Privacy, Security and the Cyber Dilemma

An Examination of New Zealand's Response to the Rising Threat of Cyber-attack

By Richard Gordon

A Thesis

submitted to the Victoria University of Wellington

in partial fulfilment of the requirements for the degree of Master of International
Relations (MIR)

School of History, Philosophy, Political Science and International Relations

Victoria University of Wellington

2014

“The Internet is a prime example of how terrorists can behave in a truly transnational way; in response, States need to think and function in an equally transnational manner.”

Ban Ki-moon

Secretary-General of the United Nations

Cyber-attacks present significant challenges to a modern, globalised world. Progressively used by criminal and terrorist organisations to attack or victimise non-state actors, governments are increasingly forced to pursue cyber-security strategies to ensure the security of their citizens and private sectors. An examination of New Zealand's response to the threat of cyber-attacks shows that successive governments have taken steps to enhance New Zealand's domestic cyber-security capacity and international cyber-security partnerships. These steps have been highly contentious where they have resulted in greater domestic surveillance capabilities. Despite this, New Zealand has enacted significant oversight mechanisms that provide reassurance that the New Zealand Government is mindful of the delicate steps it must take to maintain an appropriate balance between privacy and security.

Table of Contents

Section One: Small State Responses to Cyber Threats

1. Introduction	5
2. Cyber-Security and Mass Surveillance	7
3. Why Does Cyber Matter?	8
4. Definitions	10
5. Cyber-Attack Categories	11
6. Characteristics of Cyberspace	14
7. Asymmetric Attack	17
8. Methods of State Surveillance	18
9. Social Contract	19
10. Privacy	21
11. The Rise of Big Data	22
12. Turning off Access	24
13. Deterrence	26
14. Security Frameworks	27

Section Two: New Zealand's Response to Cyber Threats

15. New Zealand and the Rise of Cyber	30
16. New Zealand Cyber-Security Strategies	34
17. New Zealand's Security Legislation	37
18. Finding a Balance between Privacy and Security	60
19. Conclusion	62
20. Bibliography	65

Section One: Small State Responses to Cyber Threats

1. Introduction

The increasing globalisation of the world has intensified the debate concerning the balance between privacy and security. This has been especially true following the unauthorised release of highly classified intelligence by United States (US) intelligence contractor Edward Snowden. Snowden, reportedly inspired by the actions of fellow ‘whistle-blower’ Bradley (Chelsea) Manning¹, revealed a massive programme of US National Security Agency (NSA) surveillance on US and foreign citizens. Exploiting data collected from electronic databases, the Internet and cellular companies, the US was conducting what has been called an “indiscriminate and arbitrary invasion [of privacy] through the systematic and high-tech collection and retention of personal data on virtually every single [US] citizen for purposes of querying it and analysing it without judicial approval.”² These events have occurred at a time when the world is experiencing the unprecedented growth of personal data in government and online databases, which is in itself transforming the characterisation of private and public information. This has reignited a debate calling into question the extent of government access to private information and the transparency by which governments acquire and analyse this information.

At the centre of this debate is the human right to privacy upon which modern societies are built. Privacy is the ability of an individual or group to protect information about themselves and to have some ability to control the release or use of this information. The concept and boundaries of privacy are readily changing, driven by the rapid growth of ‘big data’ – data widely available online through such mediums as social media, eGovernment and data mining sites. Sophisticated algorithms allow complex analysis of this data to determine the habits, preferences and networks of billions of individuals, the results of which can be used by government and commercial organisations for national security and commercial priorities.

¹ The Guardian (10 June 2013) Greenwald, Glenn, Ewen MacAskill, and Laura Poitras. “Edward Snowden: The Whistleblower behind the NSA Surveillance Revelations.” *The Guardian*, 10 June 2013. Accessed January 12, 2014. <http://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance>.

² New York Daily News (2013) McCarthy Tom, “‘This overreach is unacceptable’: the case against NSA bulk collection.” *The Guardian*, 23 January 2014. Accessed January 12, 2014, <http://www.theguardian.com/world/2014/jan/23/nsa-bulk-collection-chorus-surveillance-under-patriot-act>

This thesis will be in two sections. Section One will examine the challenges posed to the security of state and non-state actors by the rise of cyberspace. Drawing on the extensive cyberspace literature available, it will be demonstrated that the nature of cyberspace has shifted the burden of security from the state to the individual. As one of the foremost goals of any state is to protect its citizens, this thesis will then explore the security responses available that seek to enhance the security of the state and its citizens while protecting the inherent rights of a modern democratic state. By doing so, this thesis will satisfy the question of why intelligence collection is important to modern states. Section Two will examine the expansion of state powers of surveillance over New Zealanders, and explore how this has affected New Zealand's balance between privacy and security. The thesis will focus specifically on the period following the attacks on the World Trade Centre in New York in 2001 as a point when the importance of the balance between privacy and security has been reemphasised for the modern age. This thesis will also examine New Zealand's tolerance as a society for increased surveillance powers by the state and address the question: "Why is security important in New Zealand and what is being done to maintain an appropriate balance between privacy and security?"

New Zealand makes an interesting case study in understanding the impact that technology and globalisation has on the balance between national security of states and individual privacy. An increasingly globalised and Internet-connected world brings New Zealand many advantages and opportunities. In parallel, globalisation also reduces the advantage of New Zealand's physical isolation, thereby intensifying the threat to New Zealand from state and non-state actors. The rise of the Internet has presented new challenges in countering espionage and transnational crime, which allow state and non-state actors to remotely exploit vulnerabilities in New Zealand's information and communications systems. Internationally there has been a growing escalation of cyber activities,³ and New Zealand remains equally at risk of falling victim to these activities as any other globally connected state. New Zealand has pursued security strategies and enacted legislation that seek to protect its citizens and interests from harm.

³ Ministry for Communications and Information Technology. "New Zealand's Cyber Security Strategy: June 2011". (Wellington: Ministry for Communications and Information Technology, 7 June 2011), p 1

2. Cyber-Security and Mass Surveillance

Former NSA contractor Edward Snowden will go down in history as one of America's most significant whistle-blowers. In 2013, Snowden disclosed a sizeable number of classified NSA documents, revealing the details and targets of a covert mass surveillance operation conducted by the NSA against US citizens. While working as an employee and contractor to US intelligence agencies, Snowden became bitterly disillusioned by what he saw as the surveillance state gaining in both breadth and power; "[I] watched as Obama advanced the very policies that I thought would be reined in."⁴ Snowden subsequently released a treasure trove of highly classified documents to media outlets, including British national newspaper The Guardian. Snowden's stated motivation for stealing approximately 1.7 million documents from the NSA was his desire to reveal the actions of a state he believed had eroded privacy too far in preference of security. He recounts his primary motivation was "to inform the public as to that which is done in their name and that which is done against them."⁵ After releasing the documents Snowden flew to Russia, where he was granted a one-year temporary asylum by the Russian Government. While the consequences of Snowden's actions are only just now becoming known, they have already reverberated in almost every part of the political globe.

The documents leaked by Snowden and reported by The Guardian newspaper reveal that the US Government was collecting the telephone records of tens of millions of American citizens. This included accessing data held by US telecommunications companies and Internet firms, including Facebook, Google, Microsoft, and Yahoo, which was used to track online communications through a clandestine mass electronic surveillance data mining programme known as PRISM.⁶ Snowden's leaks exposed a similar scale of surveillance on citizens of the United Kingdom (UK) by the NSA's British counterpart, the Government Communications Headquarters (GCHQ). Reports in The Guardian newspaper claim to reveal that the GCHQ had secretly gained access to the fibre-optic cables that carry most of the world's phone calls

⁴ Sean Wilentz, "Would You Feel Differently About Snowden, Greenwald, and Assange If You Knew What They Really Thought?" The New Republic, 19 January 2014. Accessed 29 January 2014. www.newrepublic.com/article/116253/edward-snowden-glenn-greenwald-julian-assange-what-they-believe,

⁵ Greenwald, Glen et al, (10 June 2013)

⁶ Ewen MacAskill et al, "GCHQ taps fibre-optic cables for secret access to world's communications" theguardian.com: The Guardian, 21 June 2013, <http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa>, accessed 14 January 2014.

and Internet traffic, and had begun to process vast streams of sensitive personal information.⁷ This information was reportedly shared with the NSA, enabling the intelligence agencies to access and process vast quantities of communications of entirely innocent people as well as targeted suspects.⁸ Known as Tempora, the GCHQ programme represented “a window on to their everyday lives, sucking up every form of communication from the fibre-optic cables that ring the world.”⁹

Snowden’s actions have seen him variously described as a hero¹⁰ or a traitor.¹¹ “I don't see myself as a hero,” he has said, “because what I'm doing is self-interested: I don't want to live in a world where there's no privacy and therefore no room for intellectual exploration and creativity.”¹² Whatever the motivations for Snowden’s actions, they have prompted an international debate regarding government mass surveillance and the balance between national security and privacy. The passionate debate that has exploded throughout the global intelligence communities, governments and civil liberties groups cannot be overstated. Rick Ledgett, the NSA official in charge of the task force investigating the Snowden leaks, has said that Snowden has 31,000 documents that Ledgett described as “the keys to the kingdom”.¹³ Commentators have speculated that the damage done to the US intelligence setup could be comparable to that of “9/11” to national security.¹⁴

3. Why Does Cyber Matter?

Since the late 1980s, the Internet has grown in terms of accessibility and importance, and has proven to be a highly dynamic means of communication. It has been both a driving factor and key characteristic of globalisation, and has granted states, corporations and individuals a truly global reach by allowing quick and effective communication across borders to an almost

⁷ Ibid

⁸ Ibid

⁹ Ibid

¹⁰ Ibid

¹¹ Charles Moore, “Edward Snowden is a traitor, just as surely as George Blake was”. Telegraph.co.uk: The Telegraph, 05 July 2013, <http://www.telegraph.co.uk/technology/internet-security/10162351/Edward-Snowden-is-a-traitor-just-as-surely-as-George-Blake-was.html>, accessed 14 January 2014

¹² Lorenzo Franceschi-Bicchieri, “Edward Snowden's Motivation: Internet Freedom”, Mashable.com, 11 June 2013, <http://mashable.com/2013/06/10/edward-snowden-Internet-freedom//>, accessed 14 January 2014

¹³ The Washington Post, December 2013

¹⁴ Chen Xiangyang, *Strategic Impacts of the 'Snowden Incident' on International Relations. China-US Focus*, September 9, 2013. Accessed February 13, 2014. <http://www.chinausfocus.com/peace-security/strategic-impacts-of-the-snowden-incident-on-international-relations/>, accessed 14 January 2014

limitless audience. The benefits of cyber technology are numerous, starting with its unique suitability for sharing information and ideas, which is recognized as a fundamental human right.¹⁵ Additionally, a high proportion of a modern states' national infrastructure today relies on information technology systems and access to cyberspace to operate. This infrastructure can include telecommunications networks, hospitals, financial and security services, energy production and distribution, among many others. Furthermore, this critical national infrastructure is linked to global information technology systems, described by Libicki as approaching "spaghetti status" in terms of their interconnections and dependencies, with the advent of cloud computing only increasing this complexity.¹⁶

The world's reliance on cyberspace and the interconnectedness of government, military and civilian sectors has resulted in calls for states to be increasingly concerned about the possible impact of a cyber-attack and its threat to national security.¹⁷ A 1998 US Commission report on National Security in the 21st Century,¹⁸ dedicated to understanding how the world will likely evolve over the next 25 years, concluded that rapid advances in information and biotechnologies will create new vulnerabilities for US security, and the national security of all advanced states will increasingly be affected by the vulnerabilities of the evolving global economic infrastructure.¹⁹ A 2014 World Economic Forum report on global risks ranked cyber-attacks as the 5th most likely global risk to occur, ahead of terrorism and interstate conflict.²⁰ The same report ranked the breakdown of critical information infrastructure as the fifth highest risk in terms of global impact.²¹ Richard Clarke and Christopher Hughes argue that large-scale strategic attacks through cyberspace against "critical infrastructure" pose a grave threat to national security.²² Such attacks might be attractive to an adversary because

¹⁵ UN General Assembly, Universal Declaration of Human Rights, Article 19 10 December 1948, 217 A (III), available at: <http://www.un.org/en/documents/udhr/>, [accessed 27 December 2013]

¹⁶ Martin Libicki. *Pulling Punches in Cyberspace*. In *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy*, edited by the National Research Council of the National Academies, 123-148. (Washington DC: The National Academies Press, 2010).

¹⁷ Natasha Solce 'The Battlefield of Cyberspace: The Inevitable New Military Branch – The Cyber Force' 18 (Alb L J Sci & Tech, 2008), p 297

¹⁸ US Commission on National Security/ in the 21st Century. "New World Coming: American Security in the 21st Century (Phase I: July 1998) – August 1999)." Accessed January 18, 2014. <http://www.fas.org/man/docs/nwc/>.

¹⁹ U.S. Ibid

²⁰ The 2012 Global Risks Report ranked cyber-attacks as 4th global risk in terms of likelihood. See World Economic Forum (2014), p 17

²¹ Ibid, p 17

²² Robert Reardon, and Nazli Choucri. *The Role of Cyberspace in International Relations: A View of the Literature*. (San Diego: MIT, 2012), p 22

they can be cheap and difficult to trace, with the anonymity of cyberspace often making it difficult or impossible to attribute an attack to a particular attacker with confidence.²³

4. Definitions

Cyberspace

Before proceeding further, it is necessary to first define and examine the term ‘cyberspace’. There are many different definitions of cyber space and a globally accepted definition has not yet been found. Richard Clarke describes cyberspace as a new “domain” of conflict, a battle space in which both states and non-state actors can launch strategic “cyber-attacks” against adversaries.²⁴ The Oxford English Dictionary simply defines cyberspace as “[t]he notional environment within which electronic communication occurs.”²⁵ An accurate description should also note that cyberspace spans the globe, using the physical infrastructure residing within the other linear domains, and that, as users pass information from one site to another, data crosses geographic boundaries by means of the cyberspace domain.²⁶ For the purposes of this paper, we will use the comprehensive definition followed by the US Department of Defence – cyberspace is “a global domain within the information environment, consisting of the interdependent network of information technology infrastructures including the Internet, telecommunications, networks, computer systems, and embedded processors and controllers.”²⁷

Cyber-attack

We are also confronted with issues of definition when considering the term ‘cyber-attack’. A cyber-attack can cause computer systems and networks to be unavailable or untrustworthy and therefore less useful to the adversary, potentially having indirect effects on entities

²³ Ibid, p 22

²⁴ Ibid p 21

²⁵ Graham Evans, and Jeffrey Newnham. *The Penguin Dictionary of International Relations*. (Auckland: Penguin Group Limited, 1998).

²⁶ Michael A. Sinks, *Cyber Warfare and International Law*, (Research Report Air Command and Staff College Air University 2008), p 7

²⁷ National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/HSPD-23). Washington DC: White House, 2008.

coupled to or reliant on them.²⁸ The US military has yet to offer an official definition of cyber-attack or cyber-warfare, although a 2009 report by the National Research Council of the US National Academies offered the following definition: “Cyber-attack refers to 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.”²⁹ This refers to deliberate actions to alter, disrupt, deceive, degrade, or destroy computer systems or networks or the information and/or programmes resident in or transiting these systems or networks.”³⁰ It should also be noted that cyber-attacks can happen over time rather than instantly, and can be conducted remotely. For this paper we will adopt the definition of cyber-attack from the US National Research Council: “the 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.”³¹ An example of a cyber-attack was seen in Israel in January 2012, involving the targeting of multiple symbolic Israeli websites, such as the websites of the Tel Aviv Stock Exchange and the national airline, and the unauthorized disclosure of the credit card and account details of thousands of Israeli nationals.³²

5. Cyber-Attack Categories

Cyber-crime

There are essentially four types of cyber-attacks. The first is a cyber-crime, being a crime committed through the use of information technology that is typically of concern to law enforcement. These may be perpetrated by organised criminal organisations, or may be individual hackers motivated by the challenge of circumventing security measures or to gain notoriety.³³ Cyber criminals may also engage in attacks and intrusions for financial gain.³⁴ The Fourth Annual ‘Cost of Cyber Crime Study: Global’ indicates that both the cost and

²⁸ Herbert S. Lin, *Offensive Cyber Operations and the Use of Force*. (Journal of National Security Law & Policy 4, 2010): 63-86, p 1

²⁹ Owens, William A., Kenneth W. Dam, and Herbert S. Lin, ed. *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*. Washington DC: National Academies Press, 2009.

³⁰ Ibid, p 1

³¹ Ibid

³² UNODC, *The Use of the Internet for Terrorist Purposes*. (New York: United Nations, 2012), p 12

³³ Nicholas C. Rueter, *The Cybersecurity Dilemma*. Masters thesis, Duke University, 2011, p 8

³⁴ Ibid, p 8

frequency of cybercrime have continued to rise for the fourth straight year, and the occurrence of cyber-attacks has more than doubled during this period, while the financial impact has increased by nearly 78 percent.³⁵

Cyber espionage

A second category is cyber espionage, which includes political and military espionage.³⁶ At a state level this is often considered an expansion of traditional efforts to collect information on an opponent's intentions and military capabilities.³⁷ Alternatively, cyber espionage may obtain useful economic information by penetrating the computer systems of a competing nation's major industrial firms, such as banks. Some of the most advanced and persistent cyber-attacks on governments and critical infrastructure worldwide are thought to originate from foreign military and intelligence services or organised criminal groups.³⁸ Media organisations around the world are reporting attacks on government systems, national infrastructure and businesses that have resulted in the loss of commercially sensitive information, intellectual property, and state or trade secrets.³⁹ It was written in 1988 that "espionage over networks can be cost-efficient, offer nearly immediate results, and target specific locations... insulated from risks of internationally embarrassing incidents."⁴⁰ Warnings about a 'cyber Pearl Harbour' extend back to 1991.⁴¹ However, although online espionage and crime remain daily issues, cyberspace has so far been resilient to truly disruptive infrastructure attacks, those that could break systems or societies and not just pilfer information.⁴² While cyber espionage may be utilised during warfare, and may at times

³⁵ "2013 Fourth Annual Cost of Cyber Crime Study: Global" (Ponemon Institute, 2013), Accessed February 18 2014, <http://www.hpenterprisesecurity.com/register/2013-fourth-annual-cost-of-cyber-crime-study-global>

³⁶ James Lewis, *A Note on the Laws of War in Cyberspace*. Washington DC: Centre for Strategic and International Studies, 2010, p 2

³⁷ Ibid, p 2

³⁸ New Zealand's Cyber Security Strategy: June 2011, p 5

³⁹ New Zealand's Cyber Security Strategy: June 2011, p 5

⁴⁰ Clifford Stoll, "Stalking the Wily Hacker." *Communications of the ACM* 31, no. 5 (1988): 484-497. http://faculty.cs.tamu.edu/pooh/course/CPSC665/Spring2001/Lessons/Intrusion_Detection_and_Response/p484-stoll.pdf.

