('hacking'), computer-related offences (forgery, computer fraud and identity theft),

---

192 *R v Khazaal* [2006] NSWSC 1061 (25 October 2006).

193 *R v Boden* [2002] QCA 164 (10 May 2002).

194 George Syrota, 'The Definition of 'Terrorist Act' in Part 5.3 of the Commonwealth Criminal Code' (2007) *University of Western Australia Law Review* 307, 341–7.

195 Bernadette McSherry, 'Terrorism Offences in the Criminal Code: Broadening the Boundaries of Australian Criminal Laws' (2004) 27 *University of New South Wales Law Journal* 354.

196 Keiran Hardy, 'Operation Titstorm: Hactivism of Cyberterrorism' (2010) 33 *University of New South Wales Law Journal* 474.

197 Maura Conway, 'Hackers as Terrorists? Why it Doesn't Compute' (2003) 12 *Computer Fraud and Security*, 10, 10–13.

198 Kathryn Kerr, Australian Computer Emergency Response Team ('AUSCERT'), *Putting Cyberterrorism into Context* (2003) <http://www.auscert.org.au/render.html?cid=2997&it=3552>.

199 See, for example, Abraham Sofaer and Seymour Goodman (eds), *The Transnational Dimension of Cyber Crime and Terrorism* (Hoover Institution Press, 2001); Shannon Hopkins, 'Cyber Crime Convention: A Positive Beginning to a Long Road Ahead' (2003) 2 *Journal of High Technology Law* 102; Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, *Background Paper for the Workshop on Crimes Related to the Computer Network*, UN Doc A/CONF.187/10 (2000).

200 House of Representatives Standing Committee on Communications, Australian Parliament, *Hackers, Fraudsters and Botnets: Tackling the Problem of Cyber Crime* (2010) [1.12].

201 Debra Yangt and Brian Hoffstadtft, 'Countering the Cyber-Crime Threat' (2006) 43 *American Criminal Law Review* 201.

content-related offences (including child pornography and racist websites) and copyright infringement.[202]

Australia is taking steps to accede to the *Convention on Cybercrime*.[203] The wisdom of accession is questionable.[204] Cybercrime in Australia is growing in scale, sophistication and success.[205] However, many existing legal concepts, particularly jurisdiction, are ill-adapted to meet the challenge and international law, which facilitates international co-operation for investigating cybercrime, is desirable.[206] Australian law is considered substantially compliant with the *Convention*.[207] Nevertheless, legislation has been introduced to implement Australia's obligations.[208] The *Cybercrime Legislation Amendment Bill 2011* (Cth) increases the powers of intelligence and law enforcement agencies to obtain electronic communications and enhances the ability of the Australian Federal Police (AFP) to exchange data with foreign counterparts.[209] Although the *Convention* does not itself contemplate human rights protections or judicial review, Australian law reputedly provides 'robust privacy safeguards and accountability mechanisms'.[210]

Commonwealth legislation provides law enforcement authorities with the power to secure electronic data in other respects.[211] For example, the *Criminal Code Act 1995* (Cth) contains a range of computer-related offences.[212] These measures reflect the principle of 'online-offline consistency' where the regulation of unlawful conduct in cyberspace is made consistent with the regulation of unlawful conduct in the physical realm.[213] Offences against pt 10.7 of the *Criminal Code Act 1995* (Cth) are investigated by the AFP's Cybercrime Operations Team. These offences include denial of service attacks, breaching computer systems or distributing malware which affects the Commonwealth's computer systems, computer networks of national interest or Australia's financial infrastructure. The AFP is legislatively mandated to counter cybercrime by maintaining a technological edge

---

202 *Convention on Cybercrime*, opened for signature 23 November 2001, 2296 UNTS 167; (entered into force 1 July 2004).

203 Robert McClelland and Stephen Smith, 'Australia to Accede to International Cybercrime Convention' (Joint Media Release, 30 April 2010).

204 Alana Maurushat, 'Australia's accession to the Cybercrime Convention: Is the Convention still Relevant in Combating Cybercrime in the Era of Botnets and Obfuscation Crime Tools?' (2010) 33 *University of New South Wales Law Journal* 431.

205 *Accession by Australia to the Convention on Cybercrime* [2011] ATNIF 5 [9].

206 Attorney-General's Department, *Australia's Proposed Accession to the Council of Europe Convention on Cybercrime* (2011) 3.

207 For an article by article commentary on Australia's compliance with the *Convention*, see Attorney-General's Department, *Outline of the Articles of the Council of Europe Convention on Cybercrime and Australia's Compliance* (2011).

