Cyber Crime and National Security: A New Zealand Perspective

Original article

Cyber Crime and National Security: A New Zealand Perspective

Sophie Victoria Ann Richardson* and Nicholas Gilmour

Abstract: The link between cyber crime and national security has become increasingly prevalent, as technology has advanced so too has the criminal capacity to cause harm and annoyance to individuals and a nation's critical infrastructure. This article will discuss two key points as they relate to New Zealand—(1) the effect of cyber crime on national security, and (2) the challenges relating to the reporting and criminal prosecution of cyber crime related offences. It will draw upon two recent events in New Zealand as examples of the threat posed by cyber criminals, namely the downing of a national telecoms service provider and an attack on the New Zealand Parliamentary website by the "hacktivist" group Anonymous. In doing so, the article will measure the value in inter-departmental governmental cooperation in the New Zealand context, at both national and international levels as the foundation to combating cyber crime.

Keywords: Cyber crime – National security – Criminal prosecution – New Zealand

*Sophie Richardson is a Masters (International Security) graduate of Massey University in Wellington, New Zealand.

Email: sophie.victoria.ann@gmail.com

Nicholas Gilmour is the New Zealand Police Teaching Fellow at Massey University in Wellington, New Zealand.

Email: n.j.gilmour@massey.ac.nz

The European Review of Organised Crime 2(2), 2015, 51-70

ISSN: 2312-1653

Introduction

Cyber crime has become a major problem for the 21st century, in relation to both prevention and detection of the growing number of associated activities. In fact, cybercrime is the fastest-growing area of crime[1]. More countries around the world are becoming increasingly dependent on digital networks and the opportunities for committing cybercrime are increasing, as “the computer” increasingly becomes a central component of commerce, entertainment, and government. This now means the opportunities for committing cybercrime are growing exponentially as more and more people utilise hand held devices capable of exploitation and the accessing of personal and professional data. Crimes such as committing fraud, hacking, trafficking in child pornography and intellectual property, stealing identities, or violating privacy are becoming everyday activities for those involved in committing cybercrime. Cybercrime has not created new crimes, simply provided an alternative method through which to commit crimes such as theft, extortion, illegal protest, and terrorism.

In a similar way, national security has seen its profile (and focus) increase due to the parallel approach to which attacks can take place. No longer are physical attacks the only approach to undermining or overcoming a nation’s security. Todays’ modern interconnected digital networks provide an almost parallel approach that is, in certain circumstances less costly, more discreet and more damaging than the once sole approach to physical attack.

Seemingly, the link between cyber crime and national security has become increasingly prevalent, as technology has advanced the criminal capacity to cause harm and annoyance to individuals and a nation’s critical infrastructure by undermining its vital instrumentalities. What this has therefore created is a new approach to the emerging ways in which old problems like protecting national security can be addressed, utilising in some instances, changes in a nation’s law. New Zealand’s first legislation related to cyber crime was introduced only relatively recently in 2003.

As decision-makers continue to tackle the myriad of security challenges posed by today’s interconnected digital world—which is inherently international, a change in practices has co-developed across law enforcement and the intelligence and security agencies. This coordinated approach to confront the merger between cyber crime and national security threat has led to the adoption of national strategies, such as New Zealand’s Cyber Security Strategy (2011) and the introduction of new legislation. In New Zealand, the primary legislation supporting preventative action is the Telecommunications (Interception Capability and Security) Act 2013, the purpose of which is to ensure that:

1. Surveillance agencies are able to effectively carry out the lawful interception of telecommunications under an interception warrant or any other lawful interception authority;
2. Surveillance agencies, in obtaining assistance for the interception of telecommunications, do not create barriers to the introduction of new or innovative telecommunications technologies;

3. Network operators and service providers have the freedom to choose system design features and specifications that are appropriate for their own purposes.

Seemingly, the adoption of these practices has become ever more apparent and in New Zealand as elsewhere, the problems associated with cybercrime and the aligned attacks on national security are increasingly creating even greater challenges while balancing the demands of personal privacy and national security.

This article will therefore discuss two key issues linked to cybercrime and national security aligned to New Zealand. Firstly, the effect of cyber crime on national security and secondly, the challenges relating to criminal prosecution of cyber crime offences. Following this, the various aspects of cyber crime and the varying opinions on what constitutes it will be discussed. This is deemed necessary to set the scene, before the article draws upon two recent events in New Zealand as examples of the threat posed by cyber criminals—namely the downing of a national telecoms service provider (Downes, 2014) and the 2011 attack on the parliamentary website by the “hacktivist” group Anonymous (The Nelson Mail, 2011). Finally, the article will measure the value in inter-departmental governmental cooperation in the New Zealand context, at both national and international levels as the foundation to combating cyber crime.

Cyber Crime and New Zealand

The concept of national security has altered significantly in recent years (Grabosky, 2014). Gone are the days when a country’s main security threats were territorial in nature and purely military in solution. No longer does a country require a physical or military invasion to take place for there to be a threat to domestic security issues such as public health, national economy, or social cohesion (Grabosky, 2014). Distance and isolation that once afforded countries like New Zealand the relatively low possibility of attack are now all but irrelevant (Burton, 2013b).

