

Department of the Prime Minister and Cabinet

Minister of Broadcasting, Communications and Digital Media November 2018

To increase transparency and open government, the Minister of Broadcasting, Communications and Digital Media has decided to make publicly available the Briefing to the Incoming Minister (BIM) responsible for cyber security policy he received from officials. The Minister has released the following BIM provided by the Department of the Prime Minister and Cabinet's National Cyber Policy Office.

Some parts of this document would not be appropriate to release and, if requested, would be withheld under the Official Information Act 1982 (the Act). Where this is the case, the relevant sections of the Act that would apply have been identified. Where information has been withheld, no public interest has been identified that would outweigh the reasons for withholding it.

Title: Briefing to the Incoming Minister responsible for cyber security policy

Information withheld with relevant section(s) of the Act:

- s 6(a) – security or defence of NZ or international relations
- s 6(c) – maintenance of the law
- s 9(2)(f)(iv) – confidential advice under active consideration
- s 9(2)(g)(i) – free and frank expression of opinions



DEPARTMENT OF THE
PRIME MINISTER AND CABINET
TE TARI O TE PIRIMIA ME TE KOMITI MATUA

Briefing to Incoming Minister responsible for cyber security policy



Date

September 2018

Priority

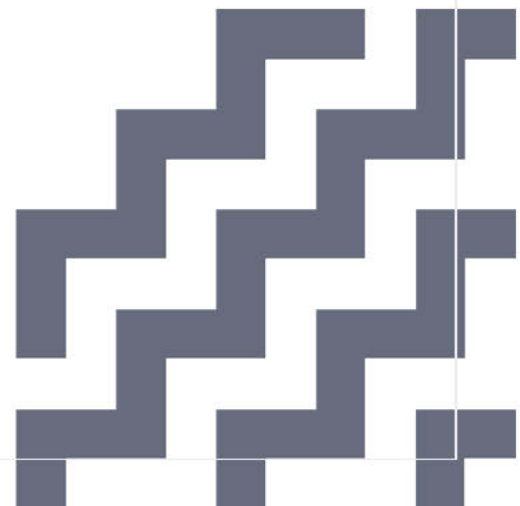
Routine

Security Classification

UNCLASSIFIED, formerly
RESTRICTED

Tracking Number

3999201





Welcome and introduction

Welcome to your role as the Minister responsible for cyber security policy.

New Zealand's national security and economic growth depends on management of our national risks, including securing and protecting our most significant information assets. The internet is simultaneously the backbone of the world's economy and a major threat vector. New Zealand's geographic isolation is no protection from cyber threats.

The National Cyber Policy Office (NCPO) within the Department of the Prime Minister and Cabinet (DPMC) leads the development of cyber security policy advice and advises the Government on investing in cyber security activities. It oversees the implementation of *New Zealand's Cyber Security Strategy* (the Strategy) and accompanying *Action Plan 2015* (the Action Plan).

Good progress has been made under this 2015 Action Plan. This includes the stand-up of CERT NZ, 'Connect Smart' public-private sector collaboration, work to build a cyber-security workforce, advice to small businesses through a cyber credentials scheme, the roll-out of the Government Communications Security Bureau's malware detection and disruption services for organisations of national importance, protective security requirements for government agencies, and significant international engagement.

There remains an upwards trajectory of cyber security threats. The widespread use of connected devices and emerging technologies has expanded the attack surface for malicious threat actors. Both CERT NZ and the National Cyber Security Centre (within the Government Communications Security Bureau) have reported a growing number of incidents. Globally, it is clear that cyber threat actors are increasingly bold, brazen and disruptive. Our international partners have intensified their efforts in response to this problem.

Cabinet agreed in April that it was timely for New Zealand to step up its cyber security efforts. Work is underway to refresh the 2015 Strategy and Action Plan to update New Zealand's cyber security posture, including to address the rapidly evolving threat and accelerate the pace of our response.

This briefing provides you with initial information you may require in your role as the Minister responsible for cyber security policy.

We look forward to working with you to advance a secure, resilient and prosperous online New Zealand.

UNCLASSIFIED (previously RESTRICTED)



Recommendation

The Department of the Prime Minister and Cabinet recommends that you:

- 1 Note the contents of this briefing
- 2 Meet with relevant officials to discuss the briefing, outline your requirements, and discuss how we can best support you.