⁴¹ The term "electronic Pearl Harbour" dates to a 1991 testimony by author Winn Schwartau to the US Congress. For a longer discussion of this dynamic, see Healey and Grindal 2013

⁴² World Economic Forum, p 38

even be considered a subset of cyber-warfare, it should not be considered warfare in and of itself.⁴³

Cyber terrorism

The third category is cyber terrorism. The Internet is often used to promote and support acts of terrorism and, while the methods of cyber terrorists may be similar to those of cyber criminals, they differ in that cyber terrorism shares an ideological drive equivalent to other forms of terrorism.⁴⁴ A 2012 United Nations (UN) report on the use of the Internet for terrorist purposes identified the following categories of use: propaganda (including recruitment, radicalization and incitement to terrorism); financing; training; planning (including through secret communication and open-source information); execution; and cyber-attacks.⁴⁵ Evan Kohlmann goes so far as to argue that the threat from cyber terrorists is greater than the risk of an attack against critical infrastructure,⁴⁶ although Nye argues that cyber terrorism – narrowly defined as using virtual tools to wreak destruction - has thus far been rare.⁴⁷

Cyber-warfare

The fourth category is cyber-warfare. Cyber-war is a conflict consisting of cyber-attacks between two state actors that relies exclusively or mostly on operations in cyberspace.⁴⁸ Modern states are investing heavily in cyber capabilities and are preparing for, and have already engaged in, cyber-warfare.⁴⁹ The People's Republic of China (PRC) is reportedly "aggressively developing" its cyber capabilities,⁵⁰ including the development of cyber-warfare elements in its army and a volunteer force, and is reportedly pursuing a battalion-sized force of computer experts to carry out cyber-attacks as a means of seeking

⁴³ Lewis, pp 1-2

⁴⁴ Rueter, p 10

⁴⁵ UNODC (2012), pp 3-12

⁴⁶ Reardon and Choueri, p 23

⁴⁷ Nye Jr., *Cyber Power*. (Cambridge: Belfer Center for Science and International Affairs, Harvard Kennedy School, 2010), p 15

⁴⁸ Libicki (2010), p 123

⁴⁹ Richard A Clarke, and Robert Knake. *Cyber War: The Next Threat to National Security and What to Do about It*. (New York: HarperCollins, 2010), pp 30-31

⁵⁰ Directorate-General for External Policies of the European Union, *Cyber Security and Politically, Socially and Religiously Motivated Cyber Attacks*, p 15

asymmetrical advantages over an adversary.⁵¹ The 2008 Russo-Georgian War demonstrated Russia's cyber-attack capabilities. Prior to the Russian invasion of the South Ossetia region, Georgian Government websites were hit with a series of Distributed Denial of Service (DDoS) attacks similar to those seen in Estonia in 2007. Although Russian authorities denied government involvement in the attacks, security experts linked the attacks to the Russian intelligence community.⁵² Acts of cyber-warfare have been attributed to North Korea, Israel, and the United States,⁵³ demonstrating the prevalent use of cyber-attacks as a tool of asymmetric warfare. While the international community remains unsettled on whether cyber techniques are legally considered weapons and whether cyber-attacks can be considered legitimate acts of armed conflict, the denial of service attacks against Estonia in 2007⁵⁴ and Georgia in 2008⁵⁵ illustrate that this new form of warfare is operational.⁵⁶

6. Characteristics of Cyberspace

Lawlessness of the Internet

The characteristics of cyberspace present great opportunities and significant challenges for states and individuals alike. A 2008 New Zealand Law Commission study stated:

*"The Internet has a number of notable characteristics that make it difficult to control, or to trace the flow of data within it. It has no borders – it is not physically located in any one state and can be accessed from anywhere. It is not centrally owned or controlled. It is interactive and dynamic."*⁵⁷

⁵¹ Daria Brankin, "Could a Cyber Attack Constitute a Crime of Aggression under the Statute of the International Criminal Court?", (University of Turin, 2011), p 9

⁵² Clarke and Knake, pp 17-20

⁵³ Rueter, p 18

⁵⁴ In early 2007, Estonia experienced distributed DDoS attacks after relocating a Soviet memorial. Estonian authorities eventually prosecuted a lone hacker, although, Estonian President Toomas Hendrik Ilves claimed the DDoS attacks could only have been orchestrated by a State actor.

⁵⁵ In late 2008, Georgia suffered several weeks of DDoS and defacement attacks against government and commercial websites in conjunction with the breakout of armed conflict between Georgia and Russia over the disputed Georgian region of South Ossetia.

⁵⁶ Brankin, p 17

⁵⁷ New Zealand Law Commission. "Privacy: Concepts and Issues. Review of the Law of Privacy: Stage 1". Wellington: Law Commission, 2008, p 18

Various described as ‘the wild west’ and ‘the world’s largest ungoverned space’,⁵⁸ cyberspace poses significant challenges to sovereignty in a globalised world. The Internet, much like the tribal areas of Pakistan or the tri-border region in South America, is not under the control of anyone and is therefore a place to which the lawless will gravitate.⁵⁹ For all intents and purposes, most actors within the cyber domain operate under conditions of anarchy, with relatively few enforceable laws and no central authority to regulate behaviour. Characteristic of a pre-Hobbesian ungoverned space, the Internet is fraught with difficulties and complexities. It can easily be used to facilitate the free flow of communication between individuals and the creation of legitimate e-commerce, but can equally be used by criminals to conduct criminal activities across geographical borders.

Yet the Internet is not completely without laws. Established international laws and norms govern activities that occur within cyberspace, outlawing many malevolent cyber-operations and allowing states to mount robust responses.⁶⁰ International agreements, such as the Convention on Cybercrime,⁶¹ are helping to increase the effectiveness of criminal law in dealing with cyber-attacks.⁶² Already states have a recognised sovereign right to exercise control over cyber-infrastructure and activities on their territory, as well as to protect them from harmful actions.⁶³ International law also obligates states to ensure that cyber-infrastructure on their territory is not used for acts that unlawfully affect other states.⁶⁴ Thus, state responsibilities extend into cyberspace, including the responsibility to take action to ensure the safety and welfare of the nation and its citizens. However, it is likely that due to the complexity anarchic nature of cyberspace, some grey areas will always exist between domestic and international law.⁶⁵

Low Cost of Entry

⁵⁸ Jared Cohen, and Eric Schmidt. “The New Digital Age: Reshaping the Future of People, Nations and Business”. California: Hodder and Stoughton Limited, 2013, p 3

⁵⁹ Clarke & Knake, p 43

⁶⁰ Michael N. Schmitt, “Cyberspace and International Law: The Penumbral Mist of Uncertainty.” (*Harvard Law Review*, (2013): 176-180, p 177

⁶¹ The Convention on Cybercrime is the first international treaty seeking to address Internet and computer crime by harmonizing national laws, improving investigative techniques, and increasing cooperation among nations. See *Convention on Cybercrime*, 23 November 2001 on the website of the Council of Europe.

⁶² Jack Goldsmith, and Tim Wu. “Who Controls the Internet: Illusions of a Borderless World”. (New York: Oxford University Press, 2006), supra note 86, at viii

⁶³ Libicki (2010), p 125.

⁶⁴ Schmitt (2013), p 177

⁶⁵ Owens, Dam and Lin (n 5) 251

Cyber-attacks are an attractive alternative to traditional state or criminal attacks due to the extremely low costs of entry in relation to potentially high returns on investment.⁶⁶ Joseph Nye states that “the barriers to entry in the cyber domain are so low that non-state actors and small states can play significant roles at low levels of cost.”⁶⁷ Physical equipment is inexpensive and widely available, and the necessary expertise is also becoming increasingly widespread. Perpetrators require little more than a laptop, Internet connection and downloadable tools available on the Internet to begin conducting attacks. This allows smaller states and non-state actors the ability to develop cyber capabilities at much lower cost than that required to develop conventional military or criminal capabilities.

Anonymity

Anonymity relates to the ability to attribute an attack to a specific source or perpetrator. Criminals operate in the cyber world partly to circumvent more conventional, established constructs such as international borders.⁶⁸ Internet communication has not only facilitated the growth of legitimate business, but it has bolstered criminals’ abilities to operate in an environment where they can broaden their pool of potential targets and rapidly exploit their victims.⁶⁹ Identifying perpetrators can be especially difficult in the cyber context due to the ability of attackers to mask their identity by “spoofing” their Internet Protocol (IP) address and obfuscating their identity by routing through a series of proxy servers or utilising a botnet.⁷⁰ Operating behind false IP addresses, foreign servers and aliases, attackers can act with almost complete anonymity and relative impunity.⁷¹ Ronald K. Noble, Secretary-General

⁶⁶ Catherine A. Theohary, “Information Operations, Cyberwarfare, and Cybersecurity,” CRS Report for Congress, (Washington D.C., Congressional Research Service, 17 March 2009) p. 3

⁶⁷ Nye, p 5

⁶⁸ Kristin Finklea, and Catherine Theohary. “Cybercrime: Conceptual Issues for Congress and U.S. Law Enforcement,” CRS Report for Congress, (Washington D.C., Congressional Research Service, January 9, 2013), p 5

⁶⁹ Cybercrime: Conceptual Issues for Congress and U.S. Law Enforcement, p 5 Ibid, p 5

⁷⁰ In a botnet attack a cybercriminal or attacker takes control of a foreign computer by surreptitiously loading software on it (without the consumer’s awareness that the computer has been compromised) in order to conduct attacks. Moreover, some botnets are huge, embracing tens of thousands of computers across the world so that attacks can seem, as in this case, to be coming from everywhere. See Stephen Blank ‘Web War I: Is Europe’s First Information War a New Kind of War?’ (27:3 Comp Strat 227, 2008)

⁷¹ Paul Cornish et al., *On Cyber Warfare*. (London: Chatham House, 2010), p 13

of Interpol since 2000, believes the anonymity of cyberspace makes it one of the most dangerous criminal threats faced by modern society.⁷²

Furthermore, the difficulty of attribution allows a degree of plausible deniability for the attacker. Perpetrators can cover their own tracks and implicate others, particularly when third-party servers and botnets in unrelated countries are used as the origin of attacks to provide cover for the actual attacker.⁷³ Targeting by criminal elements is not the only threat presented by the rise of cyberspace. Internationally, the trend in cyber-crime has been described as shifting from 'exploitation' of existing networks and security weaknesses, to 'disruption' and 'destruction'.⁷⁴ In other words, the cyber threat is changing from theft of personal and intellectual property, to denial of service attacks and destruction of computer networks. A key challenge for national security is the identification of the source of these attacks, thereby allowing the culprits to be brought to justice, or at the very least for the threat of the attack to be mitigated.

7. Asymmetric Attack

Tied to the low cost of entry, cyber-attacks are an attractive tool for waging asymmetric attack.⁷⁵ Small states or non-state actors looking to conduct offensive operations outside existing international legal agreements and obligations, or at a low cost of entry, may be convinced to fight in cyberspace.⁷⁶ As the 2008 Estonian attacks indicate, the Internet has become a powerful asymmetric tool for transnational groups who view themselves as disenfranchised and seek to intimidate the nation-states and other actors presumably responsible for their grievances.⁷⁷ However, it is unclear that such groups have the same capacities as large governments. In spite the low costs of entry and relative anonymity that cyber-attacks provide, sophisticated attacks on targets such as military systems require

⁷² Addison, Adrian. "Cybercrime is World's Most Dangerous Criminal Threat". (Agence France-Presse, September 17, 2010). Accessed December 12, 2013.

http://www.google.com/hostednews/afp/article/ALeqM5j368XIZpJo33r7xM64NgOqp1_XeQ.

⁷³ Cornish, et al., p 13

⁷⁴ Rajesh Chhana, "Regulatory Impact Statement: Government Communications Security Bureau Act Review". (Wellington: Department of Prime Minister and Cabinet, 2013), p 3

⁷⁵ Here asymmetric attack means "conflicts between actors with wide disparities in power." Rueter, p 37

⁷⁶ Cornish, pp 21-22

⁷⁷ Stephen Herzog. "Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses." *Journal of Strategic Security* 4, no. 2 (2011): 49-60. Accessed January 12, 2014. <http://www.scholarcommons.usf.edu/jss/vol4/iss2/4>, p 52

greater resources to mount, and it is generally the realm of large intelligence agencies to intrude physically and/or crack highly encrypted codes.⁷⁸ A teenage hacker and a large government can both do considerable damage over the Internet, but that does not make them equally powerful in the cyber domain.⁷⁹ However, while 'hit and run' cyber strikes by individuals are unlikely to bring governments or corporations to their knees, they can impose disproportionate costs of disruption to operations and to reputations with miniscule investment.⁸⁰

8. Methods of State Surveillance

James Der Derian argues that the emergence of the 'Digital Age' and the attacks of September 11, 2001 have in different ways "transformed the meaning and discourse of national security."⁸¹ Historically, security has been seen as a core value and ultimate goal of state behaviour. Traditional analysis of security at the state level has focused on the military dimension, although the end of the Cold War has allowed for a burgeoning of security theory to include ideas about economic and environmental security. The need for security speaks to the hierarchy of human needs, primarily the need for survival as the highest point of the hierarchy. Just as an individual's need for security increases with the threat to their physical survival, so too does a society or state's necessity for security. With the rise and evolution of cyber-related terrorism, espionage and crime, there has seldom been a time that the prediction and intervention of attacks has had such important consequences. Rarely have Governments had to rely on such disparate and speculative data to prevent attacks that have the potential to cause widespread destruction or mass panic. Sufficient data must be collected to adequately empower a state to identify and prevent terrorist threats targeting its citizens, possessions or interests. Given the global nature of the Internet, these attacks can be domestic or international in origin.

The collection of intelligence plays an important role towards ensuring governments have enough information to identify threats and make decisions relating to their national security

⁷⁸ Nye Jr, p 14

⁷⁹ Nye Jr, p 14

⁸⁰ Nye Jr, p 16

⁸¹ James Der Derian. "The Question of Information Technology in International Relations." *Millennium - Journal of International Studies* 32 (2003): 441-456, p 452

and survival. States, just like individuals, have a diverse range of security concerns, including material or resource concerns, threats or vulnerabilities, and institutional commitments. Governments maintain intelligence services to collect information that would otherwise be denied to them. Intelligence agencies also have a role in protecting the information of states that they would see denied to others. Governments are then able to act on this information collected or denied to other states through their foreign policy and interactions with extra-state actors such as Non-Government Organisations (NGOs) or multinational corporations. Thus, the collection of intelligence relates specifically to a state's national security, or ability to protect its national borders, possessions, citizens and interests.

In this respect, intelligence collection is of prime importance to any modern international relations debate. Whether covert or overt, intelligence is the collection, protection, and analysis of both publicly available and secret information, with the goal of reducing policy maker's uncertainty about a foreign policy problem. Policy makers face a great deal of uncertainty when crafting foreign policy, and in general terms lack information about a friend or foe's capabilities or intentions. Timely and appropriate intelligence can address this uncertainty by providing information that confirms or at least reduces uncertainties as to another's intentions and capabilities. The acquisition of confidential intelligence is the prime function of intelligence agencies, and can be gathered using traditional collection of information from other humans, or HUMINT, to more technical means such as signals intelligence (SIGINT), technical intelligence (TECHINT), and electronic intelligence (ELINT) collection, whereby technology is utilised to exploit weaknesses.

9. Social Contract

Social contract theory was introduced by early modern thinkers such as Thomas Hobbes, John Locke and Jean-Jacques Rousseau. It is one of the most relevant pieces of literature when it comes to affirming the need for a state-ruled social order. Rousseau proposed a contract between individuals in society, the purpose of which was the protection of individual within the security of a community.⁸² Emmanuel Kant argued that individuals do not naturally live in communities and create law, but as rational actors they do so to profit

⁸² J Rousseau and Jean Jacques. *Social Contract, & Discourses*. (New York: E. P. Dutton & Co., 1913). Bartleby.com, 2010. www.bartleby.com/168/, accessed 12 January 2014 book 1, chapter 6, para 2

from the advantages of an established community.⁸³ Individuals do not have an inherent right to leadership, but are appointed by the entire community only after the establishment of the social contract.⁸⁴ Through this contract, the population is the sovereign of the state, and the government is established only to carry out the will of the sovereign and act as an arbitrator.⁸⁵

The social contract defines the responsibility of the state to maintain rights and security the security of its citizens, and lays the intellectual groundwork for a strong central government. Hobbes' "The Leviathan" contends that in a state of nature, without benefit of law and law enforcement, life is "solitary, poor, nasty, brutish, and short."⁸⁶ Hobbes argues that in this state "all men have a natural right to all things", and without laws, man would be in a state of such liberty that there would be no limitations on his actions or behaviour.⁸⁷ To ensure peace, man relinquishes some rights to the state as part of a social contract, and the state would possess a monopoly of force within the society. In doing so, the state is able to ensure the security of its citizens and interests. While many of man's natural rights are lost through this process, such as renouncing the right to kill, the individual gains security for this trade-off. Therefore, social contract theory advocates for a twofold responsibility between states and citizens, which is reflected in the United Nations Charter and domestic laws of various countries.⁸⁸

There is a broad consensus that state responsibilities are extended to cyberspace. In 2011, the United Nations declared access to the Internet to be a basic human right,⁸⁹ and made clear the responsibilities of state to ensure the security of their citizens in cyberspace:

⁸³ R H Weber and R Weber, "Social Contract for the Internet Community? Historical and Philosophical Theories as Basis for the Inclusion of Civil Society in Internet Governance?", (2009 SCRIPTed 6), <http://www.law.ed.ac.uk/ahrc/script-ed/vol6-1/weber.asp>, accessed December 10, 2013 para 6:1

⁸⁴ Ibid, para 2.1

⁸⁵ J Rousseau, 3, ch 1, para. 18

⁸⁶ Thomas Hobbes, and J. C. A. Gaskin. *Leviathan*. (Oxford: Oxford University Press, 1998), XIII.9

⁸⁷ Hobbes & Gaskin, *Leviathan*, XIII.9

⁸⁸ Maranga, Kennedy. "The Changing Role of State Responsibility: Comparative Approach." (*Journal of Global Affairs and Public Policy* 1, no. 1, 2011): 1-24, p 3

⁸⁹ UNGA "Report of the Special Rapporteur on the promotion and protection of the right to freedom of Opinion and expression, Frank La Rue", (16 May 2011), A/HRC/17/27 , http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf, accessed 17 January 2014

*States have an obligation to protect individuals against interference by third parties that undermines the enjoyment of the right to freedom of opinion and expression. This positive obligation to protect entails that States must take appropriate and effective measures to investigate actions taken by third parties, hold the persons responsible to account, and adopt measures to prevent such recurrence in the future.*⁹⁰

10. Privacy

In seemingly direct conflict with security and the collection of intelligence is the notion of privacy. Privacy is the presumption that individuals should have an area of autonomous development, interaction and liberty, a 'private sphere' with or without interaction with others and free from state intervention, and free from excessive unsolicited intervention by other uninvited individuals. Privacy is more closely associated with democracy and liberalism than other competing political theories such as authoritarianism, communism or realism, due to the importance placed upon privacy. From a Liberal perspective, privacy is a pre-eminent individual good due to its protection of anonymity, confidentiality, seclusion and intimacy – to name a few characteristics of privacy – which help foster the freedom and equality necessary for democratic politics by structuring and limiting competition for power in ways that enable people to see and treat each other as equal despite incompatible beliefs, interests and identities.

The right to privacy has been recognised as a human right; although as with most international human rights, the right to privacy is not absolute. Absolute rights, such as freedom from torture and other cruel, inhuman or degrading treatment or punishment, cannot be limited, suspended or restricted for any reason.⁹¹ The idea of a moral right to privacy is a relatively new concept, largely a product of the modern nation state. Previously there was no widely held belief that people had a right to privacy, moral or otherwise. While there was an expectation of privacy, the right to privacy was given adequate protection by other moral and legal rights up to that point. This is seen in the right to property, whereby an

⁹⁰ UNGA, (16 May 2011), Ibid, p 15, para 52

⁹¹ Human Rights Review 2012, Article 3: "Freedom from torture and inhumane and degrading treatment or punishment", (Equality and Human Rights Commission, 2012) <http://www.equalityhumanrights.com/human-rights/our-human-rights-work/human-rights-review/the-articles/>, accessed 02 January 2014, p 5

individual's home provided adequate protection from invasions of privacy simply by barring entry to others and thus preventing external parties from collecting private information without consent. Thus the right to privacy was derived from other enumerated rights.

11. The Rise of Big Data

While the tension between privacy and intelligence is not a new phenomenon, what is new is the scale at which data can now be easily and efficiently moved. What would have taken significant effort just twenty years ago can now be achieved with the click of a mouse. The modern world's infatuation with all things electronic, including the Internet, social networking and mobile devices, has produced a vast amount of digital information that is held by public and private institutions alike. In terms of private information, the world has seen the most profound transformation of the availability and size of data ever experienced. Digital databases now contain a virtual plethora of data: financial, medical, educational, travel, locational, communications between parties, photographs of individuals and their associates, fingerprints and other biometrics such as iris-scans and DNA profiles. This data is a treasure trove for any analyst seeking to determine pattern of life, conduct network analysis, or identify persons of interest.

As the 2009 White House Cyberspace Policy Review states, "cyberspace touches practically everything and everyone."⁹² The parallel rise of 'big data' in the past decade has seen a further evolution of the concept of national security, particularly relevant in the age of popular social networking media. Intelligence collections and 'big data' presents huge challenges for privacy, security, regulation, and the power relationship between citizens and the state, potentially leading to "big data authoritarianism."⁹³ For example, in the 20th century SIGINT collection meant intercepting analogue signals carried along lines of communication that had two discrete and known target points. In the 21st century, communications are mostly digital, and can be carried globally upon any number of different systems that dynamically route billions of bits of data. The danger in the 21st century is the

⁹² Office of the White House Press Secretary. "Cyber Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure", (Washington D.C., The White House Press, 2009), p i

⁹³ Kenneth Neil Cukier, and Viktor Mayer-Schoenberger. "The Rise of Big Data: How it's Changing the Way We Think About the World". *Foreign Affairs* (May-June 2013). Accessed January 30, 2014. <http://www.foreignaffairs.com/articles/139104/kenneth-neil-cukier-and-viktor-mayer-schoenberger/the-rise-of-big-data>

use of tools that collect data with no focus, instead preferring to cast a wide net to capture as much data as possible. Taking advantage of the unparalleled availability of data available online, advances in computing have made it possible to extract, collate and analyse data in powerful and sophisticated ways that have significant implications for informational privacy. Two key techniques that are greatly facilitated by more powerful computer technology include 'data matching' and 'data mining'. Data matching involves comparing data that comes from different sources and has been collected for different purposes. Data mining involves extracting information that is implicit in data sets, usually by discovering new relationships among the data elements.

