National Plan to Address Cybercrime

2015

Improving our ability to prevent, investigate and respond to cybercrime

newzealand.govt.nz

Contents

INTRODUCTION 3

Purpose of the Plan 3

What is cybercrime? 4

The nature of the cybercrime problem and the challenges for New Zealand 4

PRINCIPLES TO UNDERPIN OUR APPROACH 8

PRIORITY ACTIONS 8

1. Build capability to address cybercrime 9

2. Adapt New Zealand's policy and legislative settings for the digital age 11

3. Enhance New Zealand's operational response to cybercrime 13

4. Use New Zealand's international connections to combat cybercrime 14

A secure, resilient and prosperous online New Zealand.

newzealand.govt.nz

INTRODUCTION

New Zealanders live in a connected world. The Internet and information communications technologies (ICT) have broken down geographical barriers, brought people together and created opportunities for economic growth and innovation. New Zealanders' private and professional lives are underpinned by digital technologies as never before. Government, business, non-governmental organisations and individuals are seizing the opportunity to deliver services, transact business and communicate in cyberspace.

The cyber environment also provides opportunities for those with criminal or hostile objectives. The scale, speed and global nature of cybercrime present a challenge to traditional law enforcement methods and skills, and to confidence in our online world.

Purpose of the National Plan to Address Cybercrime

New Zealand's Cyber Security Strategy 2015 has four goals: Cyber Resilience, Cyber Capability, Addressing Cybercrime and International Cooperation. The National Plan to Address Cybercrime (the Plan) has been developed to support the cybercrime goal and contribute to the delivery of the Strategy's vision: **"A secure, resilient and prosperous online New Zealand"**.

The Plan sets out the New Zealand government's understanding of the cybercrime issue, principles and actions to improve our ability to prevent, investigate and respond to cybercrime and reduce harm to New Zealanders.

It will ensure New Zealand's response to cybercrime is coordinated at a national and international level, while also providing individuals and businesses with the tools to protect themselves.

What is cybercrime?

Cybercrime is part of a continuum of activity that ranges from cyber safety challenges to threats to national security. Cybercrime can encompass criminal activity from cyberbullying to state-sponsored theft of intellectual property. Cybercrime can be devastating to individuals, communities and business at both ends of the scale.

For the purposes of this Plan, **the definition of cybercrime has two elements.**[1]

- A criminal act that can only be committed through the use of ICT or the Internet and where the computer or network is the target of the offence. This is regardless of what the criminal goal is – whether political or financial gain, espionage or any other reason. Examples of cybercrime include producing malicious software, network intrusions, denial of service attacks and phishing.
- Cyber-enabled crime is any criminal act that could be committed without ICT or the Internet, but is assisted, facilitated or escalated in scale by the use of technology. This includes a vast amount of serious and organised crime, such as cyber-enabled fraud or the distribution of child exploitation material.

However, cybercrime is a subset of general crime, and the boundaries will not always be hard and fast.

The nature of the cybercrime problem and the challenges for New Zealand

THE COSTS OF CYBERCRIME ARE DIFFICULT TO CALCULATE RELIABLY

The extent of the cybercrime problem is not well understood. Worldwide, many instances of cybercrime go unreported. In some instances, victims will be unaware they have been affected. Other victims are too embarrassed to report the crime, do not know to whom to report, whether a crime has been committed, or do not believe law enforcement can provide a remedy. If victims receive a remedy from a supplier or financial institution, they may not also report a crime. Finally, businesses can be reluctant to disclose losses or breaches for fear of reputational damage. According to the UK Home Office, survey data suggests that in 2012, businesses reported only 2% of online crime incidents.[2] As a result, the economic cost of cybercrime is notoriously difficult to calculate reliably.[3] What we do know is that survey and anecdotal evidence indicates a high level of experience with cybercrime. One recent report estimated the annual cost to the global economy at more than US$400 billion.[4]

The indirect costs from cybercrime are equally difficult to quantify, including the opportunity costs. For many small-to-medium enterprises, cybercrime may result in 'denial of business' – nothing may be stolen, but an attack can reduce their ability to trade. Businesses and individuals also face costs to protect against cybercrime and for remediation (if required). Overseas, well-known losses include the theft of personal and financial information for 70 million customers of US retailer Target in 2013 and the theft of data related to 56 million credit cards from Home Depot in 2014. Cybercrime can also enable the organisation and perpetration of physical crime, for example fraud, extortion, disorder, sexual and other violent assaults.