208 The *Cybercrime Legislation Amendment Bill 2011* (Cth) was introduced on 22 June 2011 and passed the House of Representatives. The Bill was passed in the Senate on 22 August 2012, with the government adopting all but one of the recommendations made by the Joint Select Committee on Cyber-Safety: Attorney-General's Department, 'New Laws in the Fight against Cyber-crime', (Media Release, 22 August 2012).

209 Joint Select Committee on Cyber-Safety, Australian Parliament, *Review of the Cybercrime Legislation Amendment Bill 2011* (2011).

210 Joint Standing Committee on Treaties, Australian Parliament, *Report No 116* (2011) [11.62].

211 For example, *Crimes Act 1914* (Cth) pt IAA allows law enforcement officers to search and seize electronic data. The *Telecommunications (Interception and Access) Act 1979* (Cth) permits the interception of communications and access to historic and real time data. See also the *Surveillance Devices Act 2004* (Cth).

212 These include hacking, malware and denial of service attacks with intent to commit a serious offence (s 477.1(1) and (4)), malware infections (s 477.2), denial of service attacks (s 477.3), hacking password-protected data (s 478.1), damaging data held on a mobile device owned or leased by the Commonwealth (s 478.2), possession or control of data (s 478.3) and the production and supply of data (s 478.4).

213 Model Criminal Code Officers Committee, *Report on the Model Criminal Code* (2001) 94.

over criminals.[214] It is currently investigating a 2009 cyber operation and sophisticated cyber intrusions into government and private networks.[215]

Cybercrime is considered 'highly prevalent' within Australia.[216] In 2009–10, Australian businesses received nearly A$143 billion worth of internet orders.[217] The risk of cybercrime to Australia's economy is estimated at more than one billion dollars per year.[218] The Commonwealth is formulating a law enforcement strategy that entails closer coordination with law enforcement agencies from other states.[219] The Attorney Generals of Canada, the US, the UK, New Zealand and Australia will develop a joint action plan to combat cybercrime.[220] They have also agreed to support the work of their Foreign Ministers 'to develop international cyber principles to guide [the] behaviour of countries'.[221]

At one end of the criminal law enforcement spectrum is intelligence-gathering. Cyber activity can be situated within the existing legal frameworks addressing espionage.[222] Espionage requires a 'collecting' state to obtain, deliver, transmit, communicate or receive information concerning the national defence of a 'victim' state. The UK has experienced attempts by hostile foreign intelligence agencies to acquire data from defence contractors and government computers have been deliberately infected with viruses.[223] Foreign intelligence services have similarly hacked into the computer systems of private military contractors with a view to obtaining sensitive information concerning US military hardware.[224]

In Australia, ASIO anticipates increasing 'non-traditional' espionage threats as cyber security becomes a growing concern.[225] Several thousand emails, including from the Prime Minister and the Defence and Foreign Ministers, were appropriated during a sustained cyber attack.[226] The parliamentary computers of 10 other federal Ministers have been hacked, their emails accessed and passwords stolen.[227] The aph.gov.au email network was compromised such that emails between Ministers and Australian resource corporations operating in China were intercepted.[228] Indeed, China and its private proxies are believed

---

214 Ministerial Direction issued pursuant to *Australian Federal Police Act 1979* (Cth) s 37(2).

215 Ian McKenzie, Defence Signals Directorate, 'Speech by Mr Ian McKenzie Director, Defence Signals Directorate 26 February 2010' (Speech delievered at the National Security Australia 2010 Conference, 26 February 2010) 11.

216 House of Representatives Standing Committee on Communications, Australian Parliament, *Hackers, Fraudsters and Botnets: Tackling the Problem of Cyber Crime* (2010) [2.84].

217 Australian Bureau of Statistics, *Internet Activity* (2010).

218 Australian Government, Department of the Prime Minister and Cabinet, *Connecting with Confidence: Optimising Australia's Digital Future* (2011) 5.

219 Australian Government, *Government Response to the House of Representatives Standing Committee on Communications Report on the Inquiry into Cyber Crime: Hackers, Fraudsters and Botnets: Tackling the Problem of Cyber Crime* (2010) 13.

220 Robert McClelland, Attorney-General (Cth), 'Key Allies Focus on Cyber Crime at Sydney "Quintet"' (Press Release, 5 July 2011).

221 Quintet of Attorneys General, *Communique*, Sydney (2011).

222 Gerald O'Harat, 'Cyber-Espionage: A Growing Threat to the American Economy' (2010) 19 *Communications Law Conspectus* 241.

223 'William Hague: UK is Under Cyber-attack', *BBC News* (online), 4 February 2011 <http://www.bbc.co.uk/news/uk-12371056>.