Both data matching and data mining can raise privacy concerns as they seek to uncover previously unknown information about people. However, the collection of this data by intelligence agencies does not necessarily diminish the privacy of individuals. Only a small fraction of the Internet's traffic involves human-to-human communications such as email messages. Most Internet communications are communications between humans and computers, such as World-Wide-Web pages in transit, commands sent to remote servers, and file transfers. Many others are computer-to-computer communications, such as network administrative traffic that keeps the Internet running smoothly.⁹⁴ However, the collection of metadata associated with communications can raise privacy concerns when the power of data matching and data mining programs are considered. As stated by New Zealand's Privacy Commissioner in 2013:

*"Metadata is not necessarily innocuous. It can provide a detailed map of a person's life – such as tracking their location, contacts and interests. This is why it is valuable in the intelligence arena. But it is also why effective oversight is required to ensure that it is collected and used appropriately, not as the tool of mass surveillance that it has the capacity to be, if unchecked."*⁹⁵

⁹⁴ Orin S Kerr "Internet Surveillance Law After the USA patriot Act: the Big Brother that Isn't" (2003), 97 Northwest U L rev) 607, -613, p 4

⁹⁵ Marie Shroff, "Submission by the Privacy Commissioner (to the Intelligence and Security Committee, (Wellington: Office of the Privacy Commissioner, 17 June 2013), s 4.3

French military theorist Charles-Jean-Jacques-Joseph Ardant du Picq wrote that “the art of war is subjected to numerous modifications by industrial and scientific progress. But one thing does not change, the heart of man.”⁹⁶ The intelligence documents leaked by Edward Snowden demonstrated the industrial scale at which highly-resourced intelligence agencies are now able to collect data. Additionally, while cyberspace may allow governments to collect data on a much larger scale, it has also allowed for a comparable increase in the ability of criminal organisations to conduct criminal activity on a mass scale. Criminal organisations are able to conduct sophisticated, targeted attacks across geographic borders with impunity. Security in the cyber age is no longer a special topic of exclusive concern to states as cyberspace has transferred risk and the responsibility for security from the state to non-state actors.

Most citizens and private organisations simply do not know where or how to start preparing for these threats, with an additional challenge presented by the pace of technology, which results in constantly evolving threats. Although cyber-attacks directed at non-state actors may not involve the sophistication or resources of an attack directed towards national infrastructure or state agencies, corporations and citizens are increasingly exposed to advanced cyber-attacks simply due to the modern world’s increased dependence on cyberspace.

12. Turning off Access

Faced with the significant challenges that cyber-attacks pose, what security strategies can states follow to provide adequate security for their citizens? At the most basic level, a state can simply choose not to have any connection to the Internet, foregoing the significant benefits that Internet communications bring. To achieve this, states may institute mechanisms for the control or regulation of cyberspace by placing restrictions on incoming and outgoing Internet traffic. Examples of national ‘firewalls’ being constructed within states include China’s ‘Golden Shield Project’, also known as the new Great Wall of China. This system, which restricts Internet traffic using a sophisticated content-filtering regime

⁹⁶ Charles-Jean-Jacques-Joseph Ardant du Picq, *Battle Studies*. (Harrisburg: The Military Service Publishing Company), 1958

involving some 50,000 domestically-based servers,⁹⁷ is intended to limit the circulation of 'objectionable' information within the country. In essence China is attempting to build a secure national "intranet" independent of the Internet,⁹⁸ which will act as a nationwide digital surveillance network, linking China's national, regional and local security agencies together. Whether this can protect China from the threat of cyber-attack is questionable, with the firewall already failing due largely to the increased volume of Internet traffic in China.⁹⁹ Other states have also attempted to shut off access to the Internet completely by blocking access to telecommunications infrastructure itself. This has occurred in authoritarian states such as Syria, Egypt and Libya during the Arab Spring. This unprecedented level of Internet censorship allowed the state to control information by effectively severing access to the global Internet.¹⁰⁰ Another example is North Korea, which, while one of the most isolated countries in the world, still has Internet access. Rather than blocking content, Internet use in North Korea is essentially banned for all but the most powerful elites.

Revelations of large-scale western surveillance have also pushed democratic countries such as Germany and Brazil to consider formulating national Internets. Germany's Deutsche Telekom has sought to tighten security through 'national routing', which would see data generated in Germany and destined for local users exclusively handled by fibre-optic cables, routing gear, and computers within Germany.¹⁰¹ Brazil is pushing to force Internet companies such as Google and Facebook to store local data within the country's borders, and to create an encrypted national e-mail service.¹⁰²

While these actions may prove effective at limiting the potential for cyber-attack from external sources, commentators have suggested that "a balkanization of the Internet is not

⁹⁷ Chris Keall. "'NZ Govt Naïve about Huawei' – security insider Selwyn Pellett details Beijing experience with Endace." (*National Business Review*, April 5, 2012). <http://www.nbr.co.nz/article/govt-naive-about-huawei-%E2%80%93-security-insider-details-beijing-experience-ck-115894>, accessed January 12, 2014.

⁹⁸ Greg Walton. *China's Golden Shield: Corporations and the Development of Surveillance Technology in the People's Republic of China*. (Quebec: International Centre for Human Rights and Democratic Development, 2001), p 18

⁹⁹ Walton, p 5

¹⁰⁰ James Glanz, and John Markoff. "Egypt Leaders Found 'Off' Switch for Internet." (*The New York Times*, February 15, 2011). Accessed January 2, 2014, http://www.nytimes.com/2011/02/16/technology/16internet.html?pagewanted=all&_r=0.

¹⁰¹ Blau, John. "NSA Surveillance Sparks Talk of National Internets." (*IEEE Spectrum*, January 23, 2014). Accessed January 30, 2014. <http://spectrum.ieee.org/telecom/internet/nsa-surveillance-sparks-talk-of-national-internets>

¹⁰² Ibid

the solution and runs totally contrary to the basic principles of the Internet.”¹⁰³ While the idea of strengthening states’ abilities to censor information transmitted over the Internet has appealed to authoritarian regimes, it flies in the face of free speech principles.¹⁰⁴ Democratic states will typically pursue other security strategies before compromising the basic democratic tenets of freedom and free speech by restricting Internet access in this manner.

13. Deterrence

Deterrence is an example of a traditional security theory that can be used by states in cyberspace. Glenn Snyder classically defined deterrence as “discouraging the enemy from taking military action by posing for him a prospect of cost and risk outweighing his prospective gain.”¹⁰⁵ If deterrence is anything that dissuades an attack, it is usually said to have two components: deterrence by denial (the ability to frustrate the attacks) and deterrence by punishment (the threat of retaliation).¹⁰⁶ Delving further, there are three approaches that must be applied to ensure deterrence is achieved. Firstly, a strong defence is needed to protect against the vast majority of aggressors and dissuade some from attacking at all.¹⁰⁷ Secondly, the ability to attribute an attack to a specific source is important for maintaining credibility and ensuring legitimacy at home and abroad.¹⁰⁸ Thirdly, an actor must project willingness and the capability to retaliate against attacks.¹⁰⁹

While classical deterrence theory focuses on nation states, cyber-attacks perpetrated by non-state actors such as terrorist or criminal groups pose a credible threat to individual and state national security, and are also subject to deterrence theory. However, as previously discussed, the nature of cyber-attacks presents difficulties in relation to each of the elements of deterrence. Firstly, the low cost, anonymity and scale of cyber-attacks makes defence against attacks difficult. No state has the resources necessary to identify, prevent and

¹⁰³ Ibid

¹⁰⁴ Rueter, p 43

¹⁰⁵ Patrick Morgan, *Deterrence Now*. (Cambridge: Cambridge University Press, 17 April 2003), p 2

¹⁰⁶ Martin Libicki, *Cyber Deterrence and Cyberwar*. (Santa Monica: RAND Corporation, 2009), p 7

¹⁰⁷ Christopher Haley, “A Theory of Cyber Deterrence”. (*Georgetown Journal of International Affairs*, 2013). Accessed January 21, 2014. http://journal.georgetown.edu/2013/02/06/a-theory-of-cyber-deterrence-christopher-haley/#_edn6

¹⁰⁸ Ibid

¹⁰⁹ Ibid

retaliate against thousands of attacks per day.¹¹⁰ Attribution is equally difficult given the relatively anonymous nature of the cyber domain. Governments can launder their actions through individual users or groups, and individuals can hide behind technology that makes identification near impossible. Lastly retaliation, crucial to any deterrence theory, may present the greatest difficulty for states due to both these issues and a lack of established international law.¹¹¹

Although cyber deterrence is highly unlikely to eliminate the occurrence of all attacks, no matter how effective the implementation,¹¹² it can play a critical role in reducing the total number of attacks to a manageable level at a relatively low cost.¹¹³ Consequently, resources that may otherwise be consumed would be available to pursue and prosecute any attacks that do slip through. To achieve this, states must continually communicate to ensure that deterrent messages are projected, received and understood, as deterrence is possible only when others have a good idea of the one's capabilities and intentions. A measure of this communication is the development of effective domestic and international cyber legislation, in parallel with the development of cyber capabilities to ensure that cyber-attacks are effective at both defending against attacks and identifying perpetrators.

14. Security Frameworks

A further conceptual framework for state cyber-security may take the form of security alliances. To deter threats and ensure the security of citizens and national interests, states raise sufficient offensive or defensive capabilities to deter attack from other states or non-state actors. To do so, states may engage in diplomacy or alliance-building to ensure enhance their security. Alliances may be temporary, or longer term, formalised and institutionalised security partnerships. For a small state, such as New Zealand, collective

¹¹⁰ Patrick M. Morgan, "Applicability of Traditional Deterrence Concepts and Theory to the Cyber Realm," Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy, (Washington DC, 2010). Accessed 17 January 2013, www.nap.edu/openbook.php?record_id=12997&page=55,

¹¹¹ Christopher Haley, "A Theory of Cyber Deterrence". (*Georgetown Journal of International Affairs*, 2013). Accessed January 21, 2014. http://journal.georgetown.edu/2013/02/06/a-theory-of-cyber-deterrence-christopher-haley/#_edn6

¹¹² Ibid

¹¹³ Ibid

security agreements are an avenue for access to greater resources and an important strategy to counter global threats such as cyber-attacks.

The significant threat that cyber-attacks pose to state security has reignited the necessity for cooperation amongst security and intelligence partners. With globalisation, the international security environment has become more interdependent than ever before with the establishment of complex networks that make responding to and managing security challenges increasingly difficult, but increasingly necessary. Intelligence sharing between close allies through various bilateral and multilateral alliances is a routine form of international cooperation and security development. As a recent White House Cyberspace Strategy memo observed:

“Enhancing national-level cybersecurity among developing nations is of immediate and long-term benefits [to the United States and all nations], as more states are equipped to confront threats emanating from within their borders and in turn, build confidence in globally interconnected networks and cooperate across borders to combat criminal misuse of information technologies. It is also essential to cultivating dynamic, international research communities able to take on next-generation challenges to cybersecurity.”¹¹⁴

While literature detailing international intelligence cooperation is sparse due to the subject’s sensitive nature, there is no doubt that all intelligence services perform some kind of liaison function. Given the vast nature of potential threats to individual states, no single intelligence agency has all the resources – financial, human and technical – to be entirely self-sufficient in all areas. These multilateral agreements are based upon perceptions of common security between like-minded states seeking as close to absolute security as possible in an anarchical global society.

An example of alliance building is the ‘Five Eyes’ security and intelligence alliance. Born of the United States and Britain’s intelligence collaboration during World War II, New Zealand,

¹¹⁴ White House. “International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World”. (May 2011). Accessed December 10, 2013. http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf, s II p 15

Australia and Canada were added as secondary parties to the treaty that established areas of technical and intelligence cooperation between each state. In this collective security agreement, each nation seeks to reduce the prospects and scope of international aggression through preventative association of participating states to protect their joint security.

A second conceptual security framework sees states participating in international institutions to encourage cooperative approaches towards shared security issues. While realists dismiss the importance of institutionalism, Robert Keohane argues that institutions are rooted in the realities of power and interest, and make a significant difference in conjunction with these power realities.¹¹⁵ Implicit in this approach are the notions that power itself has changed and that a nation's military capabilities are not the sole factor in determining its security.¹¹⁶ Rather than solely pursuing hard power approaches, institutionalism allows states to pursue soft power approaches to project its own foreign policy to influence the actions of other states. Institutionalism allows small states in particular to exhibit a firm commitment to international law, seek multilateral solutions to security issues and generally refrain from the use of military force to solve disputes.¹¹⁷

The sharing of intelligence between states is an important form of international cooperation and alliance building. Such relationships are based upon trust, confidence and common goals. This concept of collective security is an important innovation of twentieth-century international relations, asserting that realists' security dilemma can be overcome not through national self-help and the balance of power, but through the institution of communal commitments whereby states commit to joint actions against any external territorial or political threat to other states. This idea of a universal, permanent and collective agreement to oppose aggression and guarantee security is a founding tenet the United Nations. The effectiveness of this concept lies in the willingness of each member state to act against threats from aggressors.

Thirdly, states may pursue a security model based on identity and norms. States can develop and spread norms as a means of influencing the behaviour of states by creating a "standard

¹¹⁵ Robert Keohane & Lisa Martin, *The Promise of Institutional Theory*. (International Security, Vol. 20, No. 1. pp. 39-51, 1995), p 42

¹¹⁶ Joe Burton, "Small states and cyber security: The case of New Zealand". (Political Science 2013, 65: 216, 2013), p 219

¹¹⁷ Ibid

of appropriate behaviour for actors with a given identity.”¹¹⁸ Norms, including those that structure international affairs, are dynamic and capable of strengthening over time. Although cyberspace has been described as a discordant and chaotic sphere of conflict in which it is not yet obvious that a common framework of ethics, norms and values can apply,¹¹⁹ the emergence of cyber-security norms is occurring. Cyber-warfare norms are largely analogous with existing norms,¹²⁰ and although not yet codified into international law, these may become international law in the future. Norms cannot be unnaturally imposed on states as the acceptance of a norm is largely dependent on the quality of the ethical argument underpinning its creation.¹²¹ This unfortunately means that norms often take significant periods of time and effort before they spread. As such it is unclear what effect norms against cyber-attacks will have.

Section Two: New Zealand's Response to Cyber Threats

15. New Zealand and the Rise of Cyber

For a small, isolated state such as New Zealand, a well-functioning cyberspace provides important benefits. The Internet and other forms of digital communication enable New Zealanders to have global access to products and services and reduce our geographical isolation by connecting us with the rest of the world. Access to greater Internet bandwidth and wireless technology – in particular mobile devices such as smart phones – is transforming how New Zealanders access the Internet and how business is transacted in New Zealand.¹²² New Zealand’s Government and critical national infrastructure providers, including banking and finance, telecommunications, transportation and energy sectors, are more and more reliant on digital systems, with government agencies utilising the Internet, digital document management systems and shared online platforms in their day-to-day business. At least 75% of New Zealanders have access to the Internet at home, and they are increasingly communicating across the Internet, accessing government services online, and

¹¹⁸ Martha Finnemore and Kathryn Sikkink, “International Norm Dynamics and Political Change”. (International Organisation: MIT Press, Vol. 52, No. 4, Autumn, 1998): p. 891

¹¹⁹ Paul Cornish et al, On Cyber Warfare, p 37

¹²⁰ Brankin, p 13

¹²¹ Rueter, p 52

¹²² New Zealand’s Cyber Security Strategy: June 2011, p 2

using digital services to complete tasks such as submitting tax returns and making applications for passport renewals and student loans.¹²³

As far back as 2000, New Zealand governments have recognised the importance of the Internet as a worldwide revolution in information and communication technology. Under an e-government initiative, New Zealand introduced new information and communication technologies (ICTs) to the government sector in an attempt to achieve greater operational efficiency, transparency and effectiveness. Benefits of ICTs include faster, more streamlined administrative processing, lower transaction costs, better use of information resources, greater public access to government information and services, and more opportunities for public participation in democratic processes.¹²⁴

Parallel to the benefits that the Internet brings, so too does it bring a new set of security challenges for New Zealand. New Zealand's geographic isolation has traditionally provided the country with some level of protection against attack. The lack of land borders and general physical remoteness make New Zealand much less vulnerable to attack than many other countries, which has in turn influenced the country's security and national security policy. The 2010 Defence White Paper identified physical isolation as New Zealand's principal source of protection against direct military threat from other states.¹²⁵ The paper recognised, however, that this distance was no longer sufficient insulation from attack, especially given globalisation and technological reach.¹²⁶

Notwithstanding the growing threat of physical attacks in other parts of the world, the threat of physical attacks against New Zealand remains small. As New Zealand Member of Parliament (MP) Peter Dunne once observed "[New Zealand is] not a hotbed of international terrorism, nor are we likely to become such a hotbed."¹²⁷ Yet the development of global communications has increased the threat of cyber-attack against New Zealand, with the

¹²³ Ibid, p 2

¹²⁴ Rose O'Neill. "E-Government: Transformation of Public Governance in New Zealand?" (PhD diss., Victoria University of Wellington, 2009), p 2

¹²⁵ New Zealand Ministry of Defence. *Defence White Paper 2010*. (Wellington: Ministry of Defence, 2010), p 17

¹²⁶ Ibid, p 17

¹²⁷ "Counter-Terrorism Bill: Second Reading." (Hansard (debates), vol. 612, week 39, October 14, 2003).

Accessed February 12, 2014. http://www.parliament.nz/en-nz/pb/debates/debates/47HansD_20031014_00001157/counter-terrorism-bill-%E2%80%94-second-reading.

2010 Defence White Paper identifying cyber-attacks as a growing threat with potentially crippling consequences for New Zealand.¹²⁸

The Department of the Prime Minister and Cabinet's Statement of Intent to 2017 prioritised the development and implementation of robust cyber security strategies.¹²⁹ In announcing changes to the legislation for New Zealand's foreign intelligence agency, the Government Communications Security Bureau (GCSB), Prime Minister John Key stated:

*While the terrorism threat in New Zealand has remained low, there are people within our country who have links to off-shore terrorist groups... And the many other threats to our national security have continued to intensify, these include cyber-attacks against Government and private organisations where information is at risk, and the intellectual property of some of our smartest and most innovative New Zealanders is at risk. There is evidence of cyber espionage in New Zealand (and) there have been covert attempts to acquire New Zealand science and technology for programmes relating to weapons of mass destruction or weapons delivery systems. Other threats we face include countries conducting foreign interference and espionage, this includes attempts to recruit individuals who have access to sensitive political or military secrets.*¹³⁰

Furthermore, the establishment of the NCSC in 2011 shows that the New Zealand Government has been taking strategic challenge of cyber security seriously. The NCSC is responsible for the protection of government systems and information by planning for and responding to cyber incidents, and working with providers of critical national infrastructure to improve the protection and computer security of such infrastructure against cyber-borne threats.¹³¹ The NCSC's goals are divided into three priority areas: increasing awareness to promote online security, protection of online infrastructure, and computer emergency

¹²⁸ *Defence White Paper (2010)*, p 25

¹²⁹ Department of the Prime Minister and Cabinet, *Statement of Intent 2013 – 2017* (2013), p 3

¹³⁰ "Key reveals WMD cyber terrorism threat to NZ (15." (TVNZ, April 15, 2013)). Accessed January 15, 2014. <http://www.tvnz.co.nz/national-news/key-reveals-wmd-cyber-terrorism-threat-nz-5407210>.

