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

Briefing to Incoming Minister for the Digital Economy and Communications

Date	2/11/2020
Priority	Routine
Security classification	Restricted

New Zealand Government

Introduction

Welcome to your role as Minister for the Digital Economy and Communications. Part of your portfolio includes responsibility for cyber security policy. This responsibility is allocated from the Prime Minister's National Security and Intelligence portfolio.

This briefing sets out:

- your roles and responsibilities, the context of the portfolio, and how the Department of the Prime Minister and Cabinet (DPMC) can support you; and
- key areas of focus requiring consideration either immediately or within the next 100 days.

Cyber security is fundamental to New Zealand's national security and economic growth. Virtually everything now has some connection to the internet, and this connection is becoming increasingly important – for commerce, education, and government, but also social connections. As information is increasingly accessible online, New Zealanders are increasingly exposed to malicious cyber activity.

It is important to protect the confidentiality, integrity, and availability of New Zealand's data, systems, and networks, and to ensure systems are resilient. Cyber security allows these systems to keep running, keeps our personal and commercial information safe, and allows us to trust the information that we use to make decisions. COVID 19, and requirement to work and learn remotely, underscores the centrality of digital technology to New Zealand's future prosperity.

Cyber security threats continue to grow in number and complexity, and this will be fuelled by an increase in connected devices and emerging technologies, such as 5G. New Zealand continues to be affected by increasingly sophisticated cyber security 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.

Cyber security is not a 'problem' that government can fix on its own. Solutions require a multi-stakeholder approach, including the private sector, educational institutions, and civil society. But the Government has a leadership role to play in keeping New Zealand safe. This includes maintaining strong cyber security over our own networks, protecting citizens from serious cyber threats arising from criminal or nation state actors that no individual or organisation can mitigate on its own, and informing and promoting cyber security best practices to ensure individuals and organisations are getting the basics right to protect themselves.

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

Recommendation

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

1 **Note** the contents of this briefing.

NOTED

Tony Lynch
Deputy Chief Executive
Department of the Prime Minister and Cabinet

Date: / / 2020

Hon Dr David Clark
Minister for the Digital Economy and Communications

Date: / / 2020

Your roles and responsibilities

Ministerial responsibility for cyber security policy

The Minister for National Security and Intelligence has overall responsibility for national security policy. Part of this portfolio includes cyber security policy, which has been allocated to you. This includes:

- oversight, ongoing development and coordination of New Zealand's Cyber Security Strategy and associated work programme; and
- policy development related to:
    - the national security implications of digital technologies including new and emerging technologies and applications of technologies, for example, 5G, artificial intelligence, and encryption;
    - growing the size and capability of the cyber security workforce in New Zealand;
    - incentivising the growth of the cyber security industry in New Zealand;
    - the cyber resilience of New Zealand businesses and critical infrastructure providers;
    - s6(a) [redacted]
    - the national security implications of cybercrime; and
    - New Zealand's international engagement on cyber security policy issues, in consultation with the Minister of Foreign Affairs.

Other Ministers involved in cyber security issues

On cyber security, you will work closely with the:

- Minister for National Security and Intelligence (the Prime Minister);
- Minister responsible for the Government Communications Security Bureau (GCSB);
- Minister responsible for the New Zealand Security Intelligence Service (NZSIS); and
- Minister of Foreign Affairs.

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;
- Minister for Small Business; and
- Minister for Economic and Regional Development.

The nature of the digital and cyber security environment means that some issues can cross a number of portfolios (for example, resilience, encryption, and public attribution of cyber attacks). [redacted] s9(2)(f)(iv) [redacted]

Further information on Ministerial and government agency roles can be found in **Attachment A**.

We are here to support you

The National Cyber Policy Office (NCPO)

Established in 2012, NCPO formally reports to you on cyber security policy matters, consulting with other Ministers as appropriate. NCPO sits in the National Security Policy Directorate within DPMC's National Security Group. We would be happy to brief you on the work of the National Security Group.