224 'Pentagon on Cyber War Footing After Hacker Raid', *Sydney Morning Herald* (Sydney), 16–17 July 2011, 14.

225 'Security in Government 2009', *Asia Pacific Defence Reporter*, 2009, 16.

226 Commonwealth Parliamentary Library, *Flagpost: Meeting the Challenges of Cyber-Security* (31 March 2011).

227 'You May Not Know It — But We Are at War', *The Daily Telegraph* (Sydney), 16 April 2011, 40.

228 'Cyber Attack in Canberra', *Sydney Morning Herald* (Sydney), 16–17 April 2011, 7.

routinely to conduct cyber espionage immediately before intergovernmental negotiations.[229]

The extent of internet-enabled espionage as a rapidly-growing threat to Australian interests is becoming increasingly apparent.[230] Attempts by spies, criminals or hackers to infiltrate government computer networks are characterised as threats to national security.[231] ASIO's Director-General believes that an increasingly persistent threat to Australia's security originates from abuse or exploitation of the internet's vulnerabilities by both state and non-state actors.[232] The internet is a vehicle for the covert extraction of confidential information to the detriment of both economic, political or defence interests and individual privacy. Hostile intelligence agencies have a 'beyond-the-horizon' capability such that they need not leave their own shores in order to target information stored on government, business or personal computers.[233] A recent audit of four government agencies for the protection and security of their electronic information including user passwords identified significant weaknesses and deficiencies.[234] Australian military and intelligence agencies are attractive targets for foreign states, with Australia perceived as a potential alternative source of sensitive defence, intelligence or diplomatic information shared by our allies.[235] ASIO is therefore continuing to build its operational capability to address cyber espionage.[236]

It must nevertheless be acknowledged that criminal law is of limited utility.[237] Imperfect and inadequate national legal regimes are one obstacle to effective solutions.[238] The pace of transactions and transnational nature of cybercrime render traditional investigative practices 'redundant'.[239] Cybercrime has evolved against a static international legal framework. Electronic evidence is difficult to acquire in a timely manner with information exchange being limited to states with developed infrastructure. Intergovernmental agreements must resolve a range of issues including jurisdiction, cooperation in the investigation, prosecution or punishment of offenders, evidentiary admissibility and recognising penalties served in other jurisdictions.[240] In common with the three legal paradigms considered above, there are several additional questions which additionally require a distinctive Australian perspective.

---

229 'War in the Shadows', *Sydney Morning Herald News Review* (Sydney), 24–5 September 2011, 1, 6.

230 ASIO, *Annual Report* (2008–09).

231 'Hackers Attempted to Infiltrate Government Networks', *Sydney Morning Herald* (Sydney), 7 March 2008.

232 Presentation before Senate Legal and Constitutional Affairs Legislation Committee, Australian Parliament, 25 May 2011, 70 (David Irvine, Director-General of Security, ASIO).

233 ASIO, *Annual Report* (2009–10).

234 Australian National Audit Office, *Performance Audit Report into the Protection and Security of Electronic Information Held by Australian Government Agencies*, Audit Report No 33 (2010–11).

235 Kevin Rudd, *National Security Statement to Parliament* (2008).

236 ASIO, *Portfolio Budget Statements* (2010–11).

237 American Bar Association Standing Committee on Law and National Security and National Strategy Forum, *National Security Threats in Cyberspace, Report of a Workshop* (2009), 18 <http://www.abanet.org/natsecurity/threats_%20in-cyberspace.pdf>.

238 Mrinalini Singh and Shivam Singh, 'Cyber Crime Convention and Trans Border Criminality' (2007) 1 *Masaryk University Journal of Law and Technology* 53.

239 Australian Federal Police, *Response to the Public Discussion Paper: Connecting with Confidence — Optimising Australia's Digital Future* (2011) 6–7.

240 *Manual on the Prevention and Control of Computer-Related Crime*, Eighth United Nations Congress, UN Doc ST/ESA/SER.M/43-44 (1994) 4.

VIII Some Questions for Australia's International Lawyers

It is clear that international norms on cyberspace are developing rapidly in several different fields. A Commonwealth discussion paper listed international trade, intellectual property and internet governance as additional policy arenas.[241] The greatest threat to a secure digital environment was identified as competition and conflict in cyberspace between states. An understanding between them concerning responsible online behaviour had to be developed.

Although it may be thought axiomatic that law follows technology, being reactive rather than proactive, it is clear that there are already several legal principles applicable to some aspects of cyber activity. However, the relevant international legal rules have been developed for different types of situations or events, whereas ensuring cyber security involves 'additional complicating factors'.[242] Nor is the online environment currently governed by any holistic or coherent international legal framework. There is a clear need for the international community to construct appropriate 'rules of the road'.