¹³¹ Government Communications and Security Bureau (GCSB). "Annual Report for the Year Ended 30 June 2013." September 30, 2013. Accessed February 12, 2014. <http://www.gcsb.govt.nz/newsroom/annual-reports/Annual%20Report%202013.pdf>. Accessed December 20, 2013, p 14

response.¹³² Its objectives are to raise understanding and awareness among small businesses and individuals, improve government cyber-security, and improve cyber-security in critical infrastructure. In 2013, the NCSC delivered a range of education initiatives to help increase New Zealand organisations' preparedness to respond to cyber incidents and increase the resilience of New Zealand's information networks and critical infrastructures.¹³³

As part of its functions, the NCSC receives and records cyber-security incidents that are reported against New Zealand targets.¹³⁴ The NCSC 2012 Incident Report stated that in 2012 there was an increase in the number of incidents reported, from a total of 90 in 2011 to a total of 134 in 2012.¹³⁵ The largest category of reported activity was 'scam & spam' related, which made up 31% of the incidents captured. Denial of service (DoS) attacks and botnet/malware activity were the second largest categories, making up 16% and 14% of incidents respectively.¹³⁶ Of these, 60% of the incidents reported to NCSC originated from an overseas source; (31%) of reported incidents originated from domestic sources; and 9% of incidents were unable to be attributed to a specific origin.¹³⁷ Almost three-quarters of these attacks were directed against individuals and private sector organisations, with less than a quarter directed at government or critical national infrastructure.¹³⁸

International data suggests that 133,000 New Zealanders per annum are victims of identity fraud (the majority of cases having a cyber-element), with around one third of that number falling victim to identity theft and two thirds falling victim to credit or bank card fraud.¹³⁹ A 2011 global economic crime survey ranked New Zealand as fourth out of 78 countries in terms of reported fraud.¹⁴⁰ Of these, cyber-crime was responsible for almost a quarter of the reported fraud events. The NCSC estimates New Zealanders lose up to \$500m annually due

¹³² New Zealand's Cyber Security Strategy: June 2011, p 2-3

¹³³ GCSB Annual Report 2013, p 18

¹³⁴ *National Cyber Security Centre (NCSC)*, "2012 Incident Summary", (Wellington: NCSC, 2012), http://ncsc.govt.nz/sites/default/files/articles/NCSC-%202012%20Incident%20Report_0.pdf, accessed 17 January 2012, p 2

¹³⁵ While this may be attributable to a greater awareness of the importance of reporting incidents and of the role the NCSC performs, incidents must meet a certain threshold and criteria before being included in the report. See NCSC (2012), p 2

¹³⁶ NCSC (2012), p 2

¹³⁷ *ibid*, p 4

¹³⁸ *ibid*, p 5

¹³⁹ New Zealand's Cyber Security Strategy: June 2011, p 4

¹⁴⁰ PriceWaterhouseCoopers, "The 2011 Global Economic Crime Survey results for New Zealand Fraud, fraudsters and cybercrime". (PWC New Zealand, November 2011). Accessed 12 January 2014, www.pwc.co.nz/KenticoFiles/b2/b2ba49bb-785c-493c-aeef-a39a52803dc5.pdf, p 3

to cyber-borne frauds and scams,¹⁴¹ with 70% of New Zealand adults having fallen victim to some form of cyber-crime in the form of computer scams, fraud and viruses/malware.¹⁴² Other reports conservatively estimated that cyber-related crimes cost New Zealand enterprise an estimated \$625 million in 2011.¹⁴³ The cost of loss of intellectual property as a result of cyber intrusions into private sector entities is exceptionally difficult to quantify in monetary terms, in part because companies are reluctant to report losses or may not even know their property has been stolen. However, based on the scale of intrusions and exfiltration seen in other jurisdictions and the number of intrusions reported in New Zealand, the potential costs to New Zealand of cyber-based industrial espionage are likely to be significant.

More broadly, the impact of cyber threats to New Zealand is difficult to calculate with any precision, partly because of the complex nature of any potential attack. If a major attack were directed at government agencies, critical national infrastructure providers (for example telecommunications networks or water supply), or companies that drive New Zealand's economy, there could be significant disruption to commercial and personal activities.¹⁴⁴ The use of botnets or targeting of individuals would also add significant costs and disruptions at a personal level rather than at a state level. A recently conducted study determined that globally, cyber-crime and cyber espionage result in up to one trillion US dollars in annual global losses.¹⁴⁵

16. New Zealand Cyber-Security Strategies

As a small state dependant on foreign trade and a liberal rules-based international system, New Zealand's foreign policy has varied between alliances, institutional cooperation and norm promotion. Membership of security alliances such as the Five Eyes alliance allows New Zealand to compensate for its small size and lack of global reach, and enables New Zealand

¹⁴¹ Chhana, p 3

¹⁴² New Zealand's Cyber Security Strategy: June 2011, p 4

¹⁴³ Birchfield (2013), p1 Reg Birchfield, "Cyber Crime: Cyber Threats and Data Privacy." (New Zealand Management, April 2013). Accessed February 12, 2011, www.management.co.nz/Editorial.asp?eID=64698&Wcat=102, p 1

¹⁴⁴ Chhana, p 3

¹⁴⁵ Centre for Strategic and International Studies, "The Economic Impact of Cybercrime and Cyber Espionage", (California: McAfee, July 2013), p 5

to be a better informed player on the world stage than would otherwise be the case.¹⁴⁶ Intelligence collection and dissemination are important approaches that can increase New Zealand's ability to deter attacks, or identify perpetrators and retaliate if necessary. New Zealand has two central intelligence collection agencies: the GCSB and the New Zealand Security Intelligence Service (NZSIS). New Zealand's main contributing government agency to the Five Eyes intelligence system is the GCSB, which shares information with its partner agencies abroad, including the NSA, GCHQ, the Australian Signals Directorate (ASD), and Canada's Communications Security Establishment (CSE).

GCSB is responsible for SIGINT with a foreign focus. The agency does not have the legislative ability to spy on New Zealanders independently unless certain criteria are met, such as the individual being designated an 'agent of a foreign power'. The NZSIS is responsible for New Zealand's HUMINT collection, and is unique amongst the Five Eyes in having both a domestic and foreign focus.

Given the high costs of intelligence collection, membership of the Five Eyes provides a very substantial net economic benefit to New Zealand.¹⁴⁷ As the smallest member state in terms of both geographic and economic size, this security alliance grants New Zealand access to intelligence resources far beyond the capabilities of a small states, and is a strong signal of deterrence for potential aggressors.

While New Zealand may be the net beneficiary of this agreement, the cooperation between these countries is of value to each partner as none of the Five Eyes states would be able to operate a global system on its own. Indeed, the relationships fostered by this alliance are crucial to the United States' effort to secure its homeland, and necessary to its fight against terrorism. New Zealand's intelligence and military cooperation with these partners has recently been reinvigorated with the reinstatement of New Zealand to the Five Eyes¹⁴⁸ and the military and intelligence agreements known as the Wellington Declaration (2010) and Washington Declaration (2012).

¹⁴⁶ GCSB Annual Report (2013), p 6

¹⁴⁷ Ibid

¹⁴⁸ While technically remaining a member of the Five Eyes alliance, New Zealand was effectively ostracized as a consequence of its anti-nuclear stance. This relationship has since thawed, due in part to the US' strategic 'pivot' to the Asia-Pacific region.

More broadly, New Zealand has focused on extending international security alliances on cyber-security. In June 2012, New Zealand entered into an Individual Partnership Cooperation Programme with the North Atlantic Treaty Organisation (NATO), which provides for consultation and cooperation on cyber-security issues and continued intelligence sharing.¹⁴⁹ Agreements have also been entered into with the UK and Australia. Domestically, the New Zealand Government has also entered into partnerships with private sector enterprises, ensuring that the benefit of these international partnerships provides benefit to the entire spectrum of New Zealand national infrastructure and intellectual property protection. UNSC Resolutions 1267 (1999) and 1989 (2011) specifically oblige New Zealand to take action against those terrorist entities it lists.¹⁵⁰ This includes co-operating with the UN and its member states, and supporting the numerous resolutions ratified by the UN that aim to suppress international terrorism, including ratifying eight of the 12 conventions in the decades prior to the new millennium.¹⁵¹ UNSC Resolution 1373 (2001),¹⁵² adopted on 28 September 2001, voiced the UN's unequivocal condemnation of the terrorist attacks and reaffirmed the need to combat by all means.¹⁵³ The resolution was adopted in accordance with the UN Charter regarding threats to international peace and security caused by terrorist acts, and was binding on all UN member states.¹⁵⁴ The resolution obliges New Zealand to outlaw the financing of, participation in and recruitment to, terrorist entities.¹⁵⁵ Among other tasks, this resolution obligated all member states to enact "additional measures to prevent and suppress, in their territories through all lawful means, the financing and

¹⁴⁹ New Zealand Government Ministry of Foreign Affairs and Trade, "Individual Partnership and Co-operation Programme between New Zealand and NATO" (June 2012), available at: http://www.beehive.govt.nz/sites/all/files/downloads/disarmament/New_Zealand_NATO_Partnership_and_Cooperation_Programme%20Zealand%20-%20NATO%20Partnership%20and%20Cooperation%20Programme.pdf (accessed 25 January 2014)

¹⁵⁰ New Zealand Police. "Police Designated Terrorist Entities", Accessed 17 January 2014, <http://www.police.govt.nz/advice/personal-community/counterterrorism/designated-entities>

¹⁵¹ Conte, Alex. *Counter-Terrorism and Human Rights in New Zealand*. (Wellington: New Zealand Law Foundation, 2007), pp 338 and 340

¹⁵² United Nations Security Council. "Resolution 1373 (2001): Threats to international peace and security caused by terrorist acts]." (*United Nations Security Council Resolution*. September 28, 2001). Accessed February 22, 2014. <http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N01/557/43/PDF/N0155743.pdf?OpenElement>.

¹⁵³ Ibid

¹⁵⁴ United Nations Security Council. "Security Council Unanimously Adopts Wide-Ranging Anti-Terrorism Resolution; Calls for Suppressing Financing, Improving International Cooperation." (*Press Release*. September 28, 2001). Accessed February 22, 2014. <http://www.un.org/News/Press/docs/2001/sc7158.doc.htm>

¹⁵⁵ United Nations Security Council UN Resolution 1373 (28 September 2001) [hereafter UN Resolution 1373]

preparation of any acts of terrorism.”¹⁵⁶ The resolution does not specifically identify those terrorist entities, so effectively leaves it to member states to identify the entities against which they should act.¹⁵⁷ The resolution imposed a binding obligation under Chapter VII of the UN Charter, and was regarded as one of the “one of the most strongly worded resolutions in the history of the Security Council.”¹⁵⁸

The resolution had significant consequences for both international and New Zealand domestic law and laid the foundation for anti-terrorism legislation in the years to come. The meaning, scope, and implementation strategy of UNSC Resolution 1373 immediately became part of a considerable debate among New Zealand policy-makers, as well as their counterparts around the world. Its effects are still being felt over a decade later, not only in terms of the legislation that has been enacted, but also due to the urgency and extent to which UN member states were required to amend existing domestic law to comply with the provisions of the resolution.

17. New Zealand's Security Legislation

Yet for all the focus on countering international terrorism, there remains a decided absence of broad institutional cooperation and cyber-security norms to address the increasing threat of cyber-attacks. In order to respond to these growing challenges, New Zealand has taken steps to enhance its domestic cyber-security capacity.¹⁵⁹ In many cases, New Zealand did not have relevant security legislation that could address the emerging cyber threats, or if it did it predated the modern debate on privacy and security by many years. New legislation was not enacted simultaneously but was instead brought into law progressively, building upon the advances of prior legislation or seeking to address new technologies or threats that were not previously covered. To understand the effect on privacy and security, this thesis will now examine the major legislative changes that have occurred in New Zealand since the September 2001 attacks on the US:

Terrorist Suppression Act 2002

¹⁵⁶ Ibid, Preamble, s 1

¹⁵⁷ NZ Police – New Zealand’s designated terrorist individuals and organisations“ Designated Terrorist Entities”

¹⁵⁸ Conte, p 342

¹⁵⁹ Burton (2013), p 228

The Terrorist Suppression Act was passed in late 2002 and is considered New Zealand's first legislative reaction to the September 11 terrorist attacks.¹⁶⁰ This is worth noting as subsequent cyber-focused legislation used this Act as its foundation, which will be discussed shortly. First introduced to Parliament as the Terrorism (Bombing and Financing) Bill in April 2001 (pre 9/11), it proposed to criminalise the financing of terrorist acts and use of explosive devices in accordance with these international conventions. These were comparatively uncontroversial goals, reflected by the fact that, despite a public invitation, the Foreign Affairs, Defence and Trade Committee considering the Bill received no submissions on it.¹⁶¹ Before the Bill could be presented before Parliament, the September 11, 2001 terrorist attacks on the US occurred. The force and devastation of the attack rippled across the globe, with calls for the use of all necessary force to counter the threat of global terrorism.¹⁶² New Zealand joined with these calls during the first sitting of Parliament following the attacks, and, with the exception perhaps of the Green Party, issued passionate calls for support of forceful international efforts against terrorism immediately following the attacks.¹⁶³

Following those tragic events, the members of the Foreign Affairs, Defence and Trade Committee were called upon to review the adequacy of the original terrorism Bill that they had been preparing to submit to the House of Representatives.¹⁶⁴ The Chairperson of the Committee at the time, Graham Kelly, called the terror attack "horrific" and notes that it destroyed preconceived ideas of security and stability in the world: "It was like tearing down everything and starting from scratch."¹⁶⁵ The Bill was subsequently sent back for further review, and major proposed amendments were introduced by way of a Supplementary Order Paper.¹⁶⁶ This time the proposed Bill received significant comment from the public and civil liberties groups, with 140 submissions being received. The Bill was seen by some as having "a major chilling effect on dissent", or, even more troubling, as being "one giant step towards a police state".¹⁶⁷ Objections to the Bill were directed at the obligations and powers

¹⁶⁰ John E Smith, *New Zealand's Anti-Terrorism Campaign: Balancing Civil Liberties, National Security, And International Responsibilities*, (Wellington: Fullbright, December 2003), p 3

¹⁶¹ Smith, p 15

¹⁶² Hon Jim Anderton (12 September 2001) 595 NZPD 11615

¹⁶³ Smith, p 16

¹⁶⁴ Ibid, p 18

¹⁶⁵ Ibid, p 16

¹⁶⁶ Tim McBride, "Heightened State Surveillance in New Zealand, Post-"9/11" - Privacy under Threat", Accessed 18 December 2013, www.timmcbridelaw.co.nz/images/pdfs/TimMcBride_Surveillance.pdf, p 4

¹⁶⁷ McBride, p 4

that it proposed for the NZSIS, GCSB and Police, the ability to designate individuals as terrorists, and new surveillance obligations placed on banks, financial organisations and lawyers.¹⁶⁸

Despite these concerns, the Bill became law in late 2002 with few significant changes. This gave effect to New Zealand's obligations under the International Convention for the Suppression of Terrorist Bombings 1997, the International Convention for the Suppression of Financing of Terrorism 1999, and many of New Zealand's obligations under UNSC Resolution 1373.¹⁶⁹ Police would take the lead role in initiating the process of designating individuals as terrorists, and after collecting, collating, assessing and analysing relevant data, would make a preliminary decision that would then be released for consultation with other relevant government departments. Wilkes publicity of the station, Muldoon was forced to publically admit to the existence and role of the GCSB about two months later.¹⁷⁰ Unlike the SIS, the GCSB did not have its own Act of Parliament and operated without statutory basis until 2003.

Counter-Terrorism Bill 2003

The Counter-Terrorism Bill 2003 was designed to complement the Terrorism Suppression Act 2002 by closing potential gaps that may be exploited by terrorists,¹⁷¹ and ensure that New Zealand had a comprehensive legislative framework in place to help to prevent, and to deal with, terrorist offending.¹⁷² The Bill introduced new terrorism-related offences and penalties, and greatly extended state powers to lawfully intercept private communications where terrorist offences were suspected.¹⁷³ Unlike the Terrorism Suppression Act 2002, the 2003 Counter-Terrorism Bill was much more broadly focused and was "a further step by this Government to ensure that we have in place a full range of measures to prevent or respond

¹⁶⁸ 2002 No 34, *Terrorism Suppression Act 2002*, assented 17 October 2002, part 2 s 43

¹⁶⁹ *Review of the Terrorism Suppression Act 2002*, (Wellington: Foreign Affairs, Defence and Trade Committee, November 2005), Accessed 12 January 2014, www.parliament.nz/resource/0000002749, p 3

¹⁷⁰ *Ibid*, p 85

¹⁷¹ "Counter-Terrorism Bill: First Reading." (*Hansard (debates)*, vol. 607, week 20, April 1, 2003). Accessed January 12, 2014. www.parliament.nz/en-nz/pb/debates/debates/47HansD_20030402_00000001/counter-terrorism-bill-%E2%80%94-first-reading. (P Goff)

¹⁷² *Ibid*

¹⁷³ McBride, p 3

to any effort by terrorists to operate here in our country.”¹⁷⁴ A range of new criminal offences were also proposed, although not all of these were specific to terrorism.¹⁷⁵ These proposals implemented into New Zealand law the requirements of two international conventions: the Convention on the Physical Protection of Nuclear Material and the Convention on the Marking of Plastic Explosives for the Purpose of Detection, and included provisions from UNSC Resolution 1373.¹⁷⁶ Furthermore, to assist Police investigations of terrorist incidents, the Bill proposed a range of measures including permitting Police executing a search warrant to require a person, under threat of criminal penalty, to provide information or assistance that was deemed ‘reasonable and necessary’ to allow access to a computer on premises covered by the warrant.¹⁷⁷

A number of the Bill’s provisions drew concern from prominent civil liberties groups.¹⁷⁸ These concerns primarily focused on the use of tracking devices to covertly track the movement of individuals.¹⁷⁹ Until that time, New Zealand had not legislated standards for the use of most types of technologically-assisted physical surveillance for law enforcement purposes, unlike many comparable jurisdictions.¹⁸⁰ The Privacy Commissioner of the time, Bruce Slane, neatly summarised the privacy concerns in stating

“The use of electronic devices to secretly track the movement of individuals is worrying from a privacy viewpoint. The ability to travel without being systemically observed, and not to have to account for every movement to the

¹⁷⁴ New Zealand. “Counter-Terrorism Bill —: Second Reading.” Hansard (debates), vol. 612, week 39 (October 14, 2003). www.parliament.nz/en-nz/pb/debates/debates/47HansD_20031014_00001157/counter-terrorism-bill-%E2%80%94-second-reading. (P Goff)

¹⁷⁵ The new offences included: infecting animals with disease; contamination of food, crops, water, or other products intended for human consumption; threatening or falsely communicating information about harm to persons or property; harbouring or concealing terrorists; and dealing with radioactive material. Terrorism also would become an aggravating factor for sentencing purposes under the Sentencing Act 2002. (Counter-Terrorism Bill 2003)

¹⁷⁶ Smith, p 31

¹⁷⁷ 2003 No 27-2, *Counter-Terrorism Bill 2003*, (not assented). p 3

¹⁷⁸ *Counter-Terrorism Bill 2003 (Supplementary Order Papers 2003 Nos. 163 and 164)*. (Wellington: New Zealand Parliamentary Library, 2003).

¹⁷⁹ The definition provided by section 200A of the Bill was as follows: ‘Tracking device means a device that, when installed in or on any thing, may be used to help ascertain, by electronic or other means, the location of any thing or person.’

¹⁸⁰ Bruce, Slane. *Report by the Privacy Commissioner to the Minister of Justice in relation to the Counter-Terrorism Bill*. (February 7, 2003). Accessed February 7, 2014. www.privacy.org.nz/news-and-publications/reports-to-parliament-and-government/counter-terrorism-bill/, section 3.1

State, are important freedoms. Freedom from surveillance is such an ordinary expectation that one hardly gives a thought to it. However, to become aware that one is, or has been, under surveillance is a devastating blow to a sense of privacy, dignity, and autonomy.”¹⁸¹

Despite these concerns, the Privacy Commissioner supported the enactment of the legislation as the need for judicial authorisation, by way of a tracking warrant, was an important protection. Judges were “experienced, thoughtful and intelligent people, independent from the surveillance organisations” who were required to consider privacy when considering a warrant application.¹⁸²

Twenty-five public submissions were received on the Bill, including submissions from legal experts and civil liberties groups.¹⁸³ These submissions were largely against the Bill due to its fundamental impact on privacy and civil liberties, despite advice from Crown Law that the Bill was consistent with the rights and freedoms affirmed in the Bill of Rights Act.¹⁸⁴ And although widely accepted by Parliament, the bill drew significant criticism from the Green Party. The Foreign Affairs, Defence and Trade Committee considering the Bill recommended a number of amendments, including under the clause requiring persons to help Police armed with a warrant to access a computer, where persons would not be forced to provide any information tending to incriminate them, but might be required to provide information or assistance that would enable Police to access a computer containing information that may be incriminating.¹⁸⁵

The Green Party alleged that requiring persons to provide information or assistance to enable Police to access computer files violated the long-held common law privilege against self-incrimination, stating that “it is contradictory that the Bill... allow[s] a suspect to withhold ‘information tending to incriminate’ yet not apply that provision to information

¹⁸¹ Ibid, section 3.2

¹⁸² Ibid, section 3.2

¹⁸³ “Counter-Terrorism Bill: Government Bill”. As reported from the Foreign Affairs, Defence and Trade Committee. August 8, 2003. Accessed February 12, 2014. www.parliament.nz/resource/0000018928, p 15

¹⁸⁴ Butler, Andrew. *Explanatory Note: Counter-Terrorism Bill 2002*. Wellington: Ministry of Justice, 2003. Accessed February 6, 2014. www.justice.govt.nz/policy/constitutional-law-and-human-rights/human-rights/bill-of-rights/counter-terrorism-bill-2002.