NOTED

Howard Broad

Paul Ash

**Acting
Executive**

**Chief Acting Director,
National Security Policy
Directorate**

**Minister for
Broadcasting,
Communications and
Digital Media**

Date: / /2018

Date: / 09 /2018

Date: / /2018

Proactively Released by the Minister of Broadcasting, Communications and Digital Media

Contents

Briefing to Incoming Minister responsible for cyber security policy	1
Welcome and introduction	2
Recommendation	3
1. Overview	5
2. Your responsibilities regarding cyber security policy	5
3. The role of the National Cyber Policy Office	6
4. There is an upward trajectory of cyber threats	7
5. We are refreshing the Strategy and Action Plan	9
6. Progress on refreshing the Strategy and Action Plan	10
Understand Phase	10
Develop Phase	11
Deliver Phase	11
7. New Zealand's Cyber Security Strategy 2015 and Action Plan	12
8. Current Priorities	13
9. The role of other government agencies	16
The cyber security landscape	18
10. Conclusion	18
Appendix A: Additional actions 2017-2020	20

1. Overview

This briefing:

- a. explains how the National Cyber Policy Office (NCPO) within the Department of the Prime Minister and Cabinet (DPMC) can support you as Minister responsible for cyber security policy;
- b. sets out the New Zealand Cyber Security Strategy and Action Plan as the existing framework for government on cyber security;
- c. describes the increasing cyber threat trajectory;
- d. outlines work to refresh the Strategy and Action Plan in the face of this increasing threat;
- e. defines the cyber security roles of other government agencies; and
- f. signals a range of existing actions and initiatives for the 2017-20 period.

2. Your responsibilities regarding cyber security policy

Ministerial responsibility for cyber security policy


The Minister for National Security and Intelligence has overall responsibility for security policy (including cyber security). The Prime Minister through the priorities process, has allocated Ministerial responsibility for cyber security policy (and CERT NZ¹) to the Minister for Communications, Broadcasting and Digital Media.

Other Ministers involved in cyber security issues

On cyber security, you will work closely with:

- the Minister of National Security and Intelligence (the Prime Minister);
- the Minister Responsible for the Government Communications Security Bureau (GCSB);
- the Minister Responsible for the NZ Security Intelligence Service (NZSIS); and
- the Minister of Foreign Affairs and Trade.

¹ 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. CERT NZ was set up in April 2017 to receive reports of cyber incidents, analyse threats, share information and advice, coordinate incident responses and be a point of contact for the international CERT community.



Given cyber security is a cross-cutting issue, you will also have close engagement with a range of other Ministers, including the:

- Minister of Justice;
- Minister of Police;
- Minister of Internal Affairs;
- Minister of Defence; and
- Minister for Economic Development.

Section 8, below, discusses the role of government agencies involved in cyber security.

3. The role of the National Cyber Policy Office

The NCPO formally reports to you on cyber security policy matters, in consultation with other Ministers as appropriate. The NCPO is a seven-member team within the National Security Policy Directorate, led by Paul Ash. The National Security Policy Directorate sits within DPMC's National Security Group, reporting to Howard Broad as DPMC's Deputy Chief Executive, National Security. We would be happy to brief you on the work of the National Security Group.

The NCPO was established within DPMC in 2012. Since then, it has led the development of cyber security policy advice for the government and advised the government on its investment of resources in cyber security activities. The NCPO oversees the implementation of the current *New Zealand Cyber Security Strategy* and accompanying *Action Plan 2015*.

The NCPO chairs the monthly inter-agency Cyber Policy Group which involves agencies such as Government Communications Security Bureau; NZ Security Intelligence Service; NZ Police; CERT NZ; Ministry of Business, Innovation and Employment; Ministry of Justice; Ministry of Foreign Affairs and Trade; Department of Internal Affairs; Ministry of Defence; and New Zealand Defence Force.

The Cyber Policy Group is a 'clearing house' to track progress, discuss initiatives and assess the overall direction of the New Zealand cyber security eco-system. Inter-agency collaboration has been and, in our view, remains essential to cyber security efforts. Given New Zealand's size, our ability to collaborate should be a point of advantage for the country.

The NCPO works closely with counterpart policy teams in central agencies in Australia, Canada, the United Kingdom, and the United States – known collectively as the 'Five Eyes'². It conducts international engagement (working with MFAT and

² 'Five Eyes' refers to the intelligence alliance comprising Australia, Canada, New Zealand, the United Kingdom, and the United States.

others) and outreach with the private sector on cyber security policy, particularly through the 'Connect Smart' public-private partnership³.

DPMC provides a part-time Private Secretary (currently Hamish Rogers) to support your cyber security policy work. The Private Secretary works in your office up to 50% of the time. The remainder of the role is allocated to the Prime Minister's Office, supporting the Prime Minister/Minister for National Security and Intelligence. The shared role reflects, in part, the close connection between your cyber security policy work and the National Security and Intelligence portfolio.

4. There is an upward trajectory of cyber threats

An upwards trajectory of cyber threats is affecting New Zealand. An increasing number of New Zealand individuals, businesses and organisations are being affected by cyber incidents.