Valuable contributions on these issues can be made by Australia's military, government and international lawyers who appreciate Australia's distinctive national interests. It is incumbent on Australia to contribute to a uniform international criminal law that addresses cybercrime and develop new rules of engagement for cyber warfare.[243] Australia already recognises that cyber threats exist between states, corporations and individuals both locally and overseas.[244]

An initial challenge is information gathering. Cyber activities range in nature and severity. They include web vandalism (deactivating or defacing websites), disinformation campaigns (spreading rhetoric to influence opinions), infiltrating public or private information networks to procure classified data (cyber espionage), causing disruption by blocking, intercepting or polluting communications, and attacking critical national infrastructure which physically endangers lives and property. The motivation of perpetrators varies: combatants pursue military objectives during cyber conflict, criminals seek financial gain through cybercrime, cyber terrorists compel others to capitulate to political demands and cyber spies seek confidential information. Notwithstanding the use of identical or similar techniques, the nature of the activity turns upon a specific intent which may prove difficult to discern in cyberspace.

Individuals, whether naive hackers or dedicated terrorists, are likely to consider cyber activities to be an attractive prospect.[245] There are many users, tracking is difficult, systems are unregulated, anonymity is ensured, actions are easy, fast and inexpensive to execute and real-world harm or significant confusion and cost can result. Lawmakers are increasingly aware of the growing technical capability of individuals and more acquainted with hacker

---

241 Australian Government, Department of the Prime Minister and Cabinet, *Connecting with Confidence: Optimising Australia's Digital Future* (2011) 22.

242 Russell Buchan and Nicholas Tsagourias, 'Cyber War and International Law' (2012) 17 *Journal of Conflict and Security Law* 183.

243 Gary Waters, Desmond Ball and Ian Dudgeon, *Australia and Cyber-warfare* (ANU E Press, 2008) 108, 134.

244 Attorney-General's Department, *Optimising Australia's Response to the Cyber Challenge* (2011).

245 Jerrold Post, 'From Car Bombs to Logic Bombs: The Growing Threat from Information Terrorism' (2000) 12(2) *Terrorism and Political Violence* 97.

tools.[246] Such developments reflect a truism that information societies enable non-state actors to challenge state authority.[247]

Governments confront several obstacles when countering the use of information and communications technology by malevolent actors: the challenge of tracing communications, the absence of harmonised laws or investigative procedures and inadequate or ineffective information-sharing.[248] International lawyers will have to grapple, for example, with complex jurisdictional questions.[249] The effects doctrine and territorial and universal jurisdiction are the preferred bases for national-level prosecutions.[250] Critical to this end is overcoming the technical problem of attribution.[251] It may be difficult to determine when an offensive cyber operation has begun, the identity of responsible actors, what state or organisation they represent (particularly where communications are rerouted) and identifying the intended purpose and effects.

To meet these challenges, the US Department of Homeland Security sponsors large-scale cyber security exercises. In 2008, 56 Australian government and private sector organisations participated in 'Cyber Storm II' alongside government and non-government organisations from the US, Canada, New Zealand and the UK. Among the conclusions was that crisis management arrangements must be regularly reviewed and tested, be tailored to incorporate multiple inter-dependencies and be informed by clear escalation thresholds.[252] 'Cyber Storm III' (2010) reiterated a key finding that testing offered an opportunity to identify gaps and revise processes.[253] However, even the most sophisticated computer security measures cannot completely protect a state's critical electronic systems.[254]

For international lawyers, cyber activities pose several 'dilemmas'.[255] The question canvassed in this article is whether existing legal paradigms are sufficient or whether new laws are required. The contemporary international legal framework for regulating cyber activity is 'ill-informed, undeveloped and highly uncertain'.[256] In 1999, the US Department of Defense concluded that the international community was unlikely to produce any

---

246 Clay Wilson, 'Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress' (RL32114, US Congressional Research Service, Report for US Congress, 29 January 2008) 21, 37.

247 Meltem Mtftijler-Bac, 'Information Societies, New Terrorism: Its Impact on International Politics' (2007) 3 *Review of International Law and Politics* 130, 138.

248 Jody Westby, 'Countering Terrorism with Cyber Security' (2006–07) 47 *Jurimetrics* 297.

249 See, for example, Darrel Menthe, 'Jurisdiction in Cyberspace: A Theory of International Spaces' (1997–98) 4 *Michigan Telecommunications and Technology Law Review* 69.