[1] New Zealand Police "Prevention First: National Cybercrime Operating Strategy 2014-2017" (Wellington, 2014).

[2] M McGuire and S Dowling "Cyber crime: A review of the evidence" (Home Office Research Report 75, October 2013).

[3] Police National Intelligence Centre (NIC) "Summary from 'Cyber crime: The need to improve public confidence' (May 2014)" (New Zealand Police, Wellington, 2014).

[4] Police, 2014.

Cybercrime may result in social harms through embarrassment and nuisance and, in more serious cases, physical or emotional harm. In the Sony pictures hack in late 2014, large quantities of personal and commercial data were stolen and publicly released (in addition to triggering an international debate on freedom of expression in the digital age). Finally, while the financial losses from cybercrime can be small in an individual instance, the effects on public trust and confidence may be corrosive over time.

THERE IS NO COMPLETE PICTURE OF CYBERCRIME IN NEW ZEALAND

83%
of New Zealanders have experienced a cyber breach.

We are only seeing the tip of the iceberg. Research commissioned for Connect Smart Week 2014 found that 83% of New Zealanders had experienced a cyber-security breach.[5] This is not yet reflected in reporting, as New Zealand does not have a single, central point of reporting and breach disclosure is not mandatory. Even if they want to, victims do not always know where to report. Different agencies are responsible for different types of cybercrime, so some incidents will be reported to multiple places, while other victims may be passed from one agency to another in an effort to find the best place for a resolution.[6] Responses may also vary within each service. As a result, no one has a consolidated picture of cybercrime in New Zealand.

As the threat picture develops, we will gain a better understanding of what is required to effectively combat cybercrime, including the full ramifications of rapid technological change and emerging trends such as the rise of online or 'crypto' currencies. Related legislative reforms are already underway but further amendments are likely to be required to ensure New Zealand's legal framework is future-proof and facilitates an effective response to cybercrime.

IT IS DIFFICULT TO DETECT, INVESTIGATE AND PROSECUTE CYBERCRIME

Cybercrime produces high returns at a low cost and reasonably low risk to the criminal. Thousands of spam emails may generate small losses for each victim, but a much greater loss for New Zealand as a whole. The two most common techniques – social engineering (where a victim is tricked into granting access) and vulnerability exploitation (taking advantage of programming issues) – do not require much investment by criminals, due to the low marginal cost between one victim and thousands of victims.

Cybercrime can also be distinguished from 'traditional crimes' by the challenges its global nature presents for law enforcement. Individuals and groups overseas can operate wherever an Internet connection is present. The perpetrators are overwhelmingly based overseas and are highly organised – one United Nations report estimates that 80% of cybercrime is a part of organised criminal activity.[7] Traditional organised crime groups are migrating to this environment for greater profit at less risk.

[5] Connect Smart "Understanding Public Perceptions Toward Cyber Security" (July 2014). Last accessed 30/09/2014. http://www.connectsmart.govt.nz/assets/Uploads/Perceptive-Research-Understanding-Cyber-Security-Public-Perceptions-2014.pdf

[6] Police NIC, 2014.

[7] United Nations Office on Drugs and Crime "Comprehensive Study on Cybercrime: Draft." (February 2013). Last accessed: 24/09/14. http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf

The global element makes it difficult to find the perpetrator and access related evidence. Information exchange and cooperation between different countries can be poor and even where strong cooperative relationships exist, mutual legal assistance treaty processes can be very slow and cumbersome. Cases may require a disproportionate amount of investigative effort, reducing the availability of resources to deal with other demands. The country where a perpetrator is based may also not have the necessary skills or capacity to conduct a suitable investigation or preserve evidence.[8]

Investigation is further complicated by the ability to operate near-anonymously on the Internet. Attribution in cyber incidents is very difficult, particularly when an attack originates overseas. This makes cybercrime challenging not only to investigate but also to prosecute. Proxies and channels like The Onion Router (TOR) and peer-to-peer (P2P) networks can be exploited by criminals attempting to hide their identity under layers of encryption. Those networks are frequently used to facilitate criminal activity and pose challenges for law enforcement. One well-known example was the use of the now-closed 'Silk Road' site on the TOR network for drugs trading. The fastest growing is a market called 'Evolution' – advertising guns, stolen credit card data, stolen medical information and fake identification – which offers highly secure transactions.[9] Increasingly, such sites and dark markets are also selling cybercrime as a service, such as hackers for hire or simple toolkits. These developments lower the barriers for entry into cybercrime.[10]

Dark markets are selling cybercrime as a service: hackers for hire or simple toolkits.