We have recently dealt with the implications for New Zealand of a range of incidents. These include s6(a)

; the Wannacry ransomware (May 2017); and the notPetya ransomware (June 2017).


- The **National Cyber Security Centre** (NCSC) recorded 396 cyber incidents in 2016-17 – an average of 33 per month.
- In 2016-17, the NCSC worked with 33 public sector and 57 private sector organisations in relation to cyber incidents - providing hands-on intensive incident response on 31 occasions.
- **CERT NZ** recorded 506 cyber security incidents in its first three months of 2018 (January – March 2018), involving direct financial losses of over \$3,000,000. This number represents only the tip of the iceberg, as the majority of cyber security incidents go unreported.

s6(a)

This activity experienced by government agencies is mirrored in the private sector.

New Zealand's experience is not unique – we are dealing with a serious and growing international problem. Globally, there is growing use of cyber tools by state-sponsored cyber actors to pursue geo-political advantage. This might be aimed at strengthening influence, stealing commercially valuable information, undermining, or embarrassing other states, creating chaos and disruption, retaliating for the actions of other states, practicing techniques, or pre-positioning for future advantage. State-

³ 'Connect Smart' is a public-private collaboration to drive cyber security improvement in New Zealand. It includes a growing network of banks, telecommunication companies and Internet Service Providers, ICT companies, software companies, social media, retail organisations, education institutions, non-government organisations, community groups, sectoral bodies, business associations and government agencies.




sponsored threat actors are one among a range of those carrying out cybercrime, with organised crime groups and individuals with criminal intent, and issue-motivated groups and individuals, also active online.

Cyber threat actors – state-sponsored or criminally-motivated – are acting in increasingly bold, brazen, and disruptive ways. Their intent may not always be evident but it is clear that cyber threat actors are taking advantage of weaknesses in others' systems. It is often difficult to attribute responsibility for cyber incidents, complicating the responses available to governments.

For example:

- July 2018: A cyber intrusion of Singapore's largest health care institution, SingHealth, resulted in the theft of personal profiles of 1.5 million patients along with the details of prescriptions for 160,000 people, including Singapore's prime minister, Lee Hsien Loong (who was repeatedly targeted in the intrusion).
- March 2018: The US Department of Justice indicted nine Iranians charged with infiltrating 144 US universities, 176 universities in 21 other countries, 47 private companies, and other targets like the United Nations, the US Federal Energy Regulatory Commission, and the states of Hawaii and Indiana.
- October 2017: Yahoo revealed that 3 billion user accounts were breached back in 2013 (three times more than the 1 billion announced in December 2016).
- September 2017: Equifax (United States credit agency) suffered a data breach affecting 145 million US customers.
- Mid-2017: compromises of national energy systems, including UK and Ireland, and US nuclear power plants.
- 2016: Foreign, likely state-sponsored, threat actors compromised the network of a New Zealand organisation and used its infrastructure to mount a significant cyber-attack on a foreign organisation.
- 2016: Reports of Russian interference in the United States 2016 elections and unauthorised disclosures from the US Democratic National Committee.
- 2015: Theft of 21 million personnel details from the United States Office of Personnel Management (attributed in the media to Chinese espionage).
- May 2015: Compromise and theft of information from the German Bundestag (Parliament).
- December 2015 and December 2016: Ukraine power grid outages as a result of cyber incidents.

This 'new normal' is an environment where cyber threat actors take covert action against others that, while it may be an unfriendly and damaging act, often falls short of interpretation under international law as an 'act of force' or 'intervention in a state's



domestic affairs'. This 'grey area' activity poses an increasing challenge to the ability of governments to deliver security services to their economies and citizens.

Technological advances – in encryption, artificial intelligence, machine learning, and the Internet of Things⁴ – will make the threat environment more challenging.

For example:

- October 2016: a massive Distributed Denial of Service (DDoS)⁵ attack affected access to popular websites such as Twitter, Spotify, Amazon, Reddit, Tumblr, PayPal, Netflix, Airbnb, on the East Coast of the United States. The DDoS was spread by infected Internet of Things (IoT) devices, such as video cameras, CCTV cameras and digital video recorders.

5. We are refreshing the Strategy and Action Plan

Cabinet agreed on 2 April 2018 to the refresh of *New Zealand's Cyber Security Strategy and Action Plan (the Refresh)* [ERS-18-MIN-0004/CAB-18-MIN-0127]. The Chair of the Cabinet External Relations and Security Committee (ERS) subsequently agreed to extend the report back from July to October 2018 to accommodate a more collaborative engagement approach to the Refresh [ERS-18-MIN-0010].