250 Kelly Gable, 'Cyber-Apocalypse Now: Securing the Internet Against Cyberterrorism and Using Universal Jurisdiction as a Deterrent' (2010) 43 *Vanderbilt Journal of Transnational Law* 57; Jennifer Rho, 'Blackbeards of the Twenty-First Century: Holding Cybercriminals Liable Under the Alien Tort Statute' (2007) 7 *Chicago Journal of International Law* 695.

251 Herbert Lin, 'Offensive Cyber Operations and the Use of Force' (2010) 4 *Journal of National Security Law and Policy* 63, 77.

252 Attorney Generals' Department, Security and Critical Infrastructure Division, *Cyber Storm II National Cyber Security Exercise: Final Report* (2008).

253 Jakeman Business Solutions Pty Ltd, *Cyber Storm III, Cyber Security Exercise* (27–30 September 2010).

254 Andrew Colarik, *Cyberterrorism: Political and Economic Implications* (2006) 163.

255 Jyotirmo Banerjee, 'Cyber Warfare and the Dilemmas of International Law' (2007) 1(3) *ICFAI Journal of International Relations* 36.

256 William Owens, Kenneth Dam and Herbert Lin (eds), *Technology, Policy, Law and Ethics Regarding US Acquisition and Use of Cyberattack Capabilities*, (National Academies Press, 2009).

coherent body of legal rules applicable to cyber conflict.[257] That conclusion remains apposite for the foreseeable future.

A strictly territorial approach to law-making and criminal law enforcement will prove ineffective for tackling cyber security. One option is strengthening the much-overlooked telecommunications and information technology conventions. For example, operating radio stations cannot cause 'harmful interference' to the radio services or communications of other states.[258] States must also identify those stations which transmit false or deceptive distress, urgency, safety or identification signals.[259] The international community could correspondingly encourage national efforts to enhance existing legal frameworks on information and communications technology.[260]

Another possibility is to apply existing rules by analogy to a new operational environment.[261] For example, several commentators consider that the existing paradigm of arts 2(4) and 51 of the UN Charter can be applied to cyber attack.[262] Reference is made to the traditional criteria for kinetic encounters: scope, intensity and duration. The contrary view is that the existing rules regulating armed conflict and the conduct of war are insufficient, uncertain and too complex to encompass cyber operations.[263] The use of force paradigm therefore applies 'only with difficulty'.[264] The NATO-accredited Cooperative Cyber Defence Centre of Excellence in Estonia, for example, considered it 'highly problematic' to apply international law on the use of force to the Georgian cyber attacks because state participation and 'grave effect' were not apparent.[265] Clarity is also desirable on the kinds of information warfare techniques which constitute an 'armed attack' and permit self-defence measures. Additional questions include whether the concepts of 'armed attack' and self-defence are applicable to non-state actors. The answer currently appears to

---

257 Office of General Counsel, Department of Defence, *An Assessment of International Legal Issues in Information Operations* (1999) 15.

258 *International Telecommunication Convention* ('ITC'), signed 21 December 1959, 12 UST 1761, TIAS 4892 (entered into force 1 May 1961) art 35.

259 ITC art 37. States Parties may cut-off private telecommunications which appear dangerous to national security or contrary to national law, public order or decency (art 19(2)) and suspend an international telecommunication service for an indefinite time, either generally or only for certain relations or for certain kinds of correspondence, outgoing, incoming or in transit (art 20).

260 Eneken Tikk, Kadri Kaska and Liis Vihul, *International Cyber Incidents: Legal Considerations* (Cooperative Cyber Defence Centre of Excellence, 2010) 94, 99, 103.

261 Scott Shackelford, 'From Nuclear War to Net War: Analogizing Cyber Attacks in International Law' (2009) 27(1) *Berkley Journal of International Law* 246.

262 See, for example, Marco Roscini, 'World Wide Warfare — Jus ad Bellum and the Use of Cyber Force' (2010) 14 *Max Planck Yearbook of United Nations Law* 85, 105; Arie Schaap, 'Cyber Warfare Operations: Development and Use Under International Law' (2009) 64(1) *Air Force Law Review* 121, 147–8.

263 Duncan Hollis, 'Why States Need an International Law for Information Operations' (2007) 11 *Lewis and Clark Law Review* 1023.

264 Emily Haslam, 'Information Warfare: Technological Changes and International Law' (2000) 5 *Journal of Conflict and Security Law* 157, 165.