Accordingly, a growing group of unskilled actors can have a relatively damaging impact. At the other end of the spectrum, the lines are blurring between criminal actors and state actors (some of whom may also act with criminal intent) as activity proliferates and techniques become increasingly sophisticated. As technology and detection strategies evolve, so too do the actors, making it difficult for responders to keep pace.[11] New Zealand offenders are not averse to using anonymising technology, including the use of TOR to attempt to hide sites providing child exploitation material and drug dealing.

NEW ZEALAND'S RESPONSE TO CYBERCRIME IS SHARED BETWEEN GOVERNMENT, NGOs, THE PRIVATE SECTOR AND INDIVIDUALS

A range of government agencies have policy and operational responsibilities related to cybercrime. Those roles have largely evolved organically rather than by design. At present, these include:

- **New Zealand Police:** overarching responsibility for crime prevention, detection and investigation in New Zealand, the Police Cybercrime Unit, Online Child Exploitation Across New Zealand (OCEANZ), Organised Financial Crime Agency New Zealand (OFCANZ).
- **Ministry of Business, Innovation and Employment:** Scamwatch and fraud awareness.
- **Department of Internal Affairs:** Electronic Messaging Compliance (anti-spam), Censorship Compliance Unit.

[8] Calum Jeffray and Tobias Feakin "Special Report: The Underground Web: The Cybercrime Challenge" (Australian Strategic Policy Institute, March 2015).

[9] Jeffray and Feakin, 2015.

[10] Police NIC, 2014.

[11] Police NIC, 2014.

- **Department of the Prime Minister and Cabinet:** the National Cyber Policy Office, Connect Smart.
- **Ministry of Justice:** criminal justice policy development.
- **National Cyber Security Centre** (in the Government Communications Security Bureau): advanced threats against New Zealand's information infrastructures of national importance.
- **New Zealand Customs Service:** border protection.
- **New Zealand Security Intelligence Service:** investigation of state-sponsored espionage, either directed against or involving New Zealand, with emphasis on detection and investigation of threats.
- **Serious Fraud Office:** serious or complex frauds.

However, cybercrime is a shared problem – non-governmental organisations (NGOs), civil society and the private sector all have a role to play in both prevention and response. NetSafe[12] and the New Zealand Internet Taskforce,[13] for example, provide a reporting point and incident advisories – and have taken on roles not currently provided by government. Twenty-three percent of all the reports NetSafe received in 2014 were directly referred from the New Zealand Police.[14]

The New Zealand government has also initiated Connect Smart:[15] a partnership with a range of organisations to raise awareness and capability. Many private sector companies provide a response to cybercrime as a part of their core customer service – managing cybercrime is a part of doing business in the 21st century – and build a range of protections into the services they offer.

Responsibility also sits with the wider community. The New Zealand Police's operating strategy is *Prevention First*, an approach which is also relevant to cybercrime.[16] Ideally, cybercrime will be prevented before it occurs. While there is no way to totally eliminate the risk, there are simple steps every individual can take to reduce risk. New Zealanders need to take cyber security threats seriously and be equipped with the tools and techniques to protect themselves online.

To reduce the number of cybercrime victims in New Zealand, we need to raise awareness in a way that creates behavioural change. Research commissioned as part of Connect Smart Week 2014 showed that, of the 83% of New Zealanders who had experienced a cyber-security breach, 61% had not changed their online behaviour since the breach.[17] The research also suggested that New Zealanders find the topic overwhelming, meaning there is a role for government, in partnership with the private sector and NGOs, to be a trusted source of information and advice.

Accordingly, there are opportunities for the government to improve the experience for victims of cybercrime, while also gaining a better understanding of the issue. A joined-up approach will be critical to provide an effective, customer-focused response to cybercrime. Confidence in the security and use of ICT will also be critical to achieve the government's objectives in delivering services to citizens via online channels.