This decision:

- **demonstrates the government's commitment to building a connected nation** and harnessing digital technology for economic growth, community benefit and innovation. Cyber security is essential to ensure that the gains of digital technology are not eroded, to protect the information and networked systems that are vital to our economic growth, and to enable New Zealanders to interact online without suffering harm. The ability to provide good cyber security may come to be seen as an indicator of economic competitiveness (and offer economic opportunities).
- **complements other initiatives already underway, such as the development of a Digital Strategy for New Zealand**, the proposed establishment of a Chief Technology Officer and the priority accorded to digital rights;

⁴ The Internet of Things (IoT) is the inter-networking of devices – enabling devices to collect and exchange data, be controlled remotely, communicate between devices, and connect to the Internet. For example, it can include vehicles, wearable devices, smart electricity meters, smart homes with automated devices such as lighting or heating, industrial systems and sensors, and devices such as digital video recorders and Internet-connected cameras.

⁵ A 'Distributed Denial of Service' (DDoS) is when a perpetrator attempts to make an online system unavailable by overwhelming it with traffic from multiple sources. The targeted machine, website, or network resource is flooded with superfluous requests, which overloads the system, forcing it to slow down or even crash and shut down, thereby denying service to legitimate users of the system.

- **responds to the clear upward trajectory of cyber security threats.** Cyber threat actors are increasingly bold, brazen and disruptive. New Zealand's geographical location does not exempt us from this threat. Digital technology provides new avenues for criminals and hostile actors to gain advantage. The widespread use of connected devices and emerging technologies has expanded the attack surface for malicious threat actors;
- **reflects the evolving and ongoing cyber security risk.** The Strategy is an opportunity for the Government to take the lead in responding to cyber risks, but also tackle the challenge as a nation. The Strategy will be anchored in effective risk management, so the actions we take should collectively reduce the risk for everyone; and
- is in line with the **intensified cyber security efforts of our Five Eyes partners, and other like-minded states.**


6. Progress on refreshing the Strategy and Action Plan

A three-stage, collaborative approach has been used to develop the Refresh.

Phase	Understand (May–June)	Develop (June–July)	Deliver (August–October)
Purpose	Research and analyse the possible vision, goals and principles (potential framework for the Strategy) to understand what's important for cyber-security in New Zealand.	Test the potential framework for the Strategy, and research, develop, and evaluate possible actions and initiatives to achieve the vision and goals.	Test and refine a draft refreshed Strategy and a small number of actions

Understand Phase

The Refresh has completed its initial 'Understand' phase. This involved researching and analysing a possible vision, principles and goals. In late June, workshops were held in Wellington (two), Auckland (two) and Christchurch with over 200 participants



from a diverse range of government, private sector and non-government organisations.

A variety of ideas was recorded, with key recurrent concepts emerging across the groups and workshops. These concepts included being: risk-based, people-centric, and collaborative, while also promoting trust and awareness.

Participants considered 2015 Strategy's goals to be largely relevant with appropriate areas of focus, and consistently suggested there is a need to be more ambitious in delivering on these goals.

Develop Phase

Following the workshops the government agencies collaborating on the Refresh pulled together the findings from the workshops and working groups. This 'Develop' stage of the Refresh has produced an initial draft strategy that integrates the findings of the workshops and working groups into a revised vision, principles and goals for the Strategy.

This draft Strategy formed the basis for a second stage of interagency work and external engagement activities that were conducted in late August in Auckland, Wellington and Christchurch with around 60 participants.

Following these engagements and further interagency work the draft Strategy has been revised to focus on the following four values and five priorities:

Values

- Partnerships are essential
- People are secure online
- Economic growth is enabled, and
- National security is upheld

Priorities

- Cyber security aware and active citizens
- Strong and capable cyber security workforce
- Resilient and responsive NZ
- Internationally Active
- Proactively tackle cybercrime

Deliver Phase

Officials are currently developing the draft Strategy for submission to the External Relations and Security Cabinet Committee in October. The draft Strategy will include:

- A narrative which articulates the Government's policy on cyber security, and why we need a refreshed Strategy – including addressing the evolving risk, and realising the opportunities of a connected world
- The values and principles underpinning the Strategy

- The five priority areas – and a description of what we want to achieve in each
- A small number of priority actions that will be taken to achieve Government objectives in the short term. These priority actions are being developed with a view that they will deliver a significant shift in New Zealand's cyber security posture.

Following Cabinet consideration of the Strategy, officials will develop an Action Plan to accompany the Strategy. The Action Plan will include further actions for the medium and longer term. This sequenced approach will enable further planning and work with relevant government and non-government stakeholders on specific initiatives. It will also allow ongoing alignment with the future Digital Strategy, the Living Standards framework and other relevant initiatives. s9(2)(g)(i), s9(2)(f)(iv)

s9(2)(g)(i), s9(2)(f)(iv)

We will shortly provide advice on the initial scope of potential priority actions and a substantive draft of the Refreshed Strategy. We would also like to discuss how we can best support you to move the Strategy through the Cabinet Committee process and as you consult with your Ministerial colleagues.