¹⁸⁵ Select Foreign Affairs, Defence and Trade Committee Report on Counter-Terrorism Bill, p 10

sitting on the suspect's computer."¹⁸⁶ The Green Party believed that this provision may lead to 'fishing expeditions' to check for evidence of criminal behaviour on a suspect's computer.¹⁸⁷ Together with further concerns about the designation of terrorist groups proposed by the Bill, the Green Party was first and foremost seeking to protect rights of activists to protest.¹⁸⁸ In a speech to Parliament, Green Party MP Keith Locke stated:

*"There is a growing recognition in New Zealand and around the world that the so-called war against terrorism is being used for unjustified restrictions on civil liberties... We do not need to undermine civil liberties in the fight against terrorism. To do so is to concede a point to the terrorists, whose aim is to restrict civil liberties, not increase them. I think that we should not, under the guise of counter-terrorism - as in this bill - introduce general changes to our criminal law that restrict and undermine the civil liberties that we have long enjoyed: the right to avoid self-incrimination; the right to privacy in our life, including today in our computer files; the right not to be tracked throughout our travels; and the right to freedom of speech and protest without being subject potentially to designation as a terrorist by a political figure such as a Prime Minister under the Terrorism Suppression Act."*¹⁸⁹

The Green Party's fervent argument against the Bill had some effect; the Bill was divided and enacted as six separate bills, one for each statute the Bill would amend:

- the Crimes Amendment Bill 2003
- the Terrorism Suppression Amendment Bill 2003
- the Misuse of Drugs Amendment Bill 2003
- the New Zealand Security Intelligence Service Amendment Bill 2003
- the Sentencing Amendment Bill 2003
- the Summary Proceedings Amendment Bill 2003.

¹⁸⁶ Ibid, p 34

¹⁸⁷ "Counter-Terrorism Bill: Second Reading." (*Hansard (debates)*, vol. 612, week 39, October 14, 2003). www.parliament.nz/en-nz/pb/debates/debates/47HansD_20031014_00001157/counter-terrorism-bill-%E2%80%94-second-reading, p 1

¹⁸⁸ Ibid, p 1

¹⁸⁹ Ibid

All parties but the Greens ultimately supported each Bill on its third reading, with the exception of the Summary Proceedings Bill, which also was opposed by the ACT Party's eight members.¹⁹⁰

Crimes Amendment Act 2003

In September 1999, the New Zealand Government introduced the Crimes Amendment Bill (No 6) to update the Crimes Act 1961.¹⁹¹ Initially the Bill contained a range of proposed changes to update the Crimes Act, and proposed a number of provisions relating to crimes involving the use of computers. The proposed changes addressed the findings of a 1999 Law Commission report that found that "the current criminal law was inadequate to deal with the unauthorised interception of electronic data."¹⁹² The Law Commission report, titled "Computer Misuse", referred to a situation where the effects of computer misuse may be felt in New Zealand even though neither the hacker nor the computer were situated within the country, citing the following case as an example of where this had occurred:

*"Recently in New Zealand there have been two widely publicised incidents involving computer misuse. In November 1998, a computer hacker erased some 4,500 "lhug" websites. The lhug server was based in California and the sites were hosted by Auckland-based Internet service provider, the Internet Group. There was no backup facility and, unless the owners of the websites made their own copies, the web pages were lost permanently."*¹⁹³

The report noted that New Zealand did not have criminal offences dealing specifically with such conduct, and that the criminal offences that existed might have been perceived as inadequate to deal with computer misuse.¹⁹⁴ The Law Commission recommended that "new offences dealing specifically with computer misuse should be created and that such offences should be located in a separate statute or in a distinct part of the Crimes Act 1961",¹⁹⁵ and

¹⁹⁰ Smith, p 35

¹⁹¹ Crimes Amendment Bill (No 6) — Consideration of Report of Law and Order Committee

¹⁹² New Zealand Law Commission. *Computer Misuse*. (Wellington: Law Commission, 1999), s 3 p 54

¹⁹³ Ibid, s 3 p 25

¹⁹⁴ Ibid, s 3 p 24

¹⁹⁵ Ibid, s 5 p 88

suggested that four offences be created in regards to the unauthorised interception, access, use or damage of data stored in a computer.¹⁹⁶

In November 2000, Supplementary Order Paper (SOP) No 85 was introduced to Parliament. Dubbed the 'cyber snooping bill',¹⁹⁷ the SOP significantly changed the nature and scope of the changes initially proposed by the Crime Amendment Bill (No 6). Section 16B established the offence of using a listening device to intercept a private conversation, although exempting the NZSIS and GCSB from these offences. This effectively allowed the NZSIS and GCSB to access data without authorisation other than an interception warrant. Critics argued that the SOP significantly increased state surveillance powers by exempting these major state agencies from the computer hacking offences proposed in the 1999 Crimes Amendment Bill.¹⁹⁸ While an exemption for the NZSIS already existed under the 1961 Crimes Act,¹⁹⁹ the inclusion of the GCSB was of concern as the GCSB was at the time not legislated.

A report from the Privacy Commissioner supported the SOP for broadening "crimes against personal privacy" by including the interception of non-oral private communications within the prohibition against intercepting private communications, and creating a new offence of accessing a computer system without authorisation.²⁰⁰ However, the report saw the proposed exceptions for the GCSB as representing a risk to privacy, stating:

"I accept that there is a case to create appropriate exemptions to these new laws. It is essential that covert interception and computer access be limited to the level absolutely necessary to enable the relevant agencies to perform their proper functions. It must be subject to careful authorisation processes and operational controls, and be proportionate to the intrusion on privacy. My principal concerns about the bill relate to the exemptions and, in particular, to the lack of controls on ISPs and GCSB in relation to the

¹⁹⁶ Ibid, s 3 p 90 - 93

¹⁹⁷ McBride, p 7

¹⁹⁸ Ibid

¹⁹⁹ 1961 No 43, *New Zealand Crimes Act 1961*, assented 1 November 1961, s 253

²⁰⁰ Bruce Slane, "Crimes against personal privacy and crimes involving computers: Intercepting private communications and accessing computer systems without authorization". (Wellington: Office of the Privacy Commissioner, (13 December 2000), Accessed 03 January 2014, www.privacy.org.nz/assets/Files/Reports-to-ParlGovt/Report-by-Privacy-Commissioner-on-Supplementary-Order-Paper-No.-85-to-the-Crimes-Amendment-Bill-No.6-2000.pdf, p 3

expanded interception offence, and to the law enforcement and GCSB exemption in relation to the computer access offence. In each case, I suggest law changes which would more appropriately protect privacy while allowing such exemptions.”²⁰¹

and further

“I have two principal concerns at granting GCSB this exemption. First, although the Bureau is an important government intelligence agency it is not established by any statute. This lack of a statutory basis means that Parliament has had little say as to the constitution and activities of the agency and Parliament and the public has no real way of knowing precisely who GCSB is or what it does. If GCSB were to completely change the character of its activities next week, the public and Parliament would be unaware of whether it was continuing to fulfil a function for which an exemption from the criminal law is warranted. Placing GCSB on a statutory basis would bring benefits in terms of certainty, transparency and accountability depending upon how the statute were to be written.”²⁰²

The report proposed that, as a prerequisite to granting an exemption for the GCSB, the agency be placed on a statutory footing and be “subject to a statutory warrant process for the undertaking of any intrusive activity, particularly where that activity would constitute a breach of the law.”²⁰³ Submitted to the Minister of Justice in December 2000, the report noted that a GCSB statute had already been proposed, namely the Government Communications Security Bureau Act. The GCSB received royal assent on 1 April 2003, with the Crimes Amendment Act receiving royal assent just months later on 7 July 2003.²⁰⁴

Government Communications Security Bureau Act 2003

Until the establishment of the GCSB, New Zealand’s SIGINT capability and technical security (TECSEC) had been provided by bodies such as the New Zealand Defence Force and the

²⁰¹ Ibid, p 21 s 5.2

²⁰² Ibid, p 6 s 3.2.3

²⁰³ Ibid, p 7 s 3.2.5

²⁰⁴ 2003 No 39, Crimes Amendment Act 2003, assented 07 July 2003.

NZSIS.²⁰⁵ The Government of Prime Minister Robert Muldoon established the GCSB in 1977, and these functions became the responsibility of a sole agency (although the NZDF and NZSIS still retained some of their previous capabilities in this respect).²⁰⁶ The GCSB's existence was not disclosed to Cabinet and the Leader of the Opposition until 1980, and even then its SIGINT capability was not revealed. The public first learned of the agency's existence in 1984 when peace researcher Owen Wilkes revealed the existence of a GCSB radio communications interception facility in Manawatū, known as the Tangimoana station.²⁰⁷ The station had been opened in late 1981 and kept a secret from the New Zealand public. Its existence was only revealed by chance, when Wilkes accidentally discovered the station while holidaying on a friend's farm nearby.²⁰⁸ According to New Zealand writer Nicky Hager, "after years of research into intelligence issues in Europe, Wilkes was probably the only person in New Zealand who could have recognised the distinctive signals intelligence aerials as being something different from the normal radio facilities providing communications for the nearby Air Force base."²⁰⁹ Following Wilkes' publicity of the station, Muldoon was forced to publically admit the existence and role of the GCSB.²¹⁰

Unlike the NZSIS, the GCSB did not have its own Act of Parliament and operated without statutory basis until 2003. In early 2000 it was decided that the GCSB should be placed on a statutory footing similar to that of the NZSIS, and the legislative and public consultation process began.²¹¹ This culminated in the 2003 Government Communications Security Bureau Act being enacted in late 2003. Under the Act, the objective of the GCSB was to contribute to the national security of New Zealand, the international relations and well-being of New Zealand, and the economic well-being of New Zealand.²¹² To accomplish these objectives, the functions of the GCSB were identified as information assurance and cybersecurity, intelligence gathering and analysis, and co-operation with other entities to facilitate their

²⁰⁵ Government Communications Security Bureau, "History of the GCSB", accessed 12 January 2014, www.gcsb.govt.nz/about-us/history.html

²⁰⁶ Ibid

²⁰⁷ Nicky Hager, *Secret Power: New Zealand's Role in the International Spy Network*. (Nelson: Craig Potton Publishing, 1996), p 84

²⁰⁸ Ibid

²⁰⁹ Ibid

²¹⁰ Hager (1996), p 85

²¹¹ Government Communications Security Bureau, "History of the GCSB"

²¹² 2003 No 9, Government Communications Security Bureau Act 2003 (hereafter, assented 01 April 2003. Hereafter GCSB Act 2003)

functions.²¹³ This gave the GCSB jurisdiction to collect, decipher, translate, examine and analyse any foreign communication emanating from a foreign organisation.²¹⁴ Additionally, although the GCSB was not permitted to monitor the communications of New Zealand citizens or organisations, it was able to assist other New Zealand government agencies acting under judicial warrant to do so, and could also monitor any New Zealanders deemed to be an “agent of a foreign power”.²¹⁵

The Act formalised the role of the GCSB as the national authority for signals intelligence and information systems security.²¹⁶ As with the NZSIS, the minister in charge of the GCSB was the Prime Minister, but further external oversight was provided by the Inspector-General of Intelligence and Security Act 1996²¹⁷ and the Intelligence and Security Committee Act 1996.²¹⁸ While New Zealand’s Privacy Commissioner, Human Rights Commission, and Law Society all favoured formalising the GCSB’s role and functions by way of statute, others were not convinced.²¹⁹ The Green Party was completely opposed as they saw ‘legalising’ the GCSB posed a ‘major threat’ to individual privacy and undermined the independence of New Zealand’s foreign policy.²²⁰

Telecommunications (Interception Capability) Act 2004

Introduced to Parliament in 2003, the 2004 Telecommunications (Interception Capability) Act was an important precedent in New Zealand legislation as for the first time it legislated the lawful interception of data as a form of communication. The Act was a companion to the section of the 2003 Crimes Amendment Bill (no 6) that required telecommunications network operators to have all their systems intercept capable, and sought to achieve greater effectiveness in New Zealand’s law enforcement and security.

The Act obligated telecommunications companies and Internet Service Providers (ISPs) to have an interception capability and to assist surveillance agencies acting under an

²¹³ GCSB 2003

²¹⁴ Ibid

²¹⁵ Kitteridge, p 32

²¹⁶ "History of the GCSB"

²¹⁷ 2013 No 58, *Inspector-General of Intelligence and Security Act 2013*, assented 21 August 2013

²¹⁸ 1996 No 46, *Intelligence and Security Committee Act 1996*, assented 1 July 1996

²¹⁹ McBride, p 4

²²⁰ Ibid

interception warrant.²²¹ New Zealand's surveillance agencies acting under a judicial interception warrant were now allowed to access to the emails, Internet browsing, calls, texts and location for mobile phones of private citizens and businesses. Previously, interception warrants had been limited to voice communication or the ability to implant listening devices. Pursuant to section 7(1) and section 16(1)(a) of the 2004 Telecommunications (Interception Capability) Act, public switched telephone network were required to be compliant within 18 months of the Act's commencement, and public data networks by April 2009.²²² NZ\$7.92 million was budgeted for in the Police appropriations budget for the period of 2007 – 2010 to subsidise companies wiring surveillance devices into their telecommunications networks.²²³

Importantly, the Act did not in any way alter the authority of Police or intelligence and security agencies to intercept telecommunications, nor did it reduce the checks and balances on how these agencies accessed and used private communications information.²²⁴ Instead, ISPs were presented with an interception warrant and collected the relevant data, forwarding this on to the appropriate authorities.²²⁵ This important detail ensures intelligence agencies are not granted full access data held by ISPs, but instead are only granted access to relevant data they are legally entitled to under warrant. Despite this, the Act drew its fair share of detractors. The Green Party opposed that law on the grounds that it gave New Zealand's intelligence agencies great powers to spy on New Zealanders' online activity.²²⁶ Civil Liberties Council spokesman Michael Bott said the new surveillance capabilities were part of a step-by-step erosion of civil rights in New Zealand.²²⁷ "The fear is that citizens become accustomed to living in a surveillance society and, over time, freedoms of speech and belief are chilled and diminished."²²⁸ Yet the Act included the principle that the privacy of telecommunications that are not subject to an interception warrant or any

²²¹ 2004 No 19, *Telecommunications (Interception Capability) Act 2004*, assented to 05 April 2004, Part 2 s 7 (1)

²²² Ibid, Part 2 s 15 (1a)

²²³ New Zealand Police Appropriations budgets 2007/10

²²⁴ "Telecommunications (Interception Capability and Security) Bill — First Reading." *Hansard (debates)*, vol. 689, week 41 (May 8, 2013). Accessed February 12, 2014. www.parliament.nz/en-nz/pb/debates/debates/50HansD_20130508_00000028/telecommunications-interception-capability-and-security. (A Adams)

²²⁵ 2004 No 19, *Telecommunications (Interception Capability) Act 2004*, assented to 05 April 2004, Part 2 s 8 (2)

²²⁶ *Telecommunications (Interception Capability and Security) Bill - First Reading - Part 5*

²²⁷ Hager (2010)

²²⁸ Ibid

other lawful interception authority must be maintained to the extent provided for in law,²²⁹ and the principle that the interception of telecommunications, when authorised under an interception warrant or any other lawful interception authority, must be carried out without unduly interfering with any telecommunications.²³⁰

Nicky Hager claimed that the Act was the result of a decade of lobbying by American agencies such as the FBI.²³¹ This claim was based upon an investigation completed by British researchers that had unveiled a move by the European Union to create a “seamless web of telecommunications surveillance” across Europe.²³² Known as Enfopol 98, the plan involved EU nations adopting the “International User Requirements for Interception (IUR)” to standardise surveillance capabilities. This would allow the data including credit card numbers, Personal Identification Number (PIN) codes, email addresses, and computer logon identities and passwords to be passed between EU nations. Hager claimed New Zealand had been in discussion with the US and European authorities on joining the scheme from as early as 1995.²³³

Police Association vice-president Stuart Mills said that the breadth of the new capabilities was justified because “criminal networks are using the Internet and other new technologies to communicate.”²³⁴ In a 2001 Cabinet committee policy paper, Police said that the NZSIS was “impeded in its ability to intercept or decrypt an increasing number of communications”, which restricted the NZSIS’s ability “to contribute to the international effort to restrict terrorism.”²³⁵

New Zealand’s Privacy Commissioner at the time, Marie Shroff, warned Ministers through a Cabinet committee paper that modifying telecommunications networks for Police and intelligence agencies impacted on privacy by providing “enhanced opportunities for unauthorised interceptions by third parties.”²³⁶ This danger was highlighted by what was

²²⁹ Telecommunications (Interception Capability) Act 2004, Part 1 s 6 (6a)

²³⁰ Ibid, Part 1 s 6 (6b)

²³¹ Nicky Hager. “FBI role in Big Brother’s sharper eyes, ears”. (January 3, 2010). Accessed January 19, 2014. www.nickyhager.info/fbi-role-in-big-brothers-sharper-eyes-ears/

²³² Ibid

²³³ Ibid

²³⁴ Ibid

²³⁵ Ibid

²³⁶ Nicky Hager. “Google case highlights risks in NZ law change”. (January 24, 2010). Accessed January 19, 2014. www.nickyhager.info/google-case-highlights-risks-in-nz-law-change/

known as the Greek Watergate. In 2004 and 2005, hackers gained access to Vodafone Greece's mobile system and to the built-in law enforcement interception capability, tapping months of calls of more than 100 mobile phones.²³⁷ While the identities of the perpetrators were never conclusively established, it was suspected that US intelligence agencies operating from the US Embassy in Athens were to blame.²³⁸ This served as an important warning of the danger of intelligence agencies operating without proper oversight and legislative control.

New Zealand Security Intelligence Service Amendment Act 2011

The Government introduced the NZSIS Amendment Bill under urgency to Parliament in December 2010, with the aim of updating and clarifying the New Zealand Security Intelligence Service Act 1969.²³⁹ The Bill modernised the warrant framework that applied to the NZSIS, specifically addressing technological changes and other factors that affected the value of the NZSIS seizure and interception warrants framework in the New Zealand Security Intelligence Service Act 1969.²⁴⁰ The proposed amendments ensured the law clearly identified the types of surveillance practices that could be lawfully utilised by the NZSIS, and the authorisations that were required.²⁴¹ The prevalent use of mobile phones and the Internet, and the ability to hide behind cyber-identities, had not been anticipated when the framework was outlined in the NZSIS Amendment Act 1977, and amongst several new definitions included in the Bill, the following definition of the term "facility" was provided:

"[A]n electronic address, phone number, account, electronic identifier or similar identifier, or device that enables: communications to take place between individuals; or communications to be sent to or from an identified

²³⁷ "Telecommunications (Interception Capability and Security) Bill: First Reading." (*Hansard (debates)*, vol. 689, week 41, May 8, 2013). Accessed February 12, 2014. www.parliament.nz/en-nz/pb/debates/debates/50HansD_20130508_00000028/telecommunications-interception-capability-and-security

²³⁸ Bryan-Low, Cassell. "Vodafone, Ericsson Get Hung Up in Greece's Phone-Tap Scandal: Bugging of Nation's Leaders Points to Security Holes, Sets off Multiple Probes". (*The Wall Street Journal*, June 21, 2006). Accessed January 12, 2014. <http://online.wsj.com/news/articles/SB115085571895085969>

²³⁹ Bills Digest (2010) New Zealand Security Intelligence Service Amendment Bill 2010259-2. Wellington: Parliamentary Counsel Office, 2011, p 1

²⁴⁰ New Zealand Security Intelligence Service. *Regulatory Impact Statement: Modernising NZSIS Legislation – High Priority Amendments*. (August 11, 2010). Accessed January 14, 2014. www.treasury.govt.nz/publications/informationreleases/ris/pdfs/ris-nzsis-nzsis-dec10.pdf, p 1

²⁴¹ "New Zealand Security Intelligence Service Amendment Bill — First Reading." (December 9 2010). Accessed February 12 2014, www.parliament.nz/en-nz/pb/debates/debates/49HansD_20101209_00001287/new-zealand-security-intelligence-service-amendment-bill

*individual; or documents to be processed, stored, or accessed; and includes, without limitation, any of the following: a unique device identifier; a user account identifier; an Internet Protocol address; an email address; an Internet storage account (Part 1, Clause 5, definition of ‘facility’)*²⁴²

This provision allowed for warrants to be granted where specific facilities were known but the name or physical location of a subject was not known. This provision was deemed “a necessary update in an age where the use of attributable mobile phones and cyber-identities is common.”²⁴³

The proposed amendments were considered by some as long overdue in light of the significant technological advances that had occurred over the previous four decades. The regulatory impact statement by noted that “[a]spects of the NZSIS warrant framework, while remaining somewhat workable, have not kept pace with new technologies, law change, or modern requirements for intelligence acquisition.”²⁴⁴ The Law Commission noted that “[w]hile there are some impacts on privacy, this is clearly justified by the associated benefits. In particular, updating the warrant framework is a recognition of technological changes in the storage of and communication of information, and is essential in order to enable the NZSIS to continue to effectively undertake its statutory functions.”²⁴⁵

The regulatory impact statement prepared for the Intelligence and Security Committee considering the Bill identified six high priority amendments that, under the existing Act, required greater clarification.²⁴⁶ These ranged from clarifying the ability of the NZSIS to use electronic tracking devices, through to allowing greater flexibility in naming people assisting the NZSIS under warrant.²⁴⁷ It also included greater clarification in the area of computer-based surveillance. Under section 253 of the Crimes Act 1961, the NZSIS was provided a qualified exemption to the “access without authorisation” offence.²⁴⁸ The report offered that

²⁴² 2011 No 28, *New Zealand Security Intelligence Service Amendment Act 2011*, assented 12 July 2011.