[12] http://www.theorb.org.nz

[13] http://www.nzitf.org.nz

[14] Figure from NetSafe.

[15] www.connectsmart.govt.nz

[16] Police NIC, 2014.

[17] Connect Smart, 2014.

PRINCIPLES TO UNDERPIN OUR APPROACH

Four key principles underpin the New Zealand government's approach to cybercrime. Three of these are drawn from *New Zealand's Cyber Security Strategy.* The first principle (below) is specific to this Plan's cybercrime focus.

PREVENTING AND MINIMISING HARM

Initiatives and activities aimed at increasing awareness of the risks posed by cybercrime will be prioritised, with the goal of promoting behavioural change and raising capability to mitigate those risks.

ECONOMIC GROWTH IS ENABLED

Economic harm is a major consequence of cybercrime. Businesses in New Zealand – large and small – are increasingly affected by cybercrime. Ways to address cybercrime which support productivity and competitiveness will be sought.

A PARTNERSHIP APPROACH IS ESSENTIAL

The government has a role to play in cyber security – but it cannot do it alone. The cybercrime response is a shared responsibility and the New Zealand government will work in close partnership with the private sector, academia, civil society, individuals and other countries. That partnership will be based on mutual respect and trust.

The plan will seek opportunities to share experiences, best practice and to cooperate on research and development initiatives. Industry-led and targeted initiatives will be supported (for example, among the banking sector). The government will also continue to work with NGOs like NetSafe that are engaged in a range of cyber safety and security challenges on behalf of New Zealanders.

HUMAN RIGHTS ARE PROTECTED ONLINE

A key part of the New Zealand's government's approach to cyber security policy is to support the creativity, freedom, openness and dynamism that has made the Internet what it is today. New Zealanders should be able to engage online without suffering harm or unlawful interference.

PRIORITY ACTIONS

This Plan includes four priority actions. Each should be considered alongside the wider actions in the *New Zealand's Cyber Security Strategy;* all have been incorporated into the 2015 Action Plan.

1 Build capability to address cybercrime

2 Adapt New Zealand's policy and legislative settings to the digital age

3 Enhance New Zealand's operational response to cybercrime

4 Use New Zealand's international connections to combat cybercrime

PRIORITY ACTION 1

Build capability to address cybercrime

Preventing harm to New Zealanders means that increasing capability and awareness must be at the heart of any response to cybercrime, giving New Zealanders the incentives and tools to change their online behaviour. This should result in New Zealanders being alert to social engineering and other cybercrime techniques, and actively taking practical steps to protect themselves online. Law enforcement agencies will also have the capability to undertake search and evidence recovery when a crime has been committed. Success will be measured when New Zealanders know where to go for assistance and cybercrime rates reduce.

This is closely linked to the Cyber Capability goal in *New Zealand's Cyber Security Strategy.*

connect SMART
Protect yourself online

Connect Smart (www.connectsmart.govt.nz) was launched in 2014 to provide an ongoing, positive approach to cyber security, supported by a wide range of partners from across the public, private and NGO sectors.

Connect Smart is aimed at raising awareness of security and promoting ways for New Zealanders to protect themselves online.

USING THE CONNECT SMART BRAND TO PREVENT CYBERCRIME

We will continue to use the Connect Smart brand, website and partner channels to raise awareness of the cybercrime threat and promote behavioural change. Providing up-to-date alerts and information around current scams and attack vectors will help ensure New Zealanders understand the threat. Creating a clear understanding of the challenges will underpin active behavioural change by New Zealanders and foster a culture of cyber security. This will also align with initiatives like NetSafe's work with schools to 'grow digital citizens' and significant work by the Ministry of Education on digital literacy.

We will continue to provide advice, through Connect Smart, about simple tools and techniques to prevent cybercrime. It is critical that individuals and small-to-medium enterprises have up-to-date, trusted advice about what action they can take. We will work with partners to develop and distribute this advice through a range of channels, including the Connect Smart website and social media. We will also integrate Connect Smart messaging into crime-prevention initiatives and community liaison roles (such as Police community liaison officers).