One particular type of crime that exemplifies this new attack capability better than any other is that of cyber crime. Generally defined as a crime where “computers and the Internet play a central role in the crime, and not an incidental one” (Birchfield, 2013) cyber crime typifies globalization through scale, speed, and cognition (Burke, 2009). Cyber activities are increasing with significant velocity, allowing connection speeds to be almost instantaneous. Sophistication has reached levels never witnessed before representing a serious threat to society. The perception of how long things take to happen has reduced significantly owing to the speed in which cyber technology is advancing. Criminal gangs are also responding to the pressure placed upon such activities by law enforcement by reorganising their operations and attracting a new generation of coders and cyber experts. The concept that the world is a smaller place has influenced how countries now view security. In a globalised and cyber dependant world, countries and individuals can be attacked at anytime, from anywhere, in a whole manner of different ways at an incredible speed. These factors and the

relatively low operating costs of cyber crime exemplify why it is likely to pose a direct threat to national security.

Government, infrastructure, intellectual property, and personal information are all potentially threatened. These types of threats are of national security significance due to the potential for significant disruption or harm to the functioning of New Zealand society. This is of particular concern when one considers that these threats are not only posed by other states who have significant resources at their disposal but by rogue individuals who need only the know-how and access to a computer to be considered a potential threat.

The description of cybercrime in a New Zealand context has primarily been driven by the New Zealand Government (2011) New Zealand's Cyber Security Strategy. However, any description of cybercrime in this strategy is undefined. Instead, the New Zealand Ministry of Justice (2013) seeks to define what is cybercrime in the New Zealand context by suggesting that "cybercrimes include criminal activities targeted at, or which utilise, a computer or computer network".

Interestingly, in New Zealand, the likelihood of a cyber attack is considered low, with indications that attacks on data confidentiality set for 'at least once a year' and attacks on infrastructure set for "once a decade". This alarming separation of time between potential cyber attacks suggests there maybe limited understanding of the opportunities that exist and the scope through which cyber attacks can take place.

Diagram 1: New Zealand Government. (2011) New Zealand's National Security System.

One of the key issues surrounding the debate as to whether cyber crime should be considered a threat to national security is that of classification. Cyber crime, similar to transnational crime encompasses an array of crimes not all of which are considered a potential threat to national security. While cyber crime generally encompasses crimes such as child exploitation, fraud, money laundering, “hacktivism”, espionage, terrorism and so on, in New Zealand the definition is generally rather broad across agencies and organizations that deal with cyber crime. Birchfield (2013), Norton (2015), New Zealand Police (n.d) and the Ministry of Justice (2013) define cyber crime as a crime using a computer, the Internet, or other electronic device, leaving the net wide open for types of crime that could be caught in that definition.

Interestingly, Grabosky (2014) differentiates between organized and nonorganized cyber crime when he discusses national security, suggesting it is not inherently the organization that makes these groups a national security threat, instead it is their aims or motivations. Further, Rosenbach and Belk (2012) argue that segregating cyber crimes into groups based on motivation better aids the people that have to deal with them. Therefore, by classifying cyber crimes into groups a particular group of people or a government department can be given the responsibility of dealing with that crime, using specialists with the necessary know how in that particular area.

Nonetheless, in order to classify and respond appropriately to cyber crimes, the motivation behind the crime must be known and understood (Rosenbach and Belk, 2012). For example, the downing of a nuclear power plant’s control systems could be the work of “hacktivists” who seek to protest against the use of nuclear power or, it could be the work of terrorists seeking to damage critical infrastructure, or an act of corporate espionage committed by a rival power company seeking to increase its stake in the market. While the benefit in having specialist groups to deal with certain cyber crimes is clear, the ability to accurately demarcate them into groups is likely to prove almost impossible when motivations are not always definable for analysis, particularly if the perpetrator cannot be located or simply chooses not to claim responsibility.

Diagram 2: New Zealand’s National Security System (New Zealand Government, 2011)

Acknowledging the difficulty in ascribing motivation and classifying cyber crimes, Demchak (2012) argues that it is difficult to say when a cyber event happens what its purpose is. Demchak argues instead for a generalization of cyber crimes. Arguably, if this is the case there needs to be a middle ground between Rosenbach and Belk's (2012) classification of motivation and Demchak's (2012) generalization, when it comes to effectively managing cyber crime threats to national security. Clearly not all cyber crimes are threats to national security, and Grabosky (2014) concurs this by stating that […] some [cyber criminal's] activity is unquestionably annoying, offensive in the extreme and/or harmful. There are online activities which, if writ large, might conceivably weaken the integrity and economy of states and thus come to be regarded as [national] security threats (Grabosky, 2014: 10).

Particular forms of cyber crime, no matter how morally reprehensible would not necessarily be considered a national security threat, for example, activities relating to online child exploitation.. Therefore, it appears possible to segregate certain cyber crimes from others. Consequently, when deciding if the cyber crime is a direct threat to national security, it seems appropriate to determine whether the cyber crime and its scale are likely to impact on the ability for a state and its citizens to function normally.