265 Stephen Korns and Joshua Kastenberg, 'Georgia's Cyber Left Hook' (2008–09) 38(4) *Parameters — US Army War College Quarterly* 60, 63 <http://www.carlisle.army.mil/usawc/parameters/08winter/korns.pdf>.

be 'no'.[266] One consequential argument is that the 'use of force' definition should be expanded to ensure that all forms of cyber attack are prohibited by international law.[267]

The emergence of 'new wars' and asymmetric tactics render the extension of international humanitarian law to non-state actors similarly challenging.[268] Again, one view is that existing international humanitarian law is sufficient to address cyber conflict.[269] Its well-accepted principles apply whenever cyber attacks are ascribed to a state, the attacks are not sporadic in nature and are intended to or will foreseeably cause injury, death, damage or destruction to non-military objectives. Proposed new agreements for regulating computer network attacks are rejected as 'unnecessary' because commanders simply apply orthodox analysis to the new technology.[270] For example, the US Department of Defense considers that international humanitarian law 'is probably the single area of international law in which current legal obligations can be applied with the greatest confidence to information operations'.[271] It has rebuffed calls for new rules addressing information operations as 'premature' because a process of extrapolation from the existing legal framework 'appears to be reasonably predictable'.[272] However, it then concludes that cyber soldiers forfeit combatant privileges because they do not readily identify themselves by wearing uniforms or carrying arms openly. Private internet users who initiate cyber conflict can anticipate being classified as 'unlawful combatants'.[273]

The contrary position of course is that resort to the Geneva Conventions is 'detached from reality' if those legal standards are thought applicable to cyber hostilities.[274] Those instruments offer 'outdated or inapposite assumptions' concerning civilian participation in cyber conflict such that their application 'either steers State practice into empty formalism or excessively constrains States' options — both of which are proven to produce only contempt for the Geneva Conventions'.[275]

A third option is explicitly regulating cyber activity.[276] One frequent proposal is adopting an International Convention to Regulate the Use of Information Systems in Armed Conflict.[277] However, the international community does not presently support

---

266 *Case concerning Military Activities in and Against Nicaragua (Nicaragua v United States) (Merits)* [1986] ICJ Rep 14 [195]; *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory (Advisory Opinion)* [2004] ICJ Rep 136, 139 and Declaration of Judge Buergenthal [6].

267 Jason Barkham, 'Information Warfare and International Law on the Use of Force' (2001) 34 *International Law and Politics* 57, 59.

268 William Banks (ed), *New Battlefields, Old Law: Critical Debates in Asymmetric Warfare* (Columbia University Press, 2011).

269 Michael Schmitt, 'Wired Warfare: Computer Network Attack and the Jus in Bello', in Michael Schmitt and Brian O'Donnell (eds), *Computer Network Attack and International Law* (Naval War College, 2002) 187.

270 Eric Jensen, 'Unexpected Consequences from Knock-on Effects: A Different Standard for Computer Network Operations?' (2003) 18 *American University International Law Review* 1145, 1149.

271 US Department of Defense, Office of General Counsel, *An Assessment of International Legal Issues in Information Operations* (1999) 11, 14.

272 Ibid.

273 Mark Hoffman, 'The Legal Status and Responsibilities of Private Internet Users Under the Law of Armed Conflict: A Primer for the Unwary on the Shape of the Law to Come' (2003) 2 *Washington University Global Studies Law Review* 415.

274 Sean Watts, 'Low-Intensity Computer Network Attack and Self-Defense' (2011) 87 *International Law Studies* 59.

275 Sean Watts, 'Combatant Status and Computer Network Attack' (2010) 50 *Virginia Journal of International Law* 391, 396.

276 Stuart Malawer, 'Cyber Warfare: Law and Policy Proposals for US and Global Governance' (2010) 58 *Virginia Lawyer* 28, 30.

277 Davis Brown, 'A Proposal for an International Convention to Regulate the Use of Information Systems in Armed Conflict' (2006) 47 *Harvard International Law Journal* 179, 214; Philip Johnson, 'Is it Time for a Treaty on

introducing a new regime. In 2000, Russia submitted a draft resolution entitled 'Principles of International Information Security' to prohibit creating and using tools for a cyber attack.[278] States were unresponsive and only a few favoured commencing negotiations. Instead, the UN General Assembly called upon states to consider existing and potential threats to information security.[279] Article 2(4) is evidently a weak constraint on offensive cyber attacks and States may prefer both legal ambiguity and clarity within the policy arenas of military power, intelligence gathering and law enforcement depending upon their comparative advantage.[280] The divergent strategic interests of states will pull their preferred doctrinal interpretations or aspirations in different directions and further impeding the formation of a stable international consensus.[281] The US, for example, should not conclude novel legal regimes which 'unnecessarily hamper' its predominance as a digital power.[282]

An intermediate position involves pursuing a criminal law enforcement approach rather than a military one until appropriate 'rules of engagement' are formulated.[283] Characterising cyber activity as criminal in nature offers the prospect to states of subjecting offenders to their national law. Domestic law enforcement rather than military coercion is also one solution insofar as self-defence measures cannot be employed against non-state actors.