DEVELOPING GOVERNMENT CYBERCRIME CAPABILITY

The *Strategy* sets out the need to develop a cyber security professional workforce and the difficulty in both attracting and retaining highly skilled people. This also applies to law enforcement. Electronic evidence is increasingly a part of many criminal investigations. New Zealand must ensure its capability keeps up with demand for these skills and emerging technologies. All front line Police officers and other investigators need, as a minimum, to be able to identify cybercrime and cyber-enabled crime. Investigators will need to be able to identify lines of enquiry and evidential material, and specialist units must have the capability to provide assistance in more complex and sophisticated cases. There must be enough skilled investigators to keep up with the rising demand for electronic evidence.

Agencies will continue to share experience, skills, knowledge and resources through the Electronic Combined Law Agency Group (e-CLAG). E-CLAG sits within the broader Combined Law Agency Group – a group of intelligence, enforcement and compliance professionals who

collaborate on a whole-of-government approach to leverage combined resources. CLAG partnerships are used to tackle the threats of cross-agency crime.

Members of e-CLAG are the digital forensic investigators and analysts from member agencies with digital forensic divisions. The field is rapidly evolving and, in some instances, an agency will only have one investigator or analyst on staff, hence a need to make use of the knowledge, experience and resources of other e-CLAG member agencies. Past and ongoing e-CLAG activities include joint agency training sessions and the provision of assistance and tools between member agencies (and to agencies without digital forensics capability). Current projects include developing a matrix capturing equipment assets and training requirements across agencies.

New Zealand Police is actively developing capability and training to deal with cybercrime. The Police *Prevention First: National Cybercrime Operating Strategy 2014-2017* sets out Police goals to develop capacity and capability to meet the growing needs around cybercrime and cyber-enabled crime. The Police Cybercrime Unit is the core Police unit that deals with cybercrime and provides Police with a central point of contact for other agencies. The Unit has recently expanded to seven staff, comprised of a mix of detectives and technical investigators.

Investments in core capability are designed to create a foundation for further development and capacity building. All front line staff (level one) will be trained to deal with customers at the front desk and triage incoming reports. Investigators (level two) will identify and follow online lines of enquiry, identify evidential material and prosecute offenders. Specialists within the Cybercrime Unit (level three) will deal with the more complex cybercrimes impacting on New Zealand businesses and our reputation. Training material will be in line with the Australia New Zealand Police Advisory Agency Training guidelines.

PRIORITY ACTION 2

Adapt New Zealand's policy and legislative settings for the digital age

Alongside increased capability, law enforcement and the national security agencies need appropriate and effective powers to investigate cybercrime. New Zealand's legislative and policy settings must adapt to new technologies and balance security and privacy. Rapid changes require a technology-neutral framework; at the same time, the global nature of cybercrime poses a challenge to traditional thinking about borders and jurisdiction. **This area of work** will be successful when New Zealand's legal framework supports a rapid and effective response to cybercrime.

LEGISLATIVE REFORM ALREADY UNDERWAY

In recognition of these challenges and other issues, legislative reform is underway in a number of related areas.

In 2014, following a report from the Law Commission, Cabinet agreed to the Ministry of Justice undertaking work to update New Zealand's privacy laws. Advances in technology since 1993 have dramatically changed how personal information is collected, stored and shared. Reform of the **Privacy Act 1993** will emphasise identifying and addressing risks before privacy breaches can occur.

The Law Commission is currently undertaking a review of the **Extradition Act 1999** and the **Mutual Assistance in Criminal Matters Act 1992**. These Acts frame New Zealand's response to requests from foreign governments in the investigation and prosecution of crime. The review is based on the effects of technological change, alongside other developments in the international context, such as globalisation, increasing mobility and transnational crime.

Law enforcement needs to operate swiftly across many jurisdictions.

The New Zealand Customs Service is in the process of reviewing the **Customs and Excise Act 1996**. The intent of the review is to ensure that the Act is flexible and permits Customs to undertake their border protection role using new technology and operating methods.

In response to rising concerns about the harmful effects of cyberbullying on young people, the **Harmful Digital Communications Act** was passed in July 2015. Under previous laws, it could be difficult for victims to deal with harmful digital communications – for example, trying to remove abusive, intimidating and distressing material from the Internet could be difficult, drawn out and costly. Also, few sanctions were available to aid such efforts and to hold offenders to account. The Act is intended to prevent harm and provide victims with quick and efficient redress. The Act has created a range of measures to address damaging electronic communications spread through methods such as emails, texts and social media posts.