New Zealand's National Security Arrangements

The New Zealand Security Intelligence Service (SIS), who are tasked with collecting and disseminating intelligence relevant to New Zealand's national security, define security as: protecting New Zealand from espionage, sabotage and subversion. This includes protecting New Zealand from activities that are clandestine or deceptive or threaten the safety of any person, activities that impact adversely on New Zealand's international well-being or economic well-being, activities influenced by foreign organisations or persons and the prevention of any terrorist act or facilitating of any terrorist act (NZSIS Act, 1969). This definition provides for the inclusion of protection against cyber crimes such as cyber espionage or cyber crimes that could threaten the safety of a person such as downing the national power grid. The New Zealand SIS definition of security acknowledges the importance of both different types of threats and the scale of those threats. The New Zealand government defines national security as the ability for its citizens to go about their daily business confidently and free from fear, and includes that in order to achieve this, preparedness, protection and preservation of people, property, and information are key (New Zealand Government, 2011).

NZSIS are not solely responsible for the protection and detection of cyber crime in New Zealand—there are several government agencies responsible for tackling cyber security. In fact, the lead agency responsible for cyber security is the New Zealand SIS's fellow intelligence and security agency the GCSB. The GCSB's role in the protection and detection of cyber crime is not secret but neither is it widely publicised. The National Cyber Security Centre within the GCSB is tasked with the protection of government systems and to assist providers of critical national infrastructure (such as telecommunications companies) to improve their protections and response preparedness to cyber crimes. In its National Security System paper the New Zealand Government (2011)

acknowledges the importance of computers and the internet to daily life, business and trade but also the increased speed and scale with which they can threaten national security through their use in cyber crimes. Despite this they rate the likely incidence of cyber crime (including cyber attacks) to be only “once a year”. This suggests that there is a relatively low occurrence of cyber crime in New Zealand, something that even the limited reporting this article draws on, refutes.

NZ Police also have a role to play in both cyber crime and national security, through their National Cyber Crime Centre, similar to the GCSB, the National Cyber Crime Centre’s role and mission are not well publicised. The New Zealand Police is also responsible for the administration of the Crimes Act 1961, which has relatively few cyber specific provisions. For most cyber crimes, there is no cyber specific legislation within New Zealand law. Predominantly cyber crimes would fall under general definitions of crime such as fraud, terrorism, espionage etc. However, the Crimes Act (1961) does hold a few specific provisions relating to accessing computer systems without authorization or for dishonest purposes, or damaging or interfering with computer systems.

While having several agencies involved in the protection and detection of cyber crime appears comprehensive, it raises the issue of reporting. Both in the sense that it is not strictly clear about who to report cyber crimes to and in the sense that when reported they may never be officially published in annual statistics, recorded in any public sense, or actioned by way of prosecution. Reporting and prosecution will be discussed later in the article.

Cyber Crime in New Zealand

Diffusion of power also potentially contributes to cyber crime being a national security threat. The New Zealand Government comparable to other western governments is no longer the dominant player or holder of all the national defence cards. Cyber is a domain difficult to dominate or control because it is fluid and inexpensive relative to building naval carriers or airplanes (Nye, 2012). “Cyber technology gives much more power to non-state actors […] and the threats such actors pose are likely to increase” (Nye, 2012: 22). Interestingly, Nye (2012) is not only referring to clear threats such as cyber attacks by non-state actors but also that non-state actors control much of a government like New Zealand’s, infrastructure.

These non-state actors hold much of New Zealand’s economic potential and intellectual property and therefore pose a direct threat to national security if they do not actively protect their systems. It is this ‘power dependence’ and diffusion of power that Burke (2009) argues New Zealand and other western governments now rely upon. Relying on the private sector to play their part in protecting national security interests, is recognition there are in fact “limits to the state’s capacity to reduce [and prevent cyber] crime” (Burke, 2009: 313). Furthermore, the New Zealand SIS (New Zealand Security Intelligence Service, 2013) reports that cyber attacks on government and critical infrastructure are on the rise, with 134 incidents reported in their 2012 annual report. The

Government Communications Security Bureau (GCSB) reaffirmed the rise in cyber crime incidents when it announced in late 2014 that cyber security incidents had risen by 60% (RadioNZ, 2014).

A recent University of Waikato research report states that half of New Zealand businesses surveyed did not have sufficient tools or policies to mitigate cyber threats (Meadows, 2014). This is particularly concerning as researchers also identified the businesses that were the most vulnerable were also the most critical to the economy. Both the rise in cyber attacks reported by the New Zealand SIS and the lack of preparedness of New Zealand business and critical infrastructure serves to endorse the Insurance Council of New Zealand's claim, "New Zealand is woefully underprepared for the increasing threat of cyber [crime]" (Insurance Council of New Zealand, 2014).

Case Study 1: Anonymous

New Zealand is [clearly] not immune from cyber [crime]. A successful targeted cyber attack could disrupt our critical services, negatively impact our economy, and potentially, threaten our national security (New Zealand Government, 2011). It is clear that the New Zealand Government itself is a target of cyber crime and is vulnerable to attack, with the attack by the "hacktivist" group Anonymous in 2011 a prime example (The Nelson Mail, 2011). The group disabled the use of the New Zealand Parliamentary website after stating that it did not approve of the passing of the Copyright (Infringing File Sharing) Amendment Bill—imposing fines and internet suspension for those involved in illegal file sharing. Anonymous' statement, released on YouTube not only passed on their disapproval but went on to say "unless the government repeals these laws, Anonymous will continue to take down New Zealand's government websites" (Parliament Today, 2011). The group did just that two years later when they took down 13 ministerial websites after the passing of the Government Communications Security Bureau (GCSB) Amendment Bill (Keall, 2013)—which broadened the scope of the GCSB's powers. Both incidents received wide coverage by various media outlets, highlighting the attacks and parliamentary member's reactions. However, none of the coverage discussed the consequences of these attacks, no member of parliament publicly expressed a desire for justice or punishment and the New Zealand Police were not quoted as "looking into the matter". Both attacks were illegal protests that centred on denial of access to parliamentary websites/services. Arguably, there would have been more of an investigation had Anonymous, in protest, physically walked up to the parliamentary buildings, chained the doors shut and denied anyone access to the buildings. At a minimum, New Zealand Police would have attended and launched an investigation.