A fifth approach is to pool elements from each regime. A comprehensive national security strategy for cyberspace involves international diplomacy, military doctrine, economic policy tools and the participation of national intelligence and law enforcement communities.[284] There is self-evident scope for the complementary application of overlapping regimes.

For example, many of the offences in the *Convention on Cybercrime* are applicable to cyberterrorism.[285] Governments continue to revisit the terrorism definition to address newly emergent threats including bioterrorism and cyberterrorism.[286] However, the resulting interpretative difficulties arising from that definition are best avoided because prosecutions become more prolonged.[287] Although national responses to enhance cyber

---

Information Warfare?' in Michael Schmitt and Brian O'Donnell (eds), *Computer Network Attack and International Law* (Naval War College, 2002) 439.

278 *Letter Dated 23 September 1998 from the Permanent Representative of the Russian Federation to the UN Addressed to the Secretary-General*, UN Doc A/C.1/53/3 (23 September 1998); *Developments in the Field of Information and Telecommunications in the Context of International Security - Report of the Secretary-General*, UN Doc A/54/213 (10 August 1999) 8.

279 *Deveopments in the Field of Information and Telecommunications in the Context of International Security*, GA Res 53/70, UN GAOR 53rd sess, 79th plen mtg, UN Doc A/RES/53/70 (4 January 1999) 2.

280 Matthew Waxman, 'Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)' (2011) 36 *Yale Journal of International Law* 421, 427, 447.

281 Ibid 454.

282 Charles Dunlap, 'Meeting the Challenge of Cyberterrorism: Defining the Military Role in a Democracy' (2002) 76 *International Law Studies* 353, 362–3.

283 Charles Dunlap, 'Towards a Cyberspace Legal Regime in the Twenty-First Century: Considerations for American Cyber-Warriors' (2008–09) 87 *Nebraska Law Review* 712, 720.

284 Center for Strategic and International Studies, *Securing Cyberspace: A Report of the CSIS Commission on Cybersecurity for the 44th Presidency* (2008), 1 <http://csis.org/files/media/csis/pubs/081208_securingcyberspace_44.pdf>.

285 Aviv Cohen, 'Cyberterrorism: Are We Legally Ready?' (2010) 9 *Journal of International Business and Law* 1.

286 Ben Golder and George Williams, 'What is 'Terrorism'? Problems of Legal Definition' (2004) 27 *University of New South Wales Law Journal* 270, 293.

287 Parliamentary Joint Committee on Intelligence and Security, *Review of Security and Counter-Terrorism Legislation* (2006) [6.12].

security commonly include legislation,[288] combating terrorism in the digital age produces a clash of legal doctrines. Technology, state power and civil liberties are typically subverted in favour of national security.[289] The indeterminacy of terrorism suggests that the relevant laws require reformation or clarification.[290] Imposing a duty upon sanctuary states to prevent cyber attacks springs from a call for international lawyers to design imaginative ways of tackling this problem: '[i]f not, the law will become obsolete and meaningless to the States that need its guidance'.[291]

On a cautionary note, international lawyers must be mindful of several considerations. One is the prospect of overregulation. The fallacy that cybercrime is unique has encouraged legislation which is 'ill-considered and draconian': 'a pastiche of complacency, appropriate reaction, and overzealous statutory responses'.[292] The enforcement deficit is not due to a lack of legal powers because the 'spectre of over-criminalisation continues to lurk in the fine print'.[293]

Another cross-cutting theme is how to ensure respect for human rights and fundamental freedoms. Greater state control over information and communications technology might inspire 'big brother' regimes.[294] The European Union has developed more effective legislation to counter terrorist websites than the US because the right to freedom of speech is upheld by European courts with less vigour.[295] Computer systems create individual dossiers constructed upon electronic trails left in cyberspace. This 'dataveillance' enables governments to scrutinize individual conduct under the guise of national security. Such an approach could foster governmental abuse of civil liberties[296] including intruding upon individual privacy.[297]

Whichever approach is ultimately adopted, the importance of the rule of law in cyberspace, including the ability to hold malevolent actors to account, must be affirmed.[298] The US optimistically considers that many existing international legal principles apply in cyberspace.[299] Australia's international lawyers could push that line but should proceed

---

288 Tara Raghavan, 'In fear of Cyberterrorism: An Analysis of the Congressional response' (2003) *University of Illinois Journal of Law Technology & Policy* 297, 298.

289 Harvey Rishikof, 'Combating Terrorism in the Digital Age: A Clash of Doctrines: The Frontier of Sovereignty, National Security and Citizenship, the Fourth Amendment, Technology and Shifting Legal Borders' (2008–09) 78 *Mississippi Law Journal* 381, 425.