DEVELOPING A BETTER UNDERSTANDING OF OUR LEGISLATIVE NEEDS

The Law Commission reviewed 'computer crime' in 1999. The drafting of legislation is technology neutral, but given technological and global developments, since then there may be a need to update or amend it.

Elements of New Zealand's legislative framework will be tested to see whether amendment to effectively prevent, investigate and respond to cybercrime is required. This would be a targeted review. Examples may include amending section 252 of the Crimes Act to permit Police to remove

botnet infections, considering widening enforcement powers to include seeking information on care and protection matters, considering whether we need an offence of unlawful possession of stolen data, reviewing the crimes involving computers provisions in the Crimes Act and the role of the Internet in funding or supporting organised criminal or terrorist groups.

Elements of New Zealand's policy and legal frameworks will be tested to see whether they need amendment to permit further preventative operational activity. Covert work currently plays an important role in investigating and preventing the online exploitation of children. Many criminal networks online rely on trust and confidence to operate so there may be opportunities to enhance a proactive approach to preventing cybercrime or responding to offenders.

MEETING TRANS-BOUNDARY CHALLENGES

Most cybercrime is perpetrated from outside New Zealand. Criminals exploit the differences between countries and evidence relating to a criminal act may sit in multiple locations.

The government will work with partners (including multinational companies) to meet the challenges raised by extraterritorial jurisdiction. Cybercrime often means that law enforcement needs to operate swiftly across many jurisdictions and to access information under many different legal and political regimes. This challenges our traditional notions of sovereignty and jurisdiction – and the issue will not be resolved by one state alone. Exploring accession to the Council of Europe Convention on Cybercrime is an important first step, as is working with companies to ensure that law enforcement and security agencies have lawful access to data.

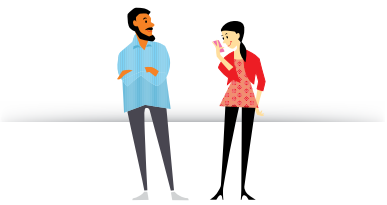
PRIORITY ACTION 3

Enhance New Zealand's operational response to cybercrime

A range of government agencies, NGOs and private sector companies play different roles in regard to cybercrime. To generate the strongest possible response to cybercrime, we need to work together and leverage our individual and collective strengths. Our measures of success will be a coordinated response to cybercrime and a better understanding of the size, nature and impact of cybercrime threats.

ENHANCING NEW ZEALAND'S RESPONSE TO CYBER INCIDENTS

As set out in *New Zealand's Cyber Security Strategy,* work is underway to establish a national CERT[18] to deal with issues across the spectrum, including cybercrime. New Zealand's cyber response capabilities have developed organically and are spread across a range of agencies. A CERT should bring some of those capabilities together and result in a more effective and efficient response for victims of cybercrime.



Making it easier for New Zealanders to report cybercrime will… help New Zealand better understand and respond to cybercrime

Ways to enhance cross-agency operational effectiveness in the prevention, investigation and response to cybercrime will be investigated. There are opportunities for agencies to share knowledge and techniques in investigations. As discussed earlier, some of this is already underway through forums like e-CLAG.

Police reporting will begin to distinguish cybercrime from other crimes. At present, it is not always possible to distinguish between crimes committed online and those committed offline. Police recording of reported incidents will need regular reviews to consider identification of cybercrime and cyber-enabled crime so that they are distinguishable from offences which are not facilitated by ICT. This will mean developing criminal behaviour is properly monitored, allowing new and developing trends to be better identified.

ENHANCING OUR CUSTOMER FOCUS

As highlighted earlier, cybercrime tends to be under-reported for a range of reasons. Making it easier for New Zealanders to report cybercrime will provide better support to victims and ensure better information is collected, to help New Zealand better understand and respond to cybercrime.

Options to establish a central point for cybercrime reporting will be considered. Options to improve customer experience will be considered by providing a single 'front door' at which issues are triaged and directed to the appropriate responder.