Case Study 2: Telecoms

A lack of or difficulty in investigating cyber crime is further exemplified in another cyber crime related event—the denial of service attack of Spark, a New Zealand telecoms service provider which lasted just over 24 hours. This coordinated attack meant that Spark customers nationwide were either unable to access the Internet or experienced slow internet speeds, both broadband and

mobile data (Downes, 2014). The attack was caused by cyber criminals using nude photos of celebrities to facilitate the passage of malware (Weekes, 2014). Spark customers who viewed these apparent pictures inadvertently installed software designed to flood the server's connection and essentially overload it causing the denial of service (Downes, 2014). Like the Anonymous attacks, neither the media nor Spark reported launching a police investigation into the matter, but rather Spark was concerned about isolating and then removing the software causing the problem, not isolating and removing the people behind the software. Also of concern, Spark reported that it was only a "handful of customers" (National Business Review, 2014) who had installed the malware, which suggests minimal effort is in fact required in order to down New Zealand's main telecoms service provider. Incidentally, a more serious cyber attack seems distinctly possible considering the apparent minimal effort that it took to down New Zealand's largest telecoms provider. Particularly so, if non-state actors such as telecommunication service providers and government websites do not actively protect systems that are critical to the maintenance of New Zealand daily life and business and therefore the maintenance of national security (Chhana, 2013).

Reporting Cyber Crime

New Zealand's reporting channels in response to increased threat from cybercrime activities is still evolving. Currently sites such as The Orb[1] are advertised as an online tool for reporting cyber crime incidents. However, the ability to accurately assess whether this is the case is significantly marred because of the lack of statistics on cyber crime in New Zealand. Currently, a website exists (The Orb) where individuals in New Zealand can report cyber crimes such as banking fraud, privacy issues, system attacks etc. (NetSafe, n.d.). Such reports are then forwarded to the government agency which The Orb, run by NetSafe thinks is the most suitable to investigate. Statistics New Zealand confirm that national crime statistics are pooled solely from New Zealand Police data and do not include data collected by other agencies (Statistics New Zealand - R. Mair, personal communication, December 15, 2014). Therefore, cyber crimes reported to The Orb are not simultaneously reported to New Zealand Police and are therefore not recorded against national statistics for overall crime, thus providing a distorted picture outlining cyber events.

The most recent crime statistics for New Zealand have categories such as, theft, homicide, and fraud; however, cyber theft, cyber fraud etc. are absent (Statistics New Zealand, 2014). New Zealand Police have recently reported that there has been a 3.2 percent drop in overall crime from last year (Boyer, 2014) opening up the debate as to whether physical crime is falling owing to a rise in cyber crime (Warner, 2014). The ability to accurately assess whether this is the case is significantly mired because of the lack of statistics on cyber crime in New Zealand. Current statistics reporting levels of cyber crime throughout New Zealand lack clarity, reinforced by statements from the New Zealand Security Intelligence Service (2013) who acknowledge that current analysis of cyber crime and its threat to New Zealand are based around estimates. This is clearly due, at least in part, to a lack of reporting or misreporting of cyber crime, not just by

individuals but also businesses. Incidentally, the NetSafe site “The Orb” does not facilitate opportunities for businesses in New Zealand to report cyber crime. However, even if the site did cater for businesses as well as individuals, it is likely companies who have been the victim of a cyber crime, may be unwilling to report the crime for fear of customers and investors losing trust and support, and choosing to withdraw investments (Birchfield, 2013; Chhana, 2013; Roeder, 2014).

Resulting from the disparities surrounding the reporting of cyber crime, several issues remain. Firstly, victims may not think to report the crime at all; secondly, they may report it but not to the police, thirdly the outlets where they are reporting it to may not pass that information on to the police and fourthly even if reported to the police, it may not be classified or coded as a cyber crime. Consequently, as Warner (2014) suggests, people in countries like New Zealand fail to seriously address cyber crime or consider it an actual crime due to its virtual nature, and as such may not treat it like an actual crime. It is clear that you contact the bank in question about a suspicious transaction on your account but whom do you call when your email has been hacked—your email provider? Accordingly, these issues may be creating a false representation of the incidence of cyber crime not only in New Zealand but globally if reporting mechanisms are unable to compile the various data related to cyber activities. Reports of a drop in overall crime may have inadvertent repercussions for New Zealand Government and New Zealand in its entirety if the significance of cyber crime activity in New Zealand is overlooked. Warner (2014) accepts these issues by suggesting cyber crime is not treated the same way as physical crimes, as evidenced by the Spark and Anonymous attacks neither of which initiated a public police enquiry or prosecution. If authorities decline to initiate accurate reporting, the allocation of sufficient resources towards the prevention of cyber crimes and opportunities to increase resilience are likely to be squandered.