7. New Zealand's Cyber Security Strategy 2015 and Action Plan

New Zealand has an existing *Cyber Security Strategy* (the Strategy), *National Plan to Address Cybercrime*, and accompanying *Action Plan 2015*. These were approved by Cabinet in November 2015 [NSC-15-Min-0012]. The Strategy has provided the framework for coordinated cross-government efforts, in partnership with the private sector, to address cyber threats facing New Zealand.

The Strategy sets a **vision** of 'A Secure, Resilient and Prosperous Online New Zealand'. A range of government agencies contribute to each of the **four goals** of the Strategy (the goals are illustrated below).

The **Action Plan is a living document**, assessed annually as part of a strategic policy process. Flexibility has been built into the Action Plan to enable adaptation to the rapidly evolving threat environment and changes in technology. Actions can be dropped, amended or added, including to reflect lessons learned about what works and what does not.



8. Current Priorities

In addition to the refresh of the Cyber Security Strategy and Action Plan, there are a number of other issues on which we will brief you in more detail in the coming weeks.

This includes:

TICSA, 5G and network security

The *Telecommunications (Interception Capability and Security) Act (TICSA) 2013* provides a regulatory risk management framework to remove security risks from proposals for the design, build and operation of public telecommunication networks, including future 5G networks. The TICSA framework is vendor-neutral and country of origin-neutral, consistent with New Zealand's obligations under relevant international trade law. You have responsibility for the TICSA legislation as part of your communications portfolio, with MBIE leading on policy and the GCSB administering the network security provisions. The NCPO also plays a role in work on the regulatory and legislative consequences of TICSA as they relate to cyber security and national security issues.

The 5th generation of mobile technology is expected to bring significant advances in capability and functionality through: higher rates and volumes of data transmission, ultra-low latency, and high reliability. 5G networks are likely to result in a number of benefits and innovations (e.g. medical technology, precision agriculture, autonomous vehicles). To achieve these results, 5G networks have a very different

network architecture from traditional networks. This makes it difficult to provide assurance that security measures can mitigate the risks from a high-risk vendor providing products or services in a 5G network. Some vendors of telecommunications equipment are considered high risk, given their relationship with their domestic governments, and the likelihood that the vendor will be subject to extrajudicial directions from governments other than New Zealand's.

s6(a), s9(2)(g)(i), s9(2)(f)(iv)

s6(a), s9(2)(g)(i), s9(2)(f)(iv)

Work to consider accession to the Budapest Convention

The *Council of Europe Convention on Cybercrime* ("Budapest Convention") is the first international agreement on cybercrime. As of September 2018, the Convention's 59 State Parties include all of New Zealand's Five Eyes partners, other like-minded partners, and countries such as Tonga, Sri Lanka, and Nigeria. The Convention operates by standardising offences, providing powers and procedures for investigating offences, and improving processes for international cooperation amongst Convention parties on investigating cybercrime.

Work is underway to assess the requirements for accession to the Convention. Accession to the *Budapest Convention* was included in the *Action Plan* of New Zealand's *Cyber Security Strategy 2015* and the accompanying National Plan to Address Cybercrime. Accession to the Convention would allow operational agencies to better access and contribute to data flows on cybercrime; have significant reputational value for New Zealand; and enable New Zealand to better participate in mainstream international work on cybercrime.

The former Minister of Broadcasting, Communications and Digital Media, Minister of Justice and Minister of Police were recently briefed on the measures required to bring New Zealand's laws and investigative processes in line with the Convention and support this work going forward. We will provide you with a copy of this briefing.

A decision on whether New Zealand should formally express interest in acceding to the Convention would need to be made by Cabinet. Any Cabinet paper would be accompanied by a National Interest Analysis, which would set out the advantages and disadvantages of becoming a party to the Convention.

s6(a)


[REDACTED]

New Zealand Responses to Malicious Cyber Activities

New Zealand and its like-minded partners are working to test the range of capabilities and activities that would enable them to respond effectively to malicious cyber activities and to seek to deter perpetrators from commissioning further malicious activity of this type.

Public statements condemning malicious cyber activity are one important element of New Zealand's toolkit to respond to and deter such behaviour by other states. They demonstrate New Zealand will not tolerate malicious behaviour online and supports the international rules-based order. Joining other countries in public statements contributes to building and reinforcing norms for responsible state behaviour in cyberspace.