290 Nicola McGarrity, '"Testing' Our Counter-Terrorism Laws: the Prosecution of Individuals for Terrorism Offences in Australia' (2010) 34 *Criminal Law Journal* 92.

291 Matthew Sklerov, 'Solving the Dilemma of State Responses to Cyberattacks: A Justification for the Use of Active Defenses Against States Which Neglect Their Duty to Prevent' (2009) 201 *Military Law Review* 1, 2.

292 Simon Bronitt and Miriam Gani, 'Shifting Boundaries of Cybercrime: from Computer Hacking to Cyberterrorism' (2003) 27 *Criminal Law Journal* 303, 316.

293 Ibid 304.

294 Andrei Medushevsky, 'Terrorism and the State: Limits of Self-protection (the Parameters of Internet (Runet) Regulation)' (2007–08) 29 *Cardozo Law Review* 21.

295 Megan Healy, 'How the Legal Regimes of the European Union and the United States Approach Islamic Terrorist Web Sites: A Comparative Analysis' (2009-2010) 84 *Tulane Law Review* 165.

296 Paul Rosenzweig, 'Privacy and Counter-Terrorism: The Pervasiveness of Data' (2009–10) 42 *Case Western Reserve Journal of International Law* 625.

297 Hearing before the Subcommittee on Technology, Terrorism and Government Information of the Senate Committee on the Judiciary, US Congress, *Cyber Attacks: The National Protection Plan and Its Privacy Implications*, Hearing on SR 106-889, 106th Cong (1 February 2000) 11.

298 Executive Office of the President of the United States, *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World* (2011) 5.

299 Ibid [16].

cautiously. The prevailing consensus is that cyber threats are real and growing. However, critical national infrastructure may be sufficiently robust such that functions can be rapidly restored following a cyber attack. Water system failures, power outages, air traffic disruptions and other scenarios which deny customer service occur nowadays without significantly affecting national security. Multiple targets would have to be affected over long time periods in order to create havoc. Activities such as cyber espionage, cybercrime, identity theft or credit card fraud may not warrant the 'turbo metaphor' of cyber war and 'heated rhetoric' could propel policy in inappropriate directions.[300]

IX Conclusions

This article is confined to examining four international legal paradigms, with an eye cast to protecting Australian cyberspace. Each paradigm carries its own particular set of questions, challenges and imperfections. Cyber activity has exposed the inadequacies of the existing patchwork offered by these regimes. The absence of regulation or penalties for conducting cyber activity currently advantages some states over others. Technological developments have put into flux the distribution of state power. The failure of international legal regimes to keep abreast relegates familiar standards to irrelevance or provokes legal fictions detached from reality. A coherent and comprehensive approach to cyber activity does not exist and an overarching organisational principle is yet to emerge. It is, however, clear that states have recognised the challenge, albeit with a view to addressing national security threats in a technology-enabled world. Effective cooperation at the inter- and intra-governmental levels and between states and private actors seems part of the solution.

This milieu represents an opportunity for further contributions in the military, anti-terrorism and law enforcement fields. Australia's international lawyers need to start thoroughly researching, assessing and creatively addressing a range of issues. In particular, what interpretative approaches are most appropriate for Australian conditions and, given current policy objectives, how can Australia's freedom of action be extended or curtailed consistent with its broader security strategy. To ensure cyber security, a singular strategy which contemplates the use or threat to use military force by way of a Cold War-style deterrence strategy is arguably wrong.[301] A 2011 Commonwealth discussion paper concluded that Australia must actively engage in all relevant fora to ensure that national interests and values are reflected in the emerging international norms on cyberspace and so that Australians can take full advantage of the opportunities afforded by the digital economy.[302]

Australia's final Cyber White Paper will be released shortly. Australian policy is undergoing rapid evolution on several fronts. Some developments uncritically follow US leadership. The existing literature is predominantly US-orientated, with European material available to a lesser extent. Contemporary Australian perspectives are largely limited to terrorism. On whether Australia's international lawyers are ready to protect Australian cyberspace, the answer by any measure would have to be: 'not yet'.

---

300 Maggie Shiels, 'Cyber War Threat Exaggerated Claims Security Expert', *BBC News* (online), 16 February 2011 <http://www.bbc.co.uk/news/technology-12473809>.

301 Mary Ellen O'Connell, 'Cyber Security Without Cyber War' (2012) 17(2) *Journal of Conflict and Security Law* 187, 199, 209.

302 Australian Government, Department of the Prime Minister and Cabinet, *Connecting with Confidence: Optimising Australia's Digital Future* (2011) 22.