The current situation is therefore potentially dangerous, suggesting New Zealand is not basing national threat assessments on accurate or complete statistics. If a significant cyber attack were to occur, New Zealand could potentially be unprepared. Hence, statistics collected through a comprehensive and accurate reporting mechanism are needed in order to ascertain whether cyber crime and the scale of the cyber crime that are likely to challenge New Zealand’s national security by altering the ability for New Zealand and its citizens to function normally. Fundamentally, non-reporting, misreporting, or an inability to accurately record cyber crime influences agencies’ ability to sufficiently combat it. Both resourcing and research stem from agencies and government more generally being able to justify the need. If cyber crime is not accurately and fully reported and recorded in a central location (like most other crimes are) then there is an inherent failure in government’s ability to predict its impacts on New Zealand business and livelihoods, therefore affecting their ability to effectively plan for defence and resilience. As the saying goes, a failure to plan means a plan to fail.

Prosecuting Cyber Crime in New Zealand

A key issue that arises out of discussions around whether cyber crime is a direct threat to New Zealand's national security and our ability to compile accurate statistics on its occurrence is prosecution and punishment. Tabansky (2012) and Burton (2013b) discuss a person's choice to use cyberspace for illegal means over physically committing the crime. They argue that the choice is obvious; cyberspace can offer speed, anonymity, remote operation, and the possibility of the crime going un-reported and therefore a reduced risk of apprehension and prosecution. However, actually committing the crime is likely to be slow and require actual presence at a location. Therefore the potential for someone to recognize the individual, increases the chance the crime will be reported, suggesting the chance of apprehension is high. Classical criminology theorises that crime is a decision and in making that decision we use the same rationale; if there is a certainty of punishment the rational choice is to not commit the crime (Pepinsky, 1980). From a classical criminological standpoint therefore, the rational choice is to commit a cyber crime in preference to physically committing a crime because punishment is far from certain. As Tabansky agrees, "state responses have not kept up with the pace of technological changes in cyberspace" (2012: 120). Where a physical crime would illicit a police investigation, a cyber crime may not even be reported to the police (Warner, 2014) or even if it were the investigation may be thwarted because the crime occurred in another country for which an extradition treaty is not available or New Zealand holds no jurisdiction (Grimes, 2014).

This point is echoed in a report by New Zealand's Ministry of Justice (2013), the Ministry also states that prosecution challenges will only increase as social and commercial use of computers and the Internet expands. Cox (2006) argues that New Zealand law has not kept pace with other western nations' responses to cyber crime. He goes on to state that although there have been minor amendments to the Crimes Act (1961) these have not sufficiently allowed for the globalized nature of most cyber crimes. As such, this indicates New Zealand would lack jurisdiction to prosecute in many cases, particularly in the instance that the victim or the effects of the cyber crime are within New Zealand but neither the hacker nor the computer are. A New Zealand Herald article in 2011 outlined how 80 percent of those surveyed did not expect cyber criminals to be punished. This could be partly due to the fact that the lead agency in cyber security, while tasked with doing "everything necessary or desirable" (GCSB Act, 2003) to protect cyber security has no actual law enforcement powers or ability to prosecute those who are threatening New Zealand's national security through committing cyber crimes. New Zealand Police would seem the natural fit to be the enforcement agency against cyber crime, being the administrators of the Crimes Act (1961). However, as discussed, there are several agencies that play a role in cyber security in New Zealand. While a multidisciplinary and multi agency approach to cyber crime is advocated, a lack of coordination between agencies can hinder not only accurate reporting and statistics but prosecutions as well.

Burton (2013b) argues that because New Zealand has not advanced its security strategy since the Cold War, it is stuck in the mentality that "enemies" or criminals will remain discouraged by classical means, such as the military or trade embargos. Burton (2013b) contends that cyber criminals are unlikely to be deterred, as the link between the punishment and the perpetrator is too

distant.

In support of the difficulties in tackling cyber crime, Hypponen (2011) goes so far as to argue that those people living in western nations, like New Zealand, are more likely to be victims of cyber crime than crime in “real life”. Manning (2013) concurs with this perception, affirming that a report from internet security firm Norton found one in four New Zealanders had fallen victim to a cyber crime in 2012. However, this finding is not reflected in either national crime statistics or prosecution records.

Discussion

Cyber crime is a direct threat to New Zealand’s national security (Hickey, 2011; Conservative Party, 2010; Burton, 2013b), in so much as it has the potential to down infrastructure, damage the economy through the loss of intellectual property, trade secrets or commercially sensitive information and disrupt and damage the lives/livelihoods of New Zealanders. New Zealand being both relatively small and geographically isolated is heavily reliant on technologies that allow both individuals and businesses to connect globally—arguably this is reflected in exports making up $65 billion of New Zealand’s Gross Domestic Profit (GDP) and investment making up $55 billion ($240 billion total) (Statistics New Zealand, 2013). Although New Zealand has previously been afforded somewhat inherent physical national security because of its isolated location, New Zealand can no longer consider itself removed or isolated as its involvement internationally and connections globally, have supported the prerequisites for being open for business from cyber criminals.