A number of Ministers, including the Prime Minister, Minister of Foreign Affairs, Minister Responsible for the GCSB, and you, are generally involved in decisions on responses to malicious cyber activity. Following such discussions, in February 2016, the Director-General of the GCSB joined international condemnation of the NotPetya campaign, noting that international partners have attributed NotPetya to Russia. In December 2017, the Director-General commented on the Wannacry ransomware campaign, noting that international partners had attributed responsibility to North



Korea. We will ensure you are briefed on any existing plans to call out malicious cyber activity.

Cyber security workforce

There is a worldwide shortage of cyber security workers, and this also affects New Zealand. To help address this, under the 2015 Strategy, a public-private Cyber Security Skills Taskforce was established to stimulate new initiatives, the most notable of which was establishing a Level 6 (sub-degree level) Diploma in Cyber Security. We will provide you with a detailed brief on workforce issues.

It is envisaged that a key part of the refreshed Strategy will be a workforce strategy outlining the nature of the problem and what further plans the government has to address it. This process has involved engaging with a wide range of stakeholders to understand the challenges facing the cyber security workforce.

Key ideas we have heard from stakeholders so far include: understanding supply and demand issues; building the participation of diverse groups in the workforce; and challenging the myths that cyber security workers adhere to a stereotype, cyber skills are the same thing as technical skills, and that there is only one pathway into a cyber security career.

9. The role of other government agencies

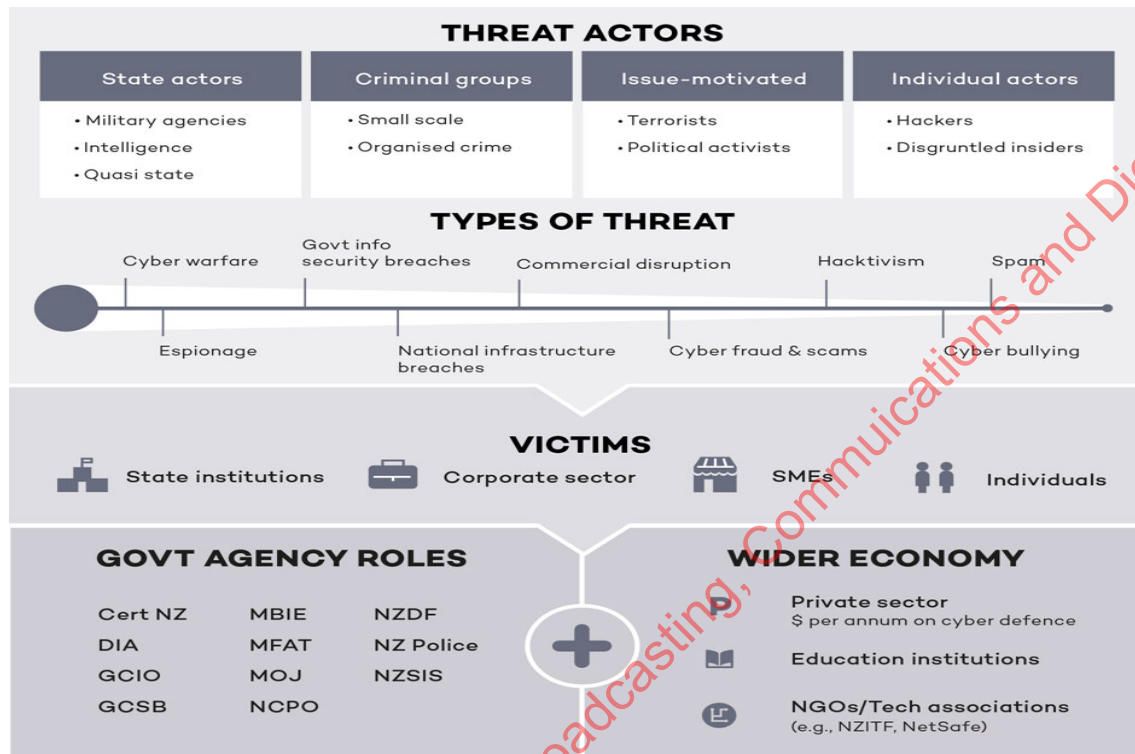
Cyber security issues intersect with the work of a wide range of other government agencies including in the areas of national security and intelligence, defence, international relations, trade and economic development, criminal justice, government digitalisation, and public service delivery:

- The **GCSB**, through the **National Cyber Security Centre (NCSC)**, responds to and mitigates cyber threats and provides defensive cyber threat services to public and private sector organisations of national significance. It delivers cyber threat intelligence to customers and partners. GCSB information assurance activities include providing high-grade encryption services to protect classified information and assessing proposed outer space and high altitude activity and changes to telecommunications networks for risks to national security. It also provides information assurance and security guidance to government agencies including through the Information Security Manual, which is an integral component of the Protective Security Requirements. The GCSB administers the network security provisions of the *Telecommunications (Interception Capability and Security) Act (TICSA) 2013*.
- The **New Zealand Security Intelligence Service (NZSIS)** delivers the Protective Security Requirements, which includes information security, for government agencies.