Victims of cybercrime have access to the same support as other victims of crime. Focusing on victims in the criminal justice system helps reduce the cost and impact of crime on individuals. Financial and emotional effects of crime on victims will be minimised and services for victims will be provided in a timely and credible way.[19]

[18] CERT was once an acronym for 'computer emergency response team'. Since 1997, CERT has been a registered trademark owned by Carnegie Mellon University and is no longer used as an acronym. New Zealand is requesting permission to use the CERT trademark.

[19] www.victimsinfo.govt.nz/

PRIORITY ACTION 4

Use New Zealand's international connections to combat cybercrime

International engagement is essential for cyber security. As a result, the principle of partnership applies equally internationally as it does domestically. New Zealand is not isolated in cyberspace, which creates challenges for law enforcement in investigating and prosecuting cybercriminals. The fundamentally global nature of the problem requires a coordinated international response. This will be successful when law enforcement in New Zealand can more effectively prevent crime and respond swiftly to cybercrime threats emanating outside our jurisdiction.

CLOSER COOPERATION ON CYBERCRIME

Differences in national laws and enforcement regimes can create barriers to effective international cooperation. New Zealand is committed to working with partners to reduce those barriers. Law enforcement agencies work closely with counterparts through INTERPOL and in Australia (particularly through the Australia New Zealand Policing Advisory Agency), Canada, the United States and the United Kingdom. New Zealand is also a member of the Virtual Global Taskforce, the Global Alliance against Child Sexual Abuse Online, the ASEAN Regional Forum and the London Action Plan on spam.

Consider progressing New Zealand's accession to the Council of Europe Convention on Cybercrime (also known as the Budapest Convention). The Council of Europe Convention on Cybercrime is the first international treaty seeking to address cybercrime by promoting harmonised legal frameworks, improving investigative techniques and increasing cross-border cooperation. It was developed by the Council of Europe but a wide range of states have since acceded to the Convention, including our closest partners. As at May 2015, 45 states parties have ratified the Convention. To accede will require a National Interest Analysis to test the benefits for New Zealand, including testing the domestic policy implications.

Continue to promote governance of cyberspace and norms of state behaviour online that reflect New Zealand's vision and interests. There is not yet a clear consensus about appropriate behaviour for states in an online environment. As set out in the *Strategy's* International Cooperation goal, New Zealand will continue to participate in the development of international consensus about appropriate state of behaviour and the development of confidence-building measures, including on cybercrime.

Strengthen New Zealand's relationships with international bodies focused on addressing cybercrime. There are opportunities for New Zealand to contribute to and benefit from relationships with other law enforcement groups (such as Europol, NGOs, and specialist bodies sponsored by the private sector such as Microsoft's Digital Crimes Unit). International cooperation currently relies largely on personal and informal relationships. New Zealand must find ways to ensure these ongoing cooperative relationships are maintained and embedded. For example, New Zealand Police currently has a secondee at the INTERPOL Global Complex for Innovation – a cutting edge research and development facility, based in Singapore.

Networks of international cooperation will be built to support operational activity, through joint investigations, joint operations, intelligence sharing, growing expertise and developing models of best practice.

CAPACITY BUILDING IN THE ASIA-PACIFIC REGION

New Zealand is committed to the maintenance of stability and security in cyberspace. Improving confidence and understanding of cyber security issues is an important part of international stability. Although the national response to cybercrime is still being developed, nevertheless New Zealand is relatively well-placed to contribute to building capacity in the Asia-Pacific region. As the Pacific region becomes more connected, the opportunities for cybercriminals will increasingly affect economic growth and regional security. Pacific states are also likely to be targets for criminal activity as criminals seek legislative settings that are less likely to facilitate their arrest and conviction.

Work with Pacific island states to identify gaps in their capability to respond to cybercrime and undertake capacity building activities in the Asia-Pacific region. New Zealand is one of 42 founding members of the Global Forum on Cyber Expertise (GFCE), launched at the 4th Global Conference on Cyber Space in the Hague in 2015. The GFCE is intended to give momentum to global cyber security capacity building. New Zealand's capacity building activities will assist in building a more secure, open and accessible cyberspace that delivers broad-based economic and social benefits. Efforts will focus on raising awareness of the opportunities and risks cyberspace offers and ways to manage those; along with practical solutions to raise the policy and operational capacity of law enforcement and other government agencies to respond cyber security risks.

newzealand.govt.nz