Both the United States and the United Kingdom have cyber crime listed as a tier one threat, or put another way, on par with terrorism (Harris, 2013; Roeder, 2014) and the World Economic Forum ranked cyber crime the single largest threat to global infrastructure in 2012 (Birchfield, 2013). Yet, in New Zealand, the threat is much lower according to government assessments (New Zealand's Cyber Security Strategy, 2011) despite high access rates compared to overseas and an increasingly high adoption rate to new technology. It is critical that New Zealand maintain the current level of confidence it receives globally in order to maintain not only trading and investment confidence but confidence in New Zealand’s ability to provide security for citizen’s and visitors alike. Should New Zealand not be able to sufficiently protect, defend against and plan for cyber crime partners may lose trust in New Zealand’s ability to maintain a secure trading environment. New Zealand markets itself globally as a safe a friendly place to visit with tourism making up 7 percent of New Zealand’s GDP. New Zealand is heavily reliant on ensuring that it maintains this image, which includes protecting its visitors from cyber crime. Cyber crime has not only the potential to influence New Zealand’s national security through its economy but also through its ability to cause damage and disruption to daily activities, such as through denial of service attacks (i.e., Spark). These types of cyber crimes are not only disruptive but are also threatening to trust and confidence in the businesses they affect.

While New Zealand does not currently receive the global attention the United Kingdom and United

States do, New Zealand is inextricably linked through the Five Eyes agreement; meaning security concerns in the United Kingdom and United States are equally as important and of concern to New Zealand. New Zealand is also as dependent on the cyber world as either of these two nations are, indicating how “computer systems and networks which underpin all essential sectors and aspects of daily life [have] characteristics similar in complexity to that of the broader terrorist threat: it is international and multifaceted” (Conservative Party, 2010: 22). Inherently, cyber crime is directly linked to national security, as it threatens the computer systems, networks, and infrastructure that support New Zealand’s daily life. However, the most compelling case as to why cyber crime is a threat to New Zealand’s national security is the potential for reward. Between September 2011 and September 2012, cyber crime reportedly cost New Zealanders an estimated $625 million (Griffin, 2012; Chhana, 2013) impaired by statistical reporting inconsistencies—this figure may only represent the tip of the iceberg, with significant supplementary cyber crime activities going unreported. It has also been argued that cyber crime in New Zealand is bigger than the black market in various narcotics (Griffin, 2012).

While this article considers cyber crime to be a threat to New Zealand’s national security, due to its speed, relative anonymity, relatively low operating cost and its ability to destabilize the economy and critical infrastructure, the authors are conscious that in doing so it evokes a potential for over securitisation of an issue. This is where a state can claim special rights to use whatever means necessary to combat an issue (Greener-Barcham and Barcham, 2006). Cyber crime is fluid and adaptive indicating governments, including the New Zealand Government, require government departments and national legislation to be equally fluid and adaptive, without excessively infringing civil liberties (Greener-Barcham and Barcham, 2006; Conservative Party, 2010). Ultimately, this then unfolds in the same way as cyber crime has unfolded through a process of trial and error—signified by revelations of the New Zealand GCSB spying on a New Zealand permanent resident (Radio New Zealand, 2014) that later resulted in the legislation being altered. So, is the New Zealand perspective different from other countries? Clearly the answer here is “no”. What it demonstrated in the New Zealand context is that the issues presented by cybercrime are something which need to be addressed through a combined agency approach-capable of promoting greater clarity around the reporting of cybercrime and current issues. Clearly, cyber crime provides the perfect example of where the line between domestic and foreign threats to national security becomes blurred beyond recognition. Therefore, government departments need to move beyond purely domestic or foreign focus and become some combination of the two. The changing demands of national security from the threat of cyber crime require continual vigilance and revision of policy and legislation to combat the growing tranche of cyber crime activities.

The authors therefore suggest the key to achieving and competing with the demands of cyber crime, remain in cooperation and resilience: “since crime [including cyber crime] has gone global, purely national responses are inadequate as they displace the problem from one country to another” (Harfield, 2010). It is necessary for not only old allies like the Five Eye’s but also emerging states to cooperate in order to combat cyber crime, as it is often these emerging nations that lack the relative capability or legislative authority to intervene in cyber crime. As Roeder (2014)

argues, cyber criminals are agile and well connected and that nations must be just as willing to connect and co-operate as their criminal counterparts. If the New Zealand Government is to fully recognize cyber crime as a threat to national security, it must ensure the development of national technological and manpower capabilities, accurate and full national reporting and promote departmental collaboration and international cooperation (Chouhan, 2014). No longer are threats by cyber crime realistically now “once a year” events that have minor relative consequences. The aim of building national and international cooperation is “primarily to have resilience across [a] nation dependent on its digital substrate” (Demchak, 2012: 66).

Therefore, “unlike the Cold War, security does not lie greatly in the preservation of state power or in its exercise but in the capacity of a society as a whole to work together in a crisis” (Conservative Party, 2010: 20). With this in mind, the New Zealand Government needs to ensure national resilience to cyber crime. It has already recognized that it is important to make the public aware of cyber crime and online security to protect its own information systems and revise its cyber incident response plan (New Zealand Government, 2011) as part of making New Zealand nationally resilient. Recognition of the importance of resilience is of course necessary given the potential for disruption to occur in a modern, networked, and interdependent society such as New Zealand (Omand, 2009). However, the authors suggest the need to place greater emphasis on building cyber resilience, awareness, and reporting within New Zealand businesses and critical infrastructure, as these are likely to be the biggest targets for cyber criminals (aside from the government itself) (Tabansky, 2012; Manning, 2013).