- 
- **New Zealand Police** addresses cybercrime (particularly through the Police Cybercrime Unit within the High Tech Group), which is one of the four goals of the *Cyber Security Strategy*.
 - The **Ministry of Justice** (MOJ) works on the rule of law and justice sector policy, including oversight of the *Harmful Digital Communications Act 2015* and the review of the *Privacy Act 1993* – the latter includes proposals on data breach reporting.
 - The **Ministry of Business, Innovation and Employment** (MBIE) links with cyber security in the areas of communications policy, the Digital Economy Work Programme, research and innovation, consumer advice, and support for small businesses. MBIE advises the Minister for Broadcasting, Communications and Digital Media (you) on the *Telecommunications (Interception Capability and Security) Act 2013*, which sets out the obligations of the communications industry in relation to legal interception and network security, and the *Unsolicited Electronic Messages Act 2007*.
 - **CERT NZ** receives reports of cyber incidents, analyses threats, shares information and advice, coordinates incident responses, and is a point of contact for the international CERT community. CERT NZ has been set up, initially, as a branded business unit within MBIE. CERT NZ runs the annual Cyber Smart Week promoting good cyber security practices to the wider community.
 - The **Department of Internal Affairs** (DIA) is the home of the Government Chief Digital Officer – the functional lead for the government's information communications technology strategy. The Department of Internal Affairs' Digital Safety team includes the Electronic Messaging Compliance Unit (the implementer and regulator of the *Unsolicited Electronic Messages Act 2007*, also known as the Anti-Spam team) and the Censorship Compliance Unit (which implements provisions of the *Films, Videos and Publications Classification Act 1993*, focussing on addressing online sexual exploitation of children, and violent extremism online).
 - The **Ministry of Foreign Affairs and Trade** (MFAT) works jointly with NCPO on cyber security diplomacy, including cyber security dialogues with other countries, advancing norms of state behaviour online, and addressing barriers to trade arising from other countries' cyber security regulations. International cooperation is one of the four goals of *New Zealand's Cyber Security Strategy*.
 - The **Ministry of Defence** (MOD) and the **New Zealand Defence Force** (NZDF) are focused on the cyber protection of the NZDF networks and deployed operations as well as the long term structure for raising, training and sustaining cyber capabilities. The *2018 Strategic Defence Policy Statement* indicated that to maintain relevant combat capabilities, the NZDF must be able to conduct a broader range of cyber operations. MOD and NZDF are working with NCPO on policy issues relating to the use of cyber operations in a military context.

This grouping of agencies, and how they fit into the wider cyber security landscape, is set out below.


The cyber security landscape



10. Conclusion

The many benefits of connectivity are today accompanied by increasing cybercrime and malicious cyber activity. In the face of this problem, effective cyber security policy and implementation really matters. It requires that we counter determined and well-equipped adversaries, coordinating across multiple organisations and sectors (not for nothing is cyber security often described as “a team sport”), adapting and changing often and at pace. Achieving this has proved challenging for New Zealand, as it has for all other governments. Along with our closest partners, we are working to catch up with and get ahead of a rapidly evolving, complex challenge.

Doing so is no longer a discretionary activity for governments (if it ever was). Good cyber security is critical to enabling New Zealand to realise the benefits of connectivity and digital innovation. Conversely, inability to address this challenge has the potential to compromise the security of New Zealanders and undermine our economic prospects. Our efforts need to be delivered while ensuring the benefits of connectivity are not impaired and that New Zealanders are equipped confidently to engage online with each other and the world.



We are working to intensify New Zealand's cyber security efforts, including through delivery of a refreshed Strategy and Action Plan. We look forward to engaging with, and supporting, you on this programme of work.

Proactively Released by the Minister of Broadcasting, Communications and Digital Media

Appendix A: Additional actions 2017-2020

Under the existing Action Plan, some actions have been completed (notably the establishment of CERT NZ), some actions are underway, some actions may need amending or updating, and we may need to consider new actions. The following sets out on-going actions and initiatives in the 2017-20 period under each of the four goals.



Goal 1: Cyber Resilience: New Zealand's information infrastructures can resist cyber threats and we have the tools to protect our national interests.