²⁴³ *New Zealand Security Intelligence Service Amendment Bill — First Reading*, Chris Finlayson,

²⁴⁴ *Regulatory Impact Statement: Modernising NZSIS Legislation – High Priority Amendments*, p 1

²⁴⁵ *Ibid*, p 2

²⁴⁶ *Ibid*

²⁴⁷ *Ibid*

²⁴⁸ *New Zealand Crimes Act 1961*, s 253

the proposed amendments would “remove uncertainty for New Zealand intelligence agencies and other agencies acting under warrant.”²⁴⁹

Notably, the amendments did not propose to change the framework within which the NZSIS operated or seek to alter the thresholds associated with the issue of warrants.²⁵⁰ The Bill instead offered additional checks and balances to address what was considered powers that posed greater risks to individual privacy. These additional checks included the proposal to increase oversight on the warrants approval process by requiring that all NZSIS warrant applications to be approved by both the Commissioner of Security Warrants (a retired High Court Judge) and the Minister in charge of the NZSIS.²⁵¹ Under the existing legislation, dual approval was required only in respect of warrant applications for the surveillance of NZ citizens and residents. This proposal added “the independent and quasi-judicial” authority of the Commissioner of Security Warrants to the warrants process, with the intention of considerably strengthening accountability and oversight.²⁵²

Given its controversial nature, the Bill was not without its detractors. The Intelligence and Security Committee considering the Bill received and considered twenty-three submissions from interested groups and individuals regarding the Bill, and privately heard seven submissions in Wellington.²⁵³ In a submission by the Human Rights Commission, Chief Commissioner Rosslyn Noonan recognised the need to update the warrants scheme and address technology, but remained apprehensive about the Bill’s potential to dilute existing accountability and undermine democratic human rights protections.²⁵⁴ The Commission recommended including an explicit reference to human rights principles in the Bill to address “the concerns of those (and there are many) who consider that our society, and other

²⁴⁹ New Zealand Security Intelligence Service Amendment Bill — First Reading (C, Chris Finlayson)

²⁵⁰ Ibid, p 10

²⁵¹ Ibid, p 5

²⁵² Ibid

²⁵³ “Submissions, advice and report to the House on the New Zealand Security Intelligence Service Amendment Bill”, (17 May 2011). Accessed January 18 2014, www.parliament.nz/en-nz/pb/legislation/bills/isc/49DPMCISC_SUB_00DBHOH_BILL10486_1/submissions-advice-and-report-to-the-house-on-the-new

²⁵⁴ Rosslyn Noonan, “New Zealand Security intelligence Service Amendment Bill”, (Wellington: Office of the Privacy Commissioner, 31 March 2011), Accessed January 06 2014. www.hrc.co.nz/wp-content/uploads/2011/04/Submission_NZ_SIS_Amendment_-Bill_Mar_31_2011.pdf, p 3

comparable societies, are rapidly becoming ever more encompassing surveillance societies.”²⁵⁵

Following consideration by the Office of the Human Rights Commissioner, the Intelligence and Security Committee recommended a set of principles be included under which the NZSIS was required to act in accordance with performing its functions under the Act. These principles broadly outlined the agency’s requirement to act in New Zealand’s interests, and act in accordance with New Zealand law and all human rights standards recognised by New Zealand law.²⁵⁶ Section 4AAA was inserted into the Bill, stating:

“In performing its functions under this Act, the Security Intelligence Service... (a) contributes to keeping New Zealand society secure, independent, and free and democratic: (b) contributes to the participation of New Zealand in the maintenance of international security:” as part of our obligations, and “(c) acts—(i) in accordance with New Zealand law and all human rights standards

Except to the extent that they are, in relation to national security, modified by an enactment: (ii) in the discharge of its operational functions, independently and impartially: (iii) with integrity and professionalism: (iv) in a manner that facilitates effective democratic oversight.”²⁵⁷

The proposed principles provided guidance to the NZSIS when applying aspects of the legislation to its surveillance work, providing explicit recognition of those matters including human rights that should guide its work.²⁵⁸ However, these principles created no obligation or duty on any person, and in particular, “this addition to the Act does not oblige the Security Intelligence Service to be guided, in its ‘working’, by the matters referred to (including ‘human rights standards’).”²⁵⁹

²⁵⁵ Ibid, p 5

²⁵⁶ *New Zealand Security Intelligence Service Amendment Bill 2010*, (Bills Digest No 1876, December 08 2010), Accessed January 08 2014, <http://www.parliament.nz/en-nz/pb/legislation/bills/digests/49PLLawBD18261/new-zealand-security-intelligence-service-amendment-bill>

²⁵⁷ 2011 No 28, *New Zealand Security Intelligence Service Amendment Act 2011*, assented 12 July 2011, s 4AAAA

²⁵⁸ Bills Digest No 1876 *New Zealand Security Intelligence Service Amendment Bill 2010* (December 08 2010)

²⁵⁹ Bills Digest No 1876

Prior to its introduction to Parliament, the Bill was reviewed by the Ministry of Justice. The Ministry stated in a report to the Attorney-General that the proposed changes recognised the need to adequately provide for national security by enabling the use of operational techniques against sophisticated security subjects. Moreover, the changes reflected technological changes in the storage and communication of information, and were a necessary and reasonable extension of the intelligence warrant framework in an age where the use of mobile phones and cyber-identities were prevalent.²⁶⁰ The report noted that the intelligence warrant framework, as amended by the Bill, would still be subject to the safeguards set out in the Bill of Rights Act, and would attract the direct attention of formal oversight authorities. In particular, for NZSIS to exercise powers of entry, a warrant based on sworn evidence would be required, in addition to the application of an objective standard, including probable and reasonable grounds.²⁶¹ The Ministry concluded that the Bill maintained an appropriate balance between security intelligence needs and reasonable expectations of privacy, and appeared consistent with the rights and freedoms affirmed by the Bill of Rights Act.²⁶²

Government Communications Security Bureau and Related Legislation Amendment Act 2013

In April 2013, Prime Minister and Minister responsible for the GCSB John Key announced a proposal for legislative changes to the GCSB Act 2003. These proposals were in response to a report completed in March 2013 by Rebecca Kitteridge entitled *Review of Compliance at the Government Communications Security Bureau*, which sought to assess GCSB's operations and whether there were systems in place to ensure the lawfulness of those actions under relevant New Zealand and international law.²⁶³ In September 2012, GCSB Director Ian Fletcher and Department of the Prime Minister and Cabinet (DPMC) Chief Executive Andrew Kibblewhite had initiated the review after it was discovered that the GCSB had unlawfully intercepted the communications of New Zealand residents, including Mr Kim Dotcom (aka

²⁶⁰ Jeff Orr, "Consistency with the New Zealand Bill of Rights Act 1990: New Zealand Security Intelligence Services Amendment Bill". (Wellington: Ministry of Justice, 2010). Accessed January 14, 2014. www.justice.govt.nz/policy/constitutional-law-and-human-rights/human-rights/bill-of-rights/government-communications-security-bureau-and-related-legislation-amendment

²⁶¹ Ibid

²⁶² Ibid

²⁶³ Kitteridge, Rebecca. "Review of Compliance at the Government Communications Security Bureau." (March, 2013). Accessed February 12, 2014. <http://www.gcsb.govt.nz/newsroom/reports-publications/Review%20of%20Compliance.pdf> 13

Kim Schmitz).²⁶⁴ Dotcom was an Internet entrepreneur of German-Finnish origin whom, at the request of the New Zealand Police, the GCSB had monitored by intercepting his communications and monitoring his whereabouts in the weeks before a police raid on Dotcom's house. Although not a New Zealand citizen, Dotcom had been granted New Zealand permanent residency, making GCSB's surveillance illegal without the authority of an interception warrant.²⁶⁵ In late September 2012, Prime Minister Key publically apologised for the illegal spying, stating that every New Zealander was entitled to be protected by the law, and "we failed to provide that appropriate protection to them."²⁶⁶

The activity of the GCSB in relation to Dotcom resulted in significant public criticism and reignited the debate within New Zealand of the appropriate balance between privacy and security. Much of this criticism centred on the agency's unauthorised surveillance of Dotcom and his family.²⁶⁷ The case raised questions as to how such unlawful activity had been able to occur, and whether GCSB had undertaken any other unlawful surveillance in the past. That situation was the catalyst for the Review of Compliance.²⁶⁸

The Compliance Review looked at whether the GCSB's activities were undertaken within its powers and with appropriate safeguards in place. It concluded that from 1 April 2003, the GCSB had provided assistance to the NZSIS and, more rarely, the New Zealand Police, to monitor the communications of 88 New Zealanders without the authority of a warrant.²⁶⁹ This activity fell outside the legal functions of the agency as the GCSB could only monitor foreign citizens or agents of foreign powers unless acting under the legal authority of another government agency. Without this authority the GCSB's activity had been non-compliant with governing legislation. The review also considered GCSB's compliance model, including the agency's ability to assess and identify legal compliance obligations, and prevent non-compliant behaviour.²⁷⁰ The Review concluded that the non-compliant activities of the

²⁶⁴ Ibid, p 125

²⁶⁵ This assessment is based on the author's interpretation of legislation governing the GCSB

²⁶⁶ Adam Bennett and Claire Trevett, "PM says sorry to Dotcom." (*Otago Daily Times*, September 27, 2012). Accessed January 12, 2014. www.odt.co.nz/news/national/227768/pm-says-sorry-dotcom. www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=10836884

²⁶⁷ Kitteridge, p 81

²⁶⁸ Ibid

²⁶⁹ This was the date that the Government Communications Security Bureau Act 2003 was passed and the GCSB activity commenced being governed by legislation.

²⁷⁰ Kitteridge, p 6

GCSB were “symptomatic of underlying problems within GCSB, concerning GCSB’s structure, management of its information, capability and capacity.”²⁷¹

The report identified two broad problems with the legislation governing the GCSB. Firstly, while the GCSB Act provided for and authorised the GCSB’s current activities, it was not easy to determine whether any given activity fell within the scope of the prescribed functions of the GCSB or not.²⁷² Secondly, since the enactment of the GCSB Act in 2003, there had been a number of changes in the threat environment facing New Zealand, particularly in the area of cyber-security, and developments in the law relating to privacy and search and surveillance, which required the GCSB Act to be updated.²⁷³

The Review made a number of recommendations, including that the legislation governing the GCSB be reviewed “to clarify the application of the GCSB Act 2003 to the work of the GCSB.”²⁷⁴ The Review recommended amending the existing GCSB Act 2003 to address the issues that had been identified, as opposed to repealing and redrafting the Act altogether.²⁷⁵ The DPMC supported amending the existing GCSB Act (as opposed to repealing it entirely), as this would enable greater clarity of the law governing the operation and administration of the GCSB; update GCSB’s functions to meet new threats, in particular cyber-security; and enable the GCSB to assist and advise other government agencies to fulfil their lawful functions with its technical capabilities and expertise.²⁷⁶

The subsequent Government Communications Security Bureau and Related Legislation Amendment Bill attracted significant public criticism but was vigorously defended by the Government:²⁷⁷ “Despite ill-informed claims to the contrary, nothing in this legislation allows for wholesale spying on New Zealanders. It actually tightens, not widens, the existing regime,” Prime Minister Key stated. “It clarifies the GCSB’s legal framework and substantially increases oversight of the country’s intelligence agencies, which will go some way to

²⁷¹ Ibid, p 6

²⁷² Chhana, p 2

²⁷³ Ibid

²⁷⁴ Kitteridge, p 7

²⁷⁵ Chhana, p 7. See also Kitteridge Report (2013)

²⁷⁶ Ibid, pp 6-7

²⁷⁷ Significant is a relative term. The Government received 124 public submissions on the GCSB Amendment Bill 2013, while at the same time received 30,000 submissions on a proposal to amend Snapper catch quotas

rebuilding public confidence in the GCSB.”²⁷⁸ The Act clarified the three functions of the GCSB, being Information assurance and cyber security; Foreign Intelligence; and assisting other agencies.

Attorney-General Chris Finlayson explained during the second reading of the Bill:

*“This Bill is not revolutionary. It is not an aggressive expansion of State powers. Its purpose is to provide concrete rules that leave less room for uncertainty.”*²⁷⁹

The controversy over the amendments largely focused on the removal of Section 3.14 of the GCSB Act 2003, which stated:

*Interceptions not to target New Zealand citizens or permanent residents for intelligence-gathering purposes (1) In performing the Bureau’s function in section 8B, the Director, any employee of the Bureau, and any person acting on behalf of the Bureau must not authorise or do anything for the purpose of intercepting the private communications of a person who is a New Zealand citizen or a permanent resident of New Zealand, unless (and to the extent that) the person comes within the definition of foreign person or foreign organisation.*²⁸⁰

The Compliance Review identified that most of the difficulties associated with GCSB performing its functions were connected with section 3.14, specifically questions about the application of section 14 to the information assurance function of GCSB: “If, for example, a government agency requested GCSB to analyse the agency’s network in a case of a suspected malware attack, could GCSB help? If not, how could GCSB carry out this aspect of its important protective function?”²⁸¹ The Review stated that it was under this section that surveillance of Dotcom had been illegal, and the legality of the 88 other New Zealand citizens

²⁷⁸ Audrey Young, “GCSB bill passes after final reading”, (The New Zealand Herald, 21 August 2013). Accessed 12 December 2013, www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=11112152

²⁷⁹ “Government Communications Security Bureau and Related Legislation Amendment Bill: Second Reading.” (Hansard (debates), vol. 692, week 49, August 1, 2013). Accessed February 12, 2014. www.parliament.nz/en-nz/pb/debates/debates/50HansD_20130801_00000012/government-communications-security-bureau-and-related-legislation

²⁸⁰ 2013 No 57, Government Communications Security Bureau Amendment Act 2013, assented 21 August 2013, S3.14

²⁸¹ Kitteridge report (2013), p 15

and permanent residents had been in dispute.²⁸² Removing section 3.14 would allow the agency to fulfil its obligations under section 8 of the GCSB Act 2003, namely assisting the Police, the New Zealand Defence Force, and the NZSIS to perform their lawful functions.²⁸³

Overall, the amendments achieved three overarching changes to the existing GCSB Act. The information assurance and cyber-security function were given greater prominence, and confirmed the GCSB's responsibility to use its cyber-security capabilities to assist a range of public entities as well as private sector organisations such as critical national infrastructure providers and organisations of national significance. Secondly, the amendments provided transparency about the nature and scope of the agency's foreign intelligence function, expressly describing the range of activities involved or the skills required in pursuit of this function.²⁸⁴ And thirdly, the amendment provided a clear legal authority for GCSB to offer expert advice and assistance to the New Zealand Defence Force, Police, and NZSIS in performing their lawful functions. It did so while ensuring the GCSB was confined to only conducting activities that the other entities were lawfully able to undertake, while being subject to limitations and restrictions that applied to the other entities.²⁸⁵

While these amendments provided significant powers for the GCSB to assist domestic agencies, other amendments in the Bill provided greater oversight of the activities of New Zealand's intelligence agencies. The Intelligence and Security Committee Amendment Act and Inspector-General of Intelligence and Security (IGIS) Amendment Act were included in the omnibus Bill.²⁸⁶ In addition to updating the statutory framework of the GCSB through the previously discussed amendments, the ISC and IGIS Amendment Acts sought to "enhance the external oversight mechanisms that applied to the intelligence agencies by strengthening the office of the Inspector-General of Intelligence and Security and by improving the operation of Parliament's Intelligence and Security Committee."²⁸⁷ Sections 15A to 15F of the IGIS Amendment Act provided for an advisory panel and advice to the Inspector-General.²⁸⁸ The panel could also report direct to the Prime Minister. Section 15C provided that the panel

²⁸² Kitteridge report (2013), p 15

²⁸³ *GCSB Act 2003*, S2.8

²⁸⁴ *GCSB and Related Legislation Amendment Bill*, Explanatory Note, p 1

²⁸⁵ *Ibid*

²⁸⁶ *Ibid*

²⁸⁷ *Ibid*, pp 1-2

²⁸⁸ 2013 No 58, *Inspector-General of Intelligence and Security (IGIS) Amendment Act 2013*, (assented 21 August 2013), s 10 p 15A & 15F

consisted of the Inspector-General plus two others appointed by the Prime Minister, one of whom must be a lawyer.²⁸⁹ The Inspector-General was also to be notified when a warrant was issued, amounting to increased independent oversight of the intelligence agencies.

The omnibus Bill put in place a robust review of New Zealand's intelligence agencies, beginning in 2015 and reoccurring every five to seven years thereafter. This review would appraise:

"The effectiveness and appropriateness of the procedures adopted by each intelligence and security agency to ensure compliance with its governing legislation in relation to the issue and execution of warrants and authorisations; and

*The effectiveness and appropriateness of compliance systems concerning operational activity, including all supporting policies and practices of an intelligence and security agency relating to – (A) administration; (B) information management; (C) risk management; (D) legal compliance generally: to conduct unscheduled audits of the procedures and compliance systems"*²⁹⁰

This review was supported by civil liberties campaigners as it would support a wider public debate on the intelligence agencies, although it was noted that such a review would ideally have occurred before, not after, the legislation that provoked it had been enacted.²⁹¹

Telecommunications (Interception Capability and Security) Act 2013

The Telecommunications (Interception Capability and Security) Act 2013 replaced the now out-dated Telecommunications (Interception Capability) Act 2004. This Act extended the Government's powers in relation to the interception of telecommunications by New Zealand's law enforcement and intelligence and security agencies by compelling communications providers to provide lawful intercept capabilities so that the Police, NZSIS

²⁸⁹ Ibid, s 10 p 15C

²⁹⁰ Ibid, p 4 s 7(d)

²⁹¹ National Business Review, "Spy bill changes an improvement, but further change needed – InternetNZ". (23 July 2013, National Business Review). Accessed December 17 2013, www.nbr.co.nz/ accessed 17 December 2013

and GCSB could access communications once they had an interception warrant. The Act also ensured that intelligence agencies were able to identify and intercept telecommunications on that network without intercepting material that was not covered by warrant. Thirdly, the Act required network operators to inform the GCSB of any proposed decision, course of action or change that raised a “network security risk” relating to New Zealand's national security.

The Act was highly contentious and prompted significant response from privacy, human rights and Internet freedom advocates who complained of intrusive state powers and a lack of adequate oversight. The Government argued that the oversight mechanisms provided by the IGIS and ISC Acts were appropriate checks on the intelligence agencies activities. It is also notable that the intelligence agencies would not collect the information themselves, and would only gain access once the network operators had been presented with an interception warrant.

18. Finding a Balance between Privacy and Security

New Zealand’s privacy and security legislation has significantly changed in the past decade as New Zealand attempts to address the changing threats presented by globalisation and cyberspace. Similar changes have been mirrored by other states, creating a politically-charged international debate regarding the appropriate balance between privacy and security. The UN Special Rapporteur of the promotion and protection of the right to freedom of opinion and expression noted a deep concern regarding actions taken by states against individuals communicating via the Internet, frequently justified broadly as being necessary to protect national security or to combat terrorism. The report noted the introduction of laws or amendments to existing laws to increase their power to monitor Internet users’ activities and content of communication without providing sufficient guarantees against abuse:

The Special Rapporteur notes that the right to privacy can be subject to restrictions or limitations under certain exceptional circumstances. This may include State surveillance measures for the purposes of administration of criminal justice, prevention of crime or combating terrorism. However, such interference is permissible only if the criteria for permissible limitations under international human rights law are met. Hence, there must be a law that

*clearly outlines the conditions whereby individuals' right to privacy can be restricted under exceptional circumstances, and measures encroaching upon this right must be taken on the basis of a specific decision by a State authority expressly empowered by law to do so, usually the judiciary, for the purpose of protecting the rights of others, for example to secure evidence to prevent the commission of a crime, and must respect the principle of proportionality.*²⁹²

While the legislation introduced in New Zealand has certainly increased the ability of New Zealand's intelligence agencies to access a wider range of data, this does not mean that all data is open and freely available. Instead, the legislation has increased transparency through public reviews of the intelligence agencies, and requires the agencies to annually declare their activities with regards to warrants and assistance provided. The legislation also gives the intelligence agencies a set of guiding principles that acknowledge the importance of human rights and the respect for individual privacy, and puts in place strong oversight mechanisms that ensure the agencies act appropriately. In addition, the New Zealand Government has emphasised that only metadata may be collected without the basis of a warrant. Any further information, such as the content of communications, can only be collected subject to an interception warrant. In a global era of increased threat from cyber-attack, these measures allow New Zealand's intelligence agencies to identify and deter threats to New Zealand, while respecting the civil liberties and privacy of individual citizens.