If security is understood not just as a question of external military threats to national sovereignty but also as that of the effective functioning of society in socioeconomic and political dimension, then there can be no doubt that […] [cyber] crime is indeed a severe security concern (Schloenhardt, 2003: 191).

As discussed, cyber crimes such as, cyber espionage, cyber terror and cyber attacks on critical infrastructure are cyber crimes that directly threaten national security in New Zealand. They achieve this by undermining trust not only in governance[2] but also in private sector service providers, nationally and internationally. It is therefore, important that the New Zealand Government continue to improve and encourage reporting of cyber crime and effective cybersecurity not only in their own systems but both in the private companies that control much of New Zealand’s critical infrastructure and New Zealand’s economic potential (e.g. intellectual property) and in the New Zealand public generally. In the past, this level of threat has been relatively low, despite threats having become real events (e.g., Anonymous). This point is further exemplified, as while this article was being written, both the New Zealand general public and businesses, fell victim to another cyber crime involving Ransomware (Morton, 2015).

Similar to tactics already adopted overseas, New Zealand requires an innovative and continuous approach capable of fully supporting all activities related to the prevention of cyber crime. Doing so, directly supports the New Zealand public’s trust and confidence and further demonstrates New

Zealand’s strength in tackling the systematic problems relating to cybercrime amongst security allies.

While New Zealand may not currently experience the volume or severity of cyber threats that our allies do their trust in our ability to manage threats and maintain security is essential in their continued willingness to share information and intelligence with New Zealand. As Schloenhardt acknowledges, cyber crime is indicative of having strong influence on national security because of its scale, where it has “reached levels that have [or will have] a strong impact on the functioning of government authorities, bilateral relations and on society and regional stability as a whole” (2003: 191). As discussed, should awareness (through reporting and prosecution) and co-operation not be improved New Zealand like most in the Western world will continue to find cyber crimes adaptive and difficult to prosecute due to globalization and a lack of reporting (Richardson, 2015). Furthermore, the literature in this area could benefit from accurate statistics on the rates of cyber crime within New Zealand and information relating to the investigation and prosecution of such crimes.

Clearly, this article concurs with Omand (2009), Bergeron (2013), Grimes (2014), Roeder (2014), and Hogg (2007) when they identify cyber crime as a broad national security issue, encompassing both public and private sectors with both national and international consequences. As Maughan succinctly states, cyber-crime “is a national and global challenge with far-reaching consequences that requires a cooperative, comprehensive effort across the public and private sectors” (2010: 30). New Zealand Inc. therefore must ensure the public and private sectors are equipped with sufficient technical expertise and knowledge to keep pace with a rapidly changing cyber security environment (Burton, 2013a).

References

Bergeron J (2013) Transnational Organised Crime and International Security. *The RUSI Journal* 158(2): 6-9.

Birchfield, R. (2013) Cyber threats and data privacy. *Management* 46-51.

Boyer S (2014) Police release crime stats: 3.2 drop in recorded offences. *The New Zealand Herald*. Retrieved from

http://www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=11334843

Burke RH (2009) *An Introduction to Criminological Theory*. Oxon, England: Taylor & Francis.

Burton J (2013a) Cyber security: the strategic challenge and New Zealand's response. *New Zealand International Review* 38(3): 5-8.

Burton J (2013b) Small states and cyber security: The case of New Zealand. *Political Science* 65(2): 216-238.

Chana R (2013) *Government Communications Security Bureau Act Review*. Wellington, New Zealand: Department of Prime Minister and Cabinet.

Chouhan R (2014) Cyber Crimes: Evolution, Detection and Future Challenges. *The IUP Journal of Information Technology* 10(1): 48-55.

Conservative Party (2010) *A Resilient Nation and National Security Green Paper* (Report No. 13). London, England: Conservative Party.

Cox N (2006) Cyber crime Jurisdiction in New Zealand. *Cyber crime Jurisdiction: A Global Survey* 11: 177- 188. Retrieved from http://www.reocities.com/noelcoxfiles/Cyber-Crime.pdf.

Demchak C (2012) Resilience, Disruption and a "Cyber Westphalia": Options for

National Security in a Cybered Conflict World. In N Burns and J Price (eds) *Securing Cyberspace – A New Domain for National Security*. Washington, DC: The Aspen Institute.

Downes S (2014) Spark broadband still down for many. *Stuff.co.nz*. Retrieved from

http://www.stuff.co.nz/business/10468128/Spark-broadband-outagesnationwide.

Government Communications Security Bureau Act (2003) Retrieved from http://www.legislation.govt.nz/act/public/2003/0009/latest/DLM187178.h tml.

Grabosky P (2014) *Organized crime and national security* (Report No. 2014/40).

Canberra, Australia: Regulatory Institutions Network.

Greener-Barcham BK and Barcham M (2006) Terrorism in the South Pacific? Thinking critically about approaches to security in the region. *Australian Journal of International Affairs* 60(1): 67-82.

Griffin P (2012) The crime online. *Listener* 52.

Grimes RA (2014) Want “perfect” security? Then threat data must be shared. *Info World*. Retrieved from http://www.infoworld.com/print/242383.