- **CERT NZ** was established in April 2017 with funding of \$22.2 million over four years [EGI-16-Min-0086]. In order to be set up quickly with organisational support, CERT NZ was established as a branded business unit within the Ministry of Business, Innovation and Employment (MBIE).
 - CERT NZ is currently funded for 7am to 7pm Monday-Friday operations. It has indicated that future consideration of 24/7 operations may be necessary, in response to public expectations.
- GCSB's National Cyber Security Centre has completed the roll-out of **Project CORTEX**, delivering malware detection and disruption services to a select group of public and private sector organisations of national importance. It is now working to scale the benefits of operating these services to a larger pool of nationally significant organisations through direct customer engagement and wider dissemination of threat reporting via a customer portal and information security exchanges.
 - The GCSB is developing a **Malware Free Networks initiative**, following a 12 month pilot as part of the CORTEX project. Cabinet approved the scaling of Malware Free Networks in March 2018. This is an important technical initiative with the prospect of significantly improving the protection of a broader set of organisations of national significance.
- A **major cyber security exercise** is planned in late October/late November to test the *Cyber Security Emergency Response Plan* (as part of the National Exercise Programme within the National Security System). The aim is to ensure that our response systems are effective and ready in the event of a major cyber incident which disrupts government organisations or other organisations of national significance.

- NCPO is working alongside the private sector-led Internet of Things Alliance to assess the security challenges arising from evolving technology, such as the **Internet of Things (IoT)**. We will work with you as we consider how to address the security challenges of the IoT and other emerging technologies.



Goal 2: Cyber Capability: New Zealanders, businesses and government agencies understand cyber threats and have the capability to protect themselves.

- Small businesses play a huge role in New Zealand's economic growth – but often do not have the skills or resources to protect their business information and remain cyber secure. We have developed a business model for a **Cyber Credentials scheme to assist small businesses** and have selected private sector providers to deliver this programme.
- There is a shortage of **cyber security professional expertise in the workforce**, which means that businesses and organisations do not have the technical staff to carry out cyber security improvements. A Cyber Security Skills Taskforce (nine private sector and education sector representatives) was set up in November 2016 to take practical actions to address this shortage.
 - A new Level 6 cyber security qualification will be launched for uptake in 2018.
 - Work is underway on other initiatives to expand the cyber security skills pipeline to the workforce. We will seek your advice on priorities and next steps.
- Protective Security Requirements (PSR), incorporating information security, are mandated for 35 government agencies. At a system level, following two years of assurance reporting, there has been strong capability improvements in personnel and physical security – s6(a) [redacted] A process is underway to improve the settings for government information security. s9(2)(f)(iv), s9(2)(g)(i) [redacted]
- A **trans-Tasman cyber security research alliance** with Australia, with the goal of jointly-funding cyber research projects in a way which lifts New Zealand's research capability, leverages off Australia's cyber security

research expertise, and helps seed new research into the cyber security ecosystem, was announced by Australia and New Zealand Prime Ministers in February 2018.




Goal 3: Addressing Cybercrime: New Zealand improves its ability to prevent, investigate and respond to cybercrime.

- There is a talented Cybercrime Unit within NZ Police's High-Tech Group – s6(c) [REDACTED]
- **International cooperation between law enforcement agencies** is essential for responding to cybercrime. NZ Police is active in the Five Eyes Law Enforcement Group. s9(2)(f)(iv), s9(2)(g)(i) [REDACTED] there would be value in considering NZ Police representation in key international cybercrime units such as the European Cybercrime Centre within Europol and the International Cybercrime Coordination Cell within the Federal Bureau of Investigation.
- With your support we will continue to work closely with NZ Police on their prioritisation of resources for addressing cybercrime, s9(2)(f)(iv), s9(2)(g)(i) [REDACTED] and to work with the Ministry of Justice on considering accession to the Budapest Convention – which will require Cabinet consideration.



Goal 4: International Cooperation: New Zealand protects and advances its interests on cyberspace issues internationally.

- International work ensures New Zealand is able to advance its interest in a free, open and secure cyberspace; participate in the growing international debate about cyber security threats; and promote norms of acceptable state behaviour online. We foresee an increasingly fractious environment for this work, given recent developments. We may need to step up our effort in this area, working in conjunction with MFAT and other agencies. We will identify opportunities for you to participate in international cyber security events, and



support you to engage on cyber security issues during your international travel and meetings with foreign counterparts.

- New Zealand engages regularly with **'Five Eyes' partners** at the policy, intelligence, CERT, law enforcement and defence levels.
- We have close connections with **Australia** on cyber security. Prime Ministers have committed to cyber security cooperation in their Annual Joint Statements.

s6(a)



- The second New Zealand-**China** cyber security dialogue was held in September 2017. The dialogue builds bilateral policy and operational relationships s6(a)



We will continue to work with Chinese officials regarding China's new cyber security and cross-border data transfer regulations which affect New Zealand businesses.

- Further work is required to enable New Zealand exporters to meet increasingly onerous 'behind the border' cyber security requirements, as states and sector groups seek to regulate for security outcomes.