Highlighting the inability of a small state such as New Zealand to conduct mass-surveillance programs, Prime Minister Key stated that "if the GCSB were to listen to every voice communication and read every text message that originated or terminated in New Zealand, it would take 130,000 people and cost NZ\$6.6 billion."²⁹³ Key made it clear that this was well outside New Zealand's capability to resource. Instead, the key focus for New Zealand would remain the collection of intelligence appropriate to the defence of New Zealand and its

²⁹² UNGA, United Nations General Assembly "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, A/HRC/17/27 ". (16 May 2011). Accessed 17 January 2014, www.2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf

²⁹³ The Standard, "Key vs Campbell: the transcript". (August 15th, 2013). Accessed January 17 2014, <http://thestandard.org.nz/key-vs-campbell-the-transcript/>, p 16 para 69

citizens, while maintaining the privacy and security of information. This was reinforced by New Zealand MP Maurice Williamson:

*“While there is a balance to be struck, there is a good deal of complementarity between the two sets of values, particularly in a strong democratic state such as New Zealand. Search powers that encroach too far on human rights values are unlikely to gain legislative or community support. Similarly, investigative powers that are too tightly controlled and that prevent law enforcement officers from doing their job effectively will bring human rights norms into disrepute.”*²⁹⁴

New Zealand has also strengthened the oversight and accountability of its intelligence services. The Intelligence and Security Committee, the Office of the Privacy Commissioner, the Inspector-General of Intelligence and Security, and the Ministry of Justice each act as a check and balance on widespread collection of data New Zealanders. If such collection were to occur, it would first be necessary to justify the collection through the application for judicial warrants. Subsequent reviews would ensure the collection was appropriate and within legal boundaries.

19. Conclusion

The purpose of this thesis has been to identify and examine the threats that an increasingly connected world presents to modern states. The rise of cyberspace and new communications technologies provides significant benefits, allowing individual citizens, private corporations and governments to interact and communicate easily and efficiently. At the same time, these advances have brought new vulnerabilities to the security of states and individuals. The scale and sophistication of cyber-attacks has risen dramatically in just the last few years and there is no single solution to address these threats. The core attributes of cyberspace that are central to the success of globalisation in the 21st century, including low cost of entry, anonymity and a global reach, also present significant challenges to traditional state security defence strategies. The diversified nature of the Internet now allows

²⁹⁴ New Zealand Law Commission, *Search and Surveillance Powers*. (Report 97, New Zealand Law Commission., June 2007) Chapter 2, paragraph 2.7

aggressors to conduct cyber-attacks across borders and attack state and non-state actors alike. As a result, the social contract between state and citizen is extended to cyberspace, and the collection of intelligence enables states to protect its citizens by deterring attacks by aggressors. We have also seen that liberal democratic states face greater challenges to addressing cyber-security challenges than authoritarian states, which are more willing to restrict or limit Internet access. The complexity and scale of cyber-threats that mean no individual state has sufficient resources to ensure complete security. To address this, states may pursue alliance building, institutionalism, and identity and norm creation strategies. A central challenge to these approaches is the lack of global government and international law governing cyberspace.

Globalisation has enlarged the security interests of New Zealand so that it can no longer rely on its isolation as the only defence against attack. As a small state, New Zealand lacks the resources to address these threats autonomously and has pursued a number of security strategies to compensate for this. Membership of security alliances and international institutions has enabled New Zealand to provide protection for its citizens beyond that which the state could provide alone. This includes strengthening intelligence sharing with the Five Eyes security alliance and developing closer bilateral ties with the US as it pivots its security interest toward Asia-Pacific. Beyond this, New Zealand has enhanced its domestic cyber capabilities to compensate for where international norms and law are insufficient. These domestic capabilities provide greater protection for New Zealand's interests, corporations and citizens by deterring potential aggressors from attacking through strong signalling of the capabilities and intentions of the state and intelligence agencies.

The legislative changes enacted by the New Zealand Government have built upon already existing laws that seek to address the technological changes that the Internet and an increasingly globalised world bring. The creation of the National Cyber Security Centre has demonstrated the New Zealand Government's willingness to address the cyber-threats by raising awareness amongst state agencies, private corporations and private citizens. Security focused legislation has been enacted that seeks to deter attacks from occurring, and provides greater capability by New Zealand's intelligence agencies to identify and prosecute perpetrators if necessary. This legislation has also removed any ambiguity regarding the lawful responsibilities of New Zealand's intelligence agencies.

As a result of these legislative changes and revelations of secret mass surveillance programmes operated by some of its security partners, New Zealand has experienced a significant debate on the power of the state to monitor cyber communications and the appropriate balance between privacy and security. While this debate is likely to continue into the future, the significant oversights that act as a check and balance over the activities of the NZSIS and GCSB provide reassurance that the New Zealand Government is mindful of the delicate steps it must take to address the rapidly evolving security environment. The 2015 review of New Zealand's security agencies will likely prove enlightening for security and civil liberties advocates alike by providing an accurate assessment of New Zealand's privacy and security balance. The challenge for New Zealand will be maintaining this balance into the future as the world becomes increasingly connected online and the deterrence of cyber threats becomes central to New Zealand's core national security imperatives.

20. Bibliography

"British-US Communication Intelligence Agreement",

www.discovery.nationalarchives.gov.uk/SearchUI/details/C11536914?uri=C11536914.

"Key reveals WMD cyber terrorism threat to NZ." *TVNZ*, April 15, 2013. Accessed January 15, 2014.

<http://www.tvnz.co.nz/national-news/key-reveals-wmd-cyber-terrorism-threat-nz-5407210>.

Addison, Adrian. "Cybercrime is World's Most Dangerous Criminal Threat". *Agence France-Presse*, September 17, 2010.

http://www.google.com/hostednews/afp/article/ALeqM5j368XIZpJo33r7xM64NgOqp1_XeQ.

Alford, Peter, and Cameron Stewart. "Jakarta puts security ties on ice - Tony Abbott expresses 'deep regret'". *The Australian*, November 21, 2013. Accessed December 12, 2013.

<http://www.theaustralian.com.au/national-affairs/policy/jakarta-puts-security-ties-on-ice-tony-abbott-expresses-deep-regret/story-fn59nm2j-1226764833945#>.

Anderton, Jim. "Ministerial Statement – Terrorist Attacks, United States". Speech to the New Zealand House of Parliament, September 12, 2001. Accessed January 20, 2014.

<http://www.vdig.net/hansard/archive.jsp?y=2001&m=09&d=12&o=3&p=11>.

Andrew, Christopher. "Intelligence, International Relations and 'Under-theorisation". *Intelligence and National Security* 19, no. 2 (2004): 170-184.

BBC, "Edward Snowden: Leaks that exposed US spy programme", *BBC*,

<http://www.bbc.co.uk/news/world-us-canada-23123964>

Bennett, Adam, and Claire Trevett. "PM says sorry to Dotcom." *Otago Daily Times*, September 27, 2012. Accessed January 12, 2014. <http://www.odt.co.nz/news/national/227768/pm-says-sorry-dotcom>.

Bimfort, Martin. "Intelligence as a Science." *Studies in Intelligence* 2, no. 2 (1958): 76.

Birchfield, Reg. "Cyber Crime: Cyber Threats and Data Privacy." *New Zealand Management*, April 2013.

Accessed February 12, 2014. <http://www.management.co.nz/Editorial.asp?eID=64698&Wcat=102>.

Blau, John. "NSA Surveillance Sparks Talk of National Internets." *IEEE Spectrum*, January 23, 2014.

Accessed January 30, 2014. <http://spectrum.ieee.org/telecom/internet/nsa-surveillance-sparks-talk-of-national-internets>.

Bobbitt, Philip. *Terror and Consent: The Wars for the 21st Century*. London: Penguin Books Ltd, 2008.

Brankin, Daria. "Could a Cyber Attack Constitute a Crime of Aggression under the Statute of the International Criminal Court?", University of Turin (2011), p 17

Browning, Christopher S. *International Security: A Very Short Introduction*. New York: Oxford University Press, 2013.

Bryan-Low, Cassell. "Vodafone, Ericsson Get Hung Up in Greece's Phone-Tap Scandal: Bugging of Nation's Leaders Points to Security Holes, Sets off Multiple Probes". *The Wall Street Journal*, June 21, 2006. Accessed January 12, 2014. <http://online.wsj.com/news/articles/SB115085571895085969>.

Burton, Joe. "Small states and cyber security: The case of New Zealand", *Political Science* 2013 65: 216 (2013), 215 - 238

Butler, Andrew. *Explanatory Note: Counter-Terrorism Bill 2002*. Wellington: Ministry of Justice, 2003. Accessed February 6, 2014. <http://www.justice.govt.nz/policy/constitutional-law-and-human-rights/human-rights/bill-of-rights/counter-terrorism-bill-2002>.

Cassidy, John. "Why Edward Snowden is a Hero." *The New Yorker*, June 10, 2013. Accessed January 12, 2014. <http://www.newyorker.com/online/blogs/johncassidy/2013/06/why-edward-snowden-is-a-hero.html>.

Castells, Manuel. *The Rise of the Network Society (The Information Age: Economy, Society and Culture: Volume 1)*. Oxford: Blackwell Publishers Inc, 1996.

Centre for Strategic and International Studies (CSIS). *The Economic Impact of Cybercrime and Cyber Espionage*. California: McAfee, July 2013.

Chhana, Rajesh. *Regulatory Impact Statement: Government Communications Security Bureau Act Review*. Wellington: Department of Prime Minister and Cabinet, 2013.

Clarke, Richard A., and Robert Knake. *Cyber War: The Next Threat to National Security and What to Do about It*. New York: HarperCollins, 2010.

Cohen, Jared, and Eric Schmidt. *The New Digital Age: Reshaping the Future of People, Nations and Business*. California: Hodder and Stoughton Limited, 2013.

Conte, Alex. *Counter-Terrorism and Human Rights in New Zealand*. Wellington: New Zealand Law Foundation, 2007.

Cornish, Paul, David Livingstone, Dave Clemente and Claire Yorke. *On Cyber Warfare*. London: Chatham House, 2010.

Cornish, Paul. *Cyber Security and Politically, Socially and Religiously Motivated Cyber Attacks*. Brussels: European Parliament, 2009.

Counter-Terrorism Bill 2003 (Supplementary Order Papers 2003 Nos. 163 and 164). Wellington: New Zealand Parliamentary Library, 2003.

Cukier, Kenneth Neil, and Viktor Mayer-Schoenberger. "The Rise of Big Data: How it's Changing the Way We Think About the World". *Foreign Affairs*, May-June 2013. <http://www.foreignaffairs.com/articles/139104/kenneth-neil-cukier-and-viktor-mayer-schoenberger/the-rise-of-big-data>.

Davies, Tim. *Open Data Barometer: 2013 Global Report*. London: Web Foundation, 2013.

Der Derian, J. "The Question of Information Technology in International Relations." *Millennium - Journal of International Studies* 32 (2003): 441-456.

Evans, Graham, and Jeffrey Newnham. *The Penguin Dictionary of International Relations*. Auckland: Penguin Group Limited, 1998.

Finklea, Kristin, and Catherine Theohary. "Cybercrime: Conceptual Issues for Congress and U.S. Law Enforcement." Washington D.C., Congressional Research Service, January 9, 2013.

Finnemore, Martha and Kathryn Sikkink, "International Norm Dynamics and Political Change", International Organisation: MIT Press, Vol. 52, No. 4, Autumn, 1998: pp. 887-917

Fletcher, Ian. Director GCSB. Richard Gordon, Pipitea House on Pipitea/05 February 2014, notes available upon request

Foreign Affairs, Defence and Trade Committee. *Counter-Terrorism Bill: Government Bill. As reported from the Foreign Affairs, Defence and Trade Committee*. August 8, 2003. Accessed February 12, 2014. <http://www.parliament.nz/resource/0000018928>.

Foreign Affairs, Defence and Trade Committee. *Interim Report on the Terrorism {(Bombings and Financing)} [Suppression] Bill*. 8 November 2001. Accessed January 12, 2014. www.brookers.co.nz/bills/enacted_bills/B011212.PDF.

Franceschi-Bicchierai, Lorenzo, "Edward Snowden's Motivation: Internet Freedom", *Mashable.com*, 11 June 2013, <http://mashable.com/2013/06/10/edward-snowden-Internet-freedom>.

Garrett, Banning. *Big Data Is Changing Your World... More than You Know*. Washington DC: Atlantic Council, 2013.

Gill, Peter, and Mark Phythian. *Intelligence in an Insecure World*. Cambridge: Polity Press, 2006.

Glanz, James, and John Markoff. "Egypt Leaders Found 'Off' Switch for Internet." *The New York Times*, February 15, 2011. Accessed January 2, 2014. http://www.nytimes.com/2011/02/16/technology/16internet.html?pagewanted=all&_r=0.

Glaser, Charles. *Rational Theory of International Politics: The Logic of Competition and Cooperation*. Princeton: Princeton University Press, 2010.

Goldsmith, Jack, and Wu Tim. *Who Controls the Internet: Illusions of a Borderless World*. New York: Oxford University Press, 2006.

Government Communications and Security Bureau (GCSB). "Annual Report for the Year Ended 30 June 2013." September 30, 2013. Accessed February 12, 2014. <http://www.gcsb.govt.nz/newsroom/annual-reports/Annual%20Report%202013.pdf>.

Government Communications Security Bureau (GCSB). Accessed December 20, 2013. www.gcsb.govt.nz.

Greenwald, Glenn, Ewen MacAskill, and Laura Poitras. "Edward Snowden: The Whistleblower Behind the NSA Surveillance Revelations." *The Guardian*, June 10, 2013. Accessed January 12, 2014. <http://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance>.

Hager, Nicky. "FBI role in Big Brother's sharper eyes, ears". January 3, 2010. Accessed January 19, 2014. www.nickyhager.info/fbi-role-in-big-brothers-sharper-eyes-ears/.

Hager, Nicky. "Google case highlights risks in NZ law change". January 24, 2010. Accessed January 19, 2014. www.nickyhager.info/google-case-highlights-risks-in-nz-law-change/.

Hager, Nicky. *Secret Power: New Zealand's Role in the International Spy Network*. Nelson: Craig Potton

Publishing, 1996.

Haley, Christopher. "A Theory of Cyber Deterrence". *Georgetown Journal of International Affairs* (2013). Accessed January 21, 2014. http://journal.georgetown.edu/2013/02/06/a-theory-of-cyber-deterrence-christopher-haley/#_edn6

Hathaway, Oona, Rebecca Crootof, Philip Levitz, Haley Nix, Aileen Nowlan, William Perdue, and Julia Spiegel. "The Law of Cyber Attack." *California Law Review* 100 (2012): 817-885.

Herz, John J. *Political Realism and Political Idealism: A Study in Theories and Realities*. Chicago: University of Chicago Press, 1951.

Herzog, Stephen. "Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses." *Journal of Strategic Security* 4, no. 2 (2011): 49-60.
<http://www.scholarcommons.usf.edu/jss/vol4/iss2/4>.

Hildreth, Steven A. "Cyberwarfare." Congressional Research Service, June 19, 2001.

Hobbes, Thomas, and J. C. A. Gaskin. *Leviathan*. Oxford: Oxford University Press, 1998.

Hon Stephen Joyce. "New Zealand's Cyber Security Strategy: June 2011". Wellington: Ministry for Communications and Information Technology, 7 June 2011

Human Rights Commission. "Submission on the New Zealand Security Intelligence Service Amendment Bill". 31 March 2011.

Human Rights Review 2012, Article 3: "Freedom from torture and inhumane and degrading treatment or punishment", Equality and Human Rights Commission, 2012
<http://www.equalityhumanrights.com/human-rights/our-human-rights-work/human-rights-review/the-articles/>,

IBM Corporation. *IBM X-Force® 2010 Trend and Risk Report*, New York: IBM Corporation, 2011.

Internet Security Alliance. *The Cyber Security Social Contract: Policy Recommendations for the Obama Administration and 111th Congress*. Arlington: ISAlliance, 2008.

Jervis, Robert. "Realism, Neorealism, and Cooperation: Understanding the Debate." *International Security* 24, no. 1 (1999): 42-63.

Kamenev, Marina. "First, China. Next: the Great Firewall of... Australia?" *TIME Magazine*, June 16, 2010. Accessed January 2, 2014. <http://content.time.com/time/world/article/0,8599,1995615,00.html>.

Keall, Chris. "'NZ Govt Naïve about Huawei' – security insider Selwyn Pellett details Beijing experience with Endace." *National Business Review*, April 5, 2012. Accessed January 12, 2014.
<http://www.nbr.co.nz/article/govt-naive-about-huawei-%E2%80%93-security-insider-details-beijing-experience-ck-115894>.

Keohane, Robert & Lisa Martin. *The Promise of Institutional Theory*, *International Security*, Vol. 20, No. 1. pp. 39-51, 1995.

Kerr, Orin. "Internet Surveillance Law after the USA Patriot Act: The Big Brother that Isn't." *Northwestern University Law Review* 97, no. 2 (2003): 607 – 613.

Kitteridge, Rebecca. "Review of Compliance at the Government Communications Security Bureau." March, 2013. Accessed February 12, 2014. <http://www.gcsb.govt.nz/newsroom/reports-publications/Review%20of%20Compliance.pdf>

Kuehl, Daniel. *From Cyberspace to Cyberpower: Defining the Problem*. Washington DC: National Defence University Press, 2009.

Larson, Leslie. "NSA's program of gathering data likely unconstitutional, federal judge rules." *New York Daily News*, December 16, 2013. Accessed December 18, 2013. <http://www.nydailynews.com/news/politics/nsa-program-gathering-data-unconstitutional-federal-judge-article-1.1549435#ixzz2tzjO6NWc>.

Lefebvre, Stéphane. "The Difficulties and Dilemmas of International Intelligence Cooperation." *International Journal of Intelligence and Counter Intelligence* 16, no. 4 (2003): 527-542.

Legg, Shane, and Marcus Hutter. "A Collection of Definitions of Intelligence." In *Advances in Artificial General Intelligence: Concepts, Architectures and Algorithms – Proceedings of the AGI Workshop 2006*, edited by Ben Goertzel and Pei Wang, 17-24. Amsterdam: IOS Press, 2007.

Lewis, James. *A Note on the Laws of War in Cyberspace*. Washington DC: Centre for Strategic and International Studies, 2010.

Lewis, James. Quoted in John Schwartz, "When Computers Attack." *The New York Times*, June 24 2007. Accessed January 14, 2014. <http://www.nytimes.com/2007/06/24/weekinreview/24schwartz.html?pagewanted=all>.

Libicki, Martin. "Pulling Punches in Cyberspace." In *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy*, edited by the National Research Council of the National Academies, 123-148. Washington DC: The National Academies Press, 2010.

Libicki, Martin. *Brandishing Cyberattack Capabilities*. Santa Monica: RAND Corporation, 2013.

Libicki, Martin. *Cyber Deterrence and Cyberwar*. Santa Monica: RAND Corporation, 2009.

Lin, Herbert S. "Offensive Cyber Operations and the Use of Force." *Journal of National Security Law & Policy* 4 (2010): 63-86.

Lind, Michael. "They Will Change Us." *Prospect Magazine*, July 28, 2005. Accessed December 12, 2013. <http://www.prospectmagazine.co.uk/magazine/theywillchangeus/#.Uw2vDvmSzCs>.

Locke, Keith. "Counter-Terrorism Bill is Counter-more than Terrorism." Parliamentary speech, October 14, 2003. Accessed February 9, 2014. <https://www.greens.org.nz/speeches/counter-terrorism-bill-counter-more-terrorism>.

Lord Lester of Herne Hill and David Pannick. *Human Rights Law and Practice*. London: Butterworth, 2004.

MacAskill, Ewen, and Lenore Taylor. "NSA: Australia and US Used Climate Change Conference to Spy on Indonesia." *The Guardian*, November 2, 2013. Accessed January 14, 2013. <http://www.theguardian.com/world/2013/nov/02/nsa-australia-bali-conference-spy-indonesia>.

MacAskill, Ewen, Julian Borger, Nick Hopkins, Nick Davies, and James Ball. "GCHQ taps fibre-optic cables for secret access to world's communications" *theguardian.com: The Guardian*, 21 June 2013, <http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa>.