Harris A (2013) How to disarm an infrastructure hacker. Engineering and Technology Magazine. *The Institution for Engineering and Technology* 8(10). Retrieved from http://eandt.theiet.org/magazine/2013/10/the-invisibleattack.cfm.

Hickey K (2011) How international cyber crime threatens national security. *GCN, Technology, Tools and Tactics for Public Sector IT*. Retrieved from http://gcn.com/Articles/2011/07.27/International-cyber-crime-threat-toUS.aspx?p=1.

Keall C (2013) Anonymous New Zealand attack on National Party sites good news for John Key, GCSB Bill supporters. *The National Business Review*. Retrieved from http://www.nbr.co.nz/opinion/ anonymous-nz-attack-national-partysites-good-news-john-key-gcsb-bill-supporters.

Manning B (2013) New Zealand’s $152 Million cyber crime bill. *The New Zealand Herald*. Retrieved from http://www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=11140703

Maughan D (2010) The need for a national Cybersecurity Research and Development Agenda. *Communications of the ACM* 53(2): 29-31.

Ministry of Justice (2011) *Strengthening New Zealand's Resistance to Organised Crime An all-of-Government Response.* Retrieved from http://www.justice.govt.nz/publications/globalpublications/s/strengthening-new-zealands-resistance-to-organised-crime.

Ministry of Justice (2013) *Protecting against cybercrimes*. Retrieved from http://www.justice.govt.nz/publications/globalpublications/s/strengthening-new-zealands-resistance-to-organisedcrime/part-two-enhanced-response/protecting-against-cybercrimes.

National Business Review (2014) *Spark stabilises network following nationwide outages*. Retrieved from http://www.nbr.co.nz/article/problems-spark-broadbandmobile-after-malware-hits-customers-ck-162016.

NetSafe (n.d.) *The Orb*. Retrieved from http://www.theorb.org.nz/.

New Zealand Government. (2011) *New Zealand's Cyber Security Strategy*. Wellington, New Zealand: New Zealand Government.

New Zealand Government. (2011) *New Zealand's National Security System*.

Wellington, New Zealand: New Zealand Government.

New Zealand Security Intelligence Service (2013) *Annual report* (Report No. G.35).

Wellington, New Zealand: New Zealand Government.

New Zealand Security Intelligence Service Act (1969) Retrieved from http://www.legislation.govt.nz/act/public/1969/0024/latest/DLM391606.h tml.

Norton by Symantec (2015) *What is Cybercrime?* Retrieved from http://nz.norton.com/cybercrime-definition.

Nye J S (2012) The Third Annual Ernest May Memorial Lecture – Nuclear Lessons for Cybersecurity. In N Burns and J Price (eds) *Securing Cyberspace – A New Domain for National Security*. Washington, DC: The Aspen Institute.

Omand D (2009) *The National Security Strategy: Implications for the UK Intelligence community*. London, England: Institute for Public Policy Research.

Parliament Today (2011) *Parliament's site Under Attack: Hackers Claim Responsibility*. Retrieved from http://parliamenttoday.co.nz/2011/05/parliaments-siteunder-attack-hackers-claim-responsibility/.

Radio New Zealand (2014) *Kim Dot Com may sue Govt spy agency*. Retrieved from http://www.radionz.co.nz/news/political/249961/kim-dotcom-may-suegovt-spy-agency.

Richardson C (2015) Cyber criminals demand a modern approach to security. *The Dominion Post*. Retrieved from http://www.stuff.co.nz/technology/digitalliving/64625717/Cyber-criminals-demand-a-modern-approach-to-security.

Roeder B (2014) Cyber Security – It isn't just for signal officers anymore. *Military Review* 38-42.

Rosenbach E and Belk R (2012) U.S. Cybersecurity: The Current Threat and Future Challenges. In N Burns and J Price (eds) *Securing Cyberspace – A New Domain for National Security*. Washington, DC: The Aspen Institute.

Schloenhardt A (2003) Transnational Crime and Island State Security in the South Pacific. In E Shibuya and J Rolfe (eds) *Security in Oceania*. Honolulu, HI: Asia Pacific Centre for Security Studies.

Statistics New Zealand (2014) *Recorded crime victim statistics – Police district and area*

boundaries. Retrieved from http://nzdotstat.stats.govt.nz/wbos/Index.aspx?DataSetCode=99992#.

Tabanksy L (2012) Cybercrime: A National Security Issue? *Military and Strategic Affairs* 4(3): 117-136.

TEDx Talks (2011) Three types of online attack. Mikko Hypponen at TEDx Brussels [Video file]. Retrieved from http://www.ted.com/talks/mikko_hypponen_three_types_of_online_attack.

TEDx Talks (2014) Why do we call it Cyber Crime? Gary Warner at TEDx Birmingham 2014 [Video file]. Retrieved from http://www.youtube.com/watch?v=MPMr5jPwA71.

Telecommunications (Interception Capability and Security) Act 2013. Retrieved from http://www.legislation.govt.nz/act/public/2013/0091/latest/DLM5177923.

The Nelson Mail (2011) Cyber centre to protect against computer crime. pp. 5. ISSN: 11735678.

Weekes J (2014) Spark users experience Internet meltdown. *The New Zealand Herald.*

Retrieved from

http://www.nzherald.co.nz/business/news/article.cfm?c_id=3&objectid=11320100.