MacAskill, Ewen. "Edward Snowden, NSA files source: 'If they want to get you, in time they will'" *The Guardian*, June 10, 2013. Accessed January 12, 2014. <http://www.theguardian.com/world/2013/jun/09/nsa-whistleblower-edward-snowden-why>.

Maranga, Kennedy. "The Changing Role of State Responsibility: Comparative Approach." *Journal of Global Affairs and Public Policy* 1, no. 1 (2011): 1-24.

McBride, Tim. "Heightened State Surveillance in New Zealand, Post-"9/11"-Privacy under Threat", Accessed 18 December 2013, www.timmcbridelaw.co.nz/images/pdfs/TimMcBride_Surveillance.pdf, p 4

McCarthy Tom. "This overreach is unacceptable': the case against NSA bulk collection." *The Guardian*, 23 January 2014. <http://www.theguardian.com/world/2014/jan/23/nsa-bulk-collection-chorus-surveillance-under-patriot-act>

Mearsheimer, John J. "The False Promise of International Institutions." *International Security* 19, no. 3 (1994-1995): 5-49.

Miller, Charles. "Kim Jong-Il and Me: How to Build a Cyber Army to Attack the US". Presented at DEF CON 2010 Hacking Conference, Las Vegas, Nevada, July 30 - August 1, 2010. Accessed January 19, 2014. <https://www.defcon.org/images/defcon-18/dc-18-presentations/Miller/DEFCON-18-Miller-Cyberwar.pdf>.

Moore, Charles. "Edward Snowden is a Traitor, Just as Surely as George Blake Was". *The Telegraph*, July 5, 2013. <http://www.telegraph.co.uk/technology/internet-security/10162351/Edward-Snowden-is-a-traitor-just-as-surely-as-George-Blake-was.html>.

Morgan, Patrick, *Deterrence Now*, Cambridge: Cambridge University Press, 17 April 2003.

Morgan, Patrick, "Applicability of Traditional Deterrence Concepts and Theory to the Cyber Realm," Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy, (Washington DC, 2010). Accessed 17 January 2013, http://www.nap.edu/openbook.php?record_id=12997&page=55

Myerson, Roger B. *Game Theory: Analysis of Conflict*. Cambridge: Harvard University Press, 1991.

National Cyber Security Centre, "2012 Incident Summary", Wellington: NCSC, 2012, http://ncsc.govt.nz/sites/default/files/articles/NCSC-%202012%20Incident%20Report_0.pdf,

National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/HSPD-23). Washington DC: White House, 2008.

New Zealand Intelligence Community. "Protecting and Advancing our National Security". Accessed January 14, 2014. www.nzic.govt.nz/about-us/securing-new-zealands-future/.

New Zealand Law Commission. *Computer Misuse*. Wellington: Law Commission, 1999.

New Zealand Law Commission. *Invasion of Privacy: Penalties and Remedies. Review of the Law of Privacy: Stage 3*. Wellington: Law Commission, 2010.

New Zealand Law Commission. *Privacy: Concepts and Issues. Review of the Law of Privacy: Stage 1*. Wellington: Law Commission, 2008.

New Zealand Law Commission. *Review of the Privacy Act 1993: Review of the Law of Privacy, Stage 4*. Wellington: Law Commission, 2011.

New Zealand Law Commission, *Search and Surveillance Powers*. Report 97, New Zealand Law Commission, June 2007.

New Zealand Ministry of Defence. *Defence White Paper 2010*. Wellington: Ministry of Defence, 2010.

New Zealand Police. *Electronic Crime Strategy to 2010: Policing with Confidence*. Wellington: New Zealand Police, 2007.

New Zealand Security Intelligence Service (NZSIS). Accessed December 20, 2013. www.security.govt.nz.

New Zealand Security Intelligence Service Amendment Bill 259-2. Wellington: Parliamentary Counsel Office, 2011.

New Zealand Security Intelligence Service. *Regulatory Impact Statement: Modernising NZSIS Legislation – High Priority Amendments*. August 11, 2010. Accessed January 14, 2014. <http://www.treasury.govt.nz/publications/informationreleases/ris/pdfs/ris-nzsis-nzsis-dec10.pdf>.

New Zealand Trade and Enterprise. *Opening Doors to China: New Zealand's 2015 Vision*. Wellington: 2012.

New Zealand. "Counter-Terrorism Bill: First Reading." *Hansard (debates)*, vol. 607, week 20 (April 1, 2003). Accessed January 12, 2014. http://www.parliament.nz/en-nz/pb/debates/debates/47HansD_20030402_00000001/counter-terrorism-bill-%E2%80%94-first-reading.

New Zealand. "Counter-Terrorism Bill: Second Reading." *Hansard (debates)*, vol. 612, week 39 (October 14, 2003). http://www.parliament.nz/en-nz/pb/debates/debates/47HansD_20031014_00001157/counter-terrorism-bill-%E2%80%94-second-reading.

New Zealand. "Crimes Amendment Bill (No. 6): Consideration of Report of Law and Order Committee." *Hansard (debates)*, vol. 609, week 26 (June 12, 2003). Accessed February 6, 2014. http://www.parliament.nz/en-nz/pb/debates/debates/47HansD_20030612_00001129/crimes-amendment-bill-no-6-%E2%80%94-consideration-of-report.

New Zealand. "Government Communications Security Bureau and Related Legislation Amendment Bill: Second Reading." *Hansard (debates)*, vol. 692, week 49 (August 1, 2013). Accessed February 12, 2014. http://www.parliament.nz/en-nz/pb/debates/debates/50HansD_20130801_00000012/government-communications-security-bureau-and-related-legislation.

New Zealand: "Review of the Terrorism Suppression Act 2002", Wellington: Foreign Affairs, Defence and Trade Committee, November 2005, www.parliament.nz/resource/0000002749

New Zealand. *"Telecommunications (Interception Capability and Security) Bill: First Reading."* Hansard (debates), vol. 689, week 41 (May 8, 2013). Accessed February 12, 2014. http://www.parliament.nz/en-nz/pb/debates/debates/50HansD_20130508_00000028/telecommunications-interception-capability-and-security.

New Zealand. *"Telecommunications (Interception Capability) Bill: First Reading."* Hansard (debates), vol. 606, week 15 (February 18, 2003). Accessed February 12, 2014. http://www.parliament.nz/en-nz/pb/debates/debates/47HansD_20030218_00001143/telecommunications-interception-capability-bill-%E2%80%94-first.

New Zealand. *"Terrorism (Bombings and Financing) Bill: First Reading."* May 3, 2013. Accessed February 12, 2014. www.vdig.net/hansard/archive.jsp?y=2001&m=05&d=03&o=40&p=44.

New Zealand. *"New Zealand Security Intelligence Service Amendment Bill — First Reading."* December 9 2010. Accessed February 12 2014, www.parliament.nz/en-nz/pb/debates/debates/49HansD_20101209_00001287/new-zealand-security-intelligence-service-amendment-bill

New Zealand, New Zealand Security Intelligence Service Amendment Bill 2010, Bills Digest No 1876, December 08 2010, <http://www.parliament.nz/en-nz/pb/legislation/bills/digests/49PLLawBD18261/new-zealand-security-intelligence-service-amendment-bill>

New Zealand. Wellington. 1961 No 43, Crimes Act 1961, assented 1 November 1961.

New Zealand. Wellington, 2003 No 9, Government Communications Security Bureau Act 2003, assented 01 April 2003.

New Zealand. Wellington, 2013 No 57, Government Communications Security Bureau Amendment Act 2013, assented 21 August 2013.

New Zealand. Wellington, 2013 No 58, Inspector-General of Intelligence and Security Act 2013, assented 21 August 2013.

New Zealand. Wellington, 2013 No 59, Intelligence and Security Committee Act 2013, assented 21 August 2013.

New Zealand. Wellington , 1996 No 46, Intelligence and Security Committee Act 1996, assented 1 July 1996

New Zealand. Wellington. 2002 No 34, Terrorism Suppression Act 2002, assented 17 October 2002.

New Zealand. Wellington. 2003 No 27-2, Counter-Terrorism Bill 2003, not assented.

New Zealand. Wellington. 2003 No 39, Crimes Amendment Act 2003, assented 07 July 2003.

New Zealand. Wellington. 2004 No 19, Telecommunications (Interception Capability) Act 2004, assented to 05 April 2004.

New Zealand. Wellington. 2011 No 28, New Zealand Security Intelligence Service Amendment Act 2011, assented 12 July 2011.

New Zealand. Wellington. 2013 No 108-2, Telecommunications (Interception Capability and Security)

Act 2013, assented to 11 November 2013.

New Zealand's National Security System. Wellington: Department of the Prime Minister and Cabinet, 2011.

Noonan, Rosslyn. "New Zealand Security intelligence Service Amendment Bill", Wellington: Office of the Privacy Commissioner, 31 March 2011, www.hrc.co.nz/wp-content/uploads/2011/04/Submission_NZ_SIS_Amendment_-Bill_Mar_31_2011.pdf

Nye, Jr., Joseph S. *Cyber Power*. Cambridge: Belfer Center for Science and International Affairs, Harvard Kennedy School, 2010.

O'Neill, Rose Regina. "E-Government: Transformation of Public Governance in New Zealand?" PhD diss., Victoria University of Wellington, 2009.

Odom, William E. "Intelligence Analysis." *Intelligence and National Security* 23, no. 3 (2008): 316-332.

Office of the White House Press Secretary. "Executive Order 13587 Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information." *White House Press Release*. October 7, 2011. Accessed January 12, 2014. <http://www.whitehouse.gov/the-press-office/2011/10/07/executive-order-structural-reforms-improve-security-classified-networks->

Office of the White House Press Secretary. "Statement by the President." *White House Press Release*. June 7, 2013. Accessed December 10, 2013. <http://www.whitehouse.gov/the-press-office/2013/06/07/statement-president>.

Office of the White House Press Secretary. "Cyber Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure", Washington D.C., The White House Press, 2009.

Oltermann, Philip. "Angela Merkel Warns US over Surveillance in First Speech of Third Term." *The Guardian*, January 29, 2014. Accessed January 30, 2014.

<http://www.theguardian.com/world/2014/jan/29/angela-merkel-us-surveillance-speech-germany-chancellor>.

Orr, Jeff. *Consistency with the New Zealand Bill of Rights Act 1990: New Zealand Security Intelligence Services Amendment Bill*. Wellington: Ministry of Justice, 2010. Accessed January 14, 2014. <http://www.justice.govt.nz/policy/constitutional-law-and-human-rights/human-rights/bill-of-rights/government-communications-security-bureau-and-related-legislation-amendment>.

Owens, William A., Kenneth W. Dam, and Herbert S. Lin. *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*. Washington DC: The National Academies Press, 2009.

Oxford English Dictionary (third edition). New York: Oxford University Press, 1997.

Palmer, Darren, and Ian J Warren. "Global Policing and the Case of Kim Dotcom." *Crime and Justice Journal* 2, no. 3 (2013): 105 – 119.

Poitras, Laura, and Glenn Greenwald. "NSA Whistleblower Edward Snowden: 'I Don't Want to Live in a Society That Does These Sort of Things'" *The Guardian*, June 9, 2013. Accessed December 10, 2013.

<http://www.theguardian.com/world/video/2013/jun/09/nsa-whistleblower-edward-snowden-interview-video>.

PriceWaterhouseCoopers, "The 2011 Global Economic Crime Survey results for New Zealand Fraud, fraudsters and cybercrime". (PWC New Zealand, November 2011). Accessed 12 January 2014, www.pwc.co.nz/KenticoFiles/b2/b2ba49bb-785c-493c-aeef-a39a52803dc5.pdf

Reardon, Robert, and Nazli Choucri. *The Role of Cyberspace in International Relations: A View of the Literature*. San Diego: MIT, 2012.

Rousseau, Jean Jacques. *Social Contract & Discourses*. (New York: E. P. Dutton & Co., 1913). Bartleby.com, 2010. www.bartleby.com/168/

Rueter, Nicholas C. "The Cybersecurity Dilemma." Master's thesis, Duke University, 2011.

Schmid, Alex P. *The Routledge Handbook of Terrorism Research*. New York: Routledge, 2011.

Schmitt, Eric, and Michael S. Schmidt. "The New York Times, Qaeda Plot Leak Has Undermined U.S. Intelligence." *The New York Times*, September 29, 2013. Accessed December 21, 2013. http://www.nytimes.com/2013/09/30/us/qaeda-plot-leak-has-undermined-us-intelligence.html?pagewanted=all&_r=0.

Schmitt, Michael N. "Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework." *The Colombia Journal of Transnational Law* 37 (1999): 885-937.

Schmitt, Michael N. "Cyberspace and International Law: The Penumbral Mist of Uncertainty." *Harvard Law Review* 126 (2013): 176-180.

Schneier, Bruce. *Beyond Fear: Thinking Sensibly About Security in an Uncertain World*. New York: Copernicus Books, 2003.

Sheldon, John B. *Achieving Mutual Comprehension: Why Cyberpower Matters to Both Developed and Developing Countries*. George C. Marshall Institute, 2011.

Shroff, Marie. *Report by the Privacy Commissioner to the Minister of Justice in relation to the Telecommunications Bill*. June 26, 2001. Accessed February 7, 2014. <http://www.privacy.org.nz/news-and-publications/reports-to-parliament-and-government/telecommunications-bill-report/>.

Shroff, Marie. "Submission by the Privacy Commissioner to the Intelligence and Security Committee, Wellington: Office of the Privacy Commissioner, 17 June 2013, <http://www.privacy.org.nz/assets/Files/Reports-to-ParlGovt/2013-06-17-Select-Committee-submission-Government-Communications-Security-Bureau-and-Related-Legislation-Amendment-Act-A322600.pdf>

Shroff, Marie. "Constitutional Necessity or Constant Nuisance?" The Privacy Commissioner and the Role of ICEs." New Zealand Centre for Public Law: Public Office Holders' Lecture Series, January 28, 2014. Accessed January 30, 2014. <http://www.privacy.org.nz/assets/Files/Speeches-presentations/Public-Office-Holders-Speech-3-by-Marie-Shroff-Privacy-Commissioner-28-01-14.pdf>.

Shroff, Marie. *Government Communications Security Bureau and Related Legislation Amendment Bill: Submission by the Privacy Commissioner to the Intelligence and Security Committee*. June 17, 2013. Accessed January 17, 2014. <http://www.privacy.org.nz/assets/Files/Reports-to-ParlGovt/2013-06-17->

Select-Committee-submission-Government-Communications-Security-Bureau-and-Related-Legislation-Amendment-Act-A322600.pdf.

Sinks, Michael A. *'Cyber Warfare and International Law'*. Research Report Air Command and Staff College Air University 2008),

Slane, Bruce. *Crimes against personal privacy and crimes involving computers: Intercepting private communications and accessing computer systems without authorization*, (Wellington: Office of the Privacy Commissioner, 13 December 2000, www.privacy.org.nz/assets/Files/Reports-to-ParlGovt/Report-by-Privacy-Commissioner-on-Supplementary-Order-Paper-No.-85-to-the-Crimes-Amendment-Bill-No.6-2000.pdf)

Slane, Bruce. *Report by the Privacy Commissioner to the Minister of Justice in relation to the Counter-Terrorism Bill*. February 7, 2003. Accessed February 7, 2014. <http://www.privacy.org.nz/news-and-publications/reports-to-parliament-and-government/counter-terrorism-bill/>.

Smith, John E. *New Zealand's Anti-Terrorism Campaign: Balancing Civil Liberties, National Security, And International Responsibilities*, Wellington: Fullbright, December 2003.

Snyder, Glenn Herald. *Deterrence and Defence: Towards a Theory of National Security*. Princeton: Princeton University Press, 1961.

Solce, Natasha. 'The Battlefield of Cyberspace: The Inevitable New Military Branch – The Cyber Force' (2008) 18 Alb L J Sci & Tech.

State Services Commission. "E-government - A Vision for New Zealanders". Last modified April 9, 2003. Accessed January 14, 2014. <http://www.ssc.govt.nz/egovt-vision-for-nzers>.

Blank, Stephen. 'Web War I: Is Europe's First Information War a New Kind of War?', 2008, 27:3 Comp Strat 227.

Stoll, Clifford. "Stalking the Wily Hacker." *Communications of the ACM* 31, no. 5 (1988): 484-497.

Taillon, J. Paul D. *Hijacking and Hostages: Government Responses to Terrorism*. Westport: Praeger, 2002.

The European Commission on Trade. "Countries and regions: United States." Accessed January 20, 2013. <http://ec.europa.eu/trade/policy/countries-and-regions/countries/united-states/>.

The National Commission on Terrorist Attacks upon the United States. "The 9/11 Commission Report." July 22, 2004. Accessed December 10, 2013. <http://www.9-11commission.gov/report/911Report.pdf>.

The Office of Public Affairs. *A Consumer's Guide to Intelligence*. Washington DC: Central Intelligence Agency, 1999.

The Standard, "Key vs Campbell: the transcript". (August 15th, 2013). <http://thestandard.org.nz/key-vs-campbell-the-transcript/>

The Treasury. "Vote Police: The Estimates of Appropriations 2009/10." May 28, 2009. Accessed February 8, 2014. www.treasury.govt.nz/budget/2009/estimates/est09police.pdf.

The Treasury. "Vote Police: The Supplementary Estimates of Appropriations and Supporting

Information 2007/08." May 22, 2008. Accessed February 8, 2014.

<http://www.treasury.govt.nz/budget/2008/suppestimates/suppest08police.pdf>.

Theohary, Catherine A. "Information Operations, Cyberwarfare, and Cybersecurity", CRS Report for Congress, Washington D.C., Congressional Research Service, 17 March 2009.

United Nations General Assembly. "Universal Declaration of Human Rights." 10 December 1948.

Accessed February 15, 2014. <http://www.refworld.org/docid/3ae6b3712c.html>.

United Nations General Assembly. *International Covenant on Civil and Political Rights*. New York: United Nations Press, 1996.

United Nations General Assembly "Report of the Special Rapporteur on the promotion and protection of the right to freedom of Opinion and expression, Frank La Rue", 16 May 2011, A/HRC/17/27, http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf

United Nations Security Council. "Resolution 1373 (2001): Threats to international peace and security caused by terrorist acts]." *United Nations Security Council Resolution*. September 28, 2001. Accessed February 22, 2014. <http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N01/557/43/PDF/N0155743.pdf?OpenElement>.

United Nations Security Council. "Resolution 1566 (2004): Threats to international peace and security caused by terrorist acts." *United Nation Security Council Resolution*. October 8, 2004. Accessed February 22, 2014. <http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N04/542/82/PDF/N0454282.pdf?OpenElement>.

United Nations Security Council. "Security Council Unanimously Adopts Wide-Ranging Anti-Terrorism Resolution; Calls for Suppressing Financing, Improving International Cooperation." *Press Release*. September 28, 2001. Accessed February 22, 2014. <http://www.un.org/News/Press/docs/2001/sc7158.doc.htm>.

UNODC. *The Use of the Internet for Terrorist Purposes*. New York: United Nations, 2012.

US Commission on National Security in the 21st Century. "New World Coming: American Security in the 21st Century (Phase I: July 1998 – August 1999)." <http://www.fas.org/man/docs/nwc/nwc.htm>.

Van Cleve, Michelle. "Myth, Paradox & the Obligations of Leadership: Edward Snowden, Bradley Manning and the Next Leak." *Centre for Security Policy: Occasional Paper Series*, 2013.

Walton, Greg. *China's Golden Shield: Corporations and the Development of Surveillance Technology in the People's Republic of China*. Quebec: International Centre for Human Rights and Democratic Development, 2001.

Waltz, Kenneth. *Theory of International Relations*. New York: Random House, 1979.

Weber, Rolf H., and Romana Weber. "Social Contract for the Internet Community? Historical and Philosophical Theories as Basis for the Inclusion of Civil Society in Internet Governance?" *Scripted* 6, no. 1 (2009). <http://www.law.ed.ac.uk/ahrc/script-ed/vol6-1/weber.asp>.

White House. *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*. May 2011. Accessed December 10, 2013. http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

Wilentz, Sean. "Would You Feel Differently About Snowden, Greenwald, and Assange If You Knew What They Really Thought?" *The New Republic*, 19 January 2014, www.newrepublic.com/article/116253/edward-snowden-glenn-greenwald-julian-assange-what-they-believe

World Economic Forum. *Insight Report: Global Risks 2014 (Ninth Edition)*. Geneva: World Economic Forum, 2014.

Xiangyang, Chen. "Strategic Impacts of the 'Snowden Incident' on International Relations". *China-US Focus*, September 9, 2013. <http://www.chinausfocus.com/peace-security/strategic-impacts-of-the-snowden-incident-on-international-relations/>.

Young, Audrey. "GCSB bill passes after final reading", *The New Zealand Herald*, 21 August 2013. www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=11112152