NCPO leads the development of cyber security policy advice for the government and advises the government on its investment of resources in cyber security activities. This includes developing and coordinating implementation of cyber security strategies. NCPO oversees the implementation of the current New Zealand Cyber Security Strategy 2019.

NCPO conducts international engagement (working with the Ministry of Foreign Affairs and Trade and others) and works closely with counterpart policy teams in Australia, Canada, the United Kingdom, the United States, and other like-minded countries.

NCPO, along with the Cyber Coordinator (see below), also conducts outreach with the private sector and civil society on cyber security policy issues.

DPMC provides a part-time Private Secretary to support your cyber security policy work.

Cyber Security Strategy Coordination Committee

The Deputy Chief Executive National Security chairs a monthly inter-agency Cyber Security Strategy Coordination Committee (CSSCC). This committee governs the annual work programme to implement the Strategy, ensures initiatives are aligned and any gaps identified, and assesses the overall direction of New Zealand's cyber security ecosystem.

Committee members include representatives from DPMC, Crown Law, Department of Internal Affairs, Government Communications Security Bureau, Ministry of Business, Innovation and Employment, Ministry of Defence, Ministry of Foreign Affairs and Trade, Ministry of Justice, New Zealand Defence Force, and New Zealand Police.

Cyber Coordinator

A core institutional element of the Cyber Security Strategy 2019 (see below) was the establishment of a specialist Cyber Coordinator function. The Cyber Coordinator is also the Prime Minister's Special Representative on Cyber and Digital. This role enables senior-level engagement with the technology sector in New Zealand and overseas to address digital challenges. The main responsibilities of the role are to:

- build and maintain relationships with the key players in the domestic and international technology industry;
- represent New Zealand perspectives on key technology issues, with a particular focus on safety and security;
- work towards, and enable solutions to, challenges posed by new technologies, in a collaborative, multi-stakeholder manner;
- assist in coordination across the many New Zealand agencies working on these issues; and
- support agencies in developing policy advice and advancing operational solutions.

Cyber Security Strategy 2019

New Zealand's latest Cyber Security Strategy was released in 2019. Its vision is that "New Zealand is confident and secure in the digital world". The Strategy takes an all-of-New Zealand approach to cyber security, in recognition that cyber risks are pervasive and, although the government has a significant role to play, it cannot address these risks alone.

Budget 2019 allocated $2 million per year over four years to implement the Strategy. A work programme is prepared annually.

There are five priority areas in the Strategy, each with a set of actions to improve New Zealand's cyber security. The priorities are:

1. Cyber security aware and active citizens;
2. Strong and capable cyber security workforce and ecosystem;
3. Internationally active;
4. Resilient and responsive New Zealand; and
5. Proactively tackle cybercrime.

These priorities inform the annual work programme.

Immediate priorities and decisions

Key decisions you will need to take in the first 100 days are:

- the direction of the 2020/21 work programme to implement the Cyber Security Strategy; and
- presenting advice to Cabinet (with the Minister of Justice) on acceding to the Council of Europe Convention on Cybercrime. An earlier decision by the then-Cabinet directed this occur by the end of 2020.

Annual work programme

When the Cyber Security Strategy was finalised in 2019, the Cabinet Economic Development Committee invited the Minister of Broadcasting, Communications and Digital Media to report back to Cabinet with a work programme to implement the Strategy. The report back to Cabinet identified several priority actions, including:

- s9(2)(f)(iv) ;
- s9(2)(f)(iv) ;
- s9(2)(f)(iv) ;
- s9(2)(f)(iv) ;
- s9(2)(f)(iv)
- s9(2)(f)(iv)

s9(2)(f)(iv)

s9(2)(f)(iv)

Council of Europe Convention on Cybercrime

One of the Strategy's priorities is proactively to tackle cybercrime. As part of this, NCPO is currently working with the Ministry of Justice to provide advice on accession to the Council of Europe Convention on Cybercrime (the Budapest Convention). The Budapest Convention aims to prevent, deter, and detect crimes committed via the internet and other computer networks. Accession is a priority in the Cyber Security Strategy 2019, and a key deliverable of the countering violent extremism work programme developed in response to the terror attack in Christchurch in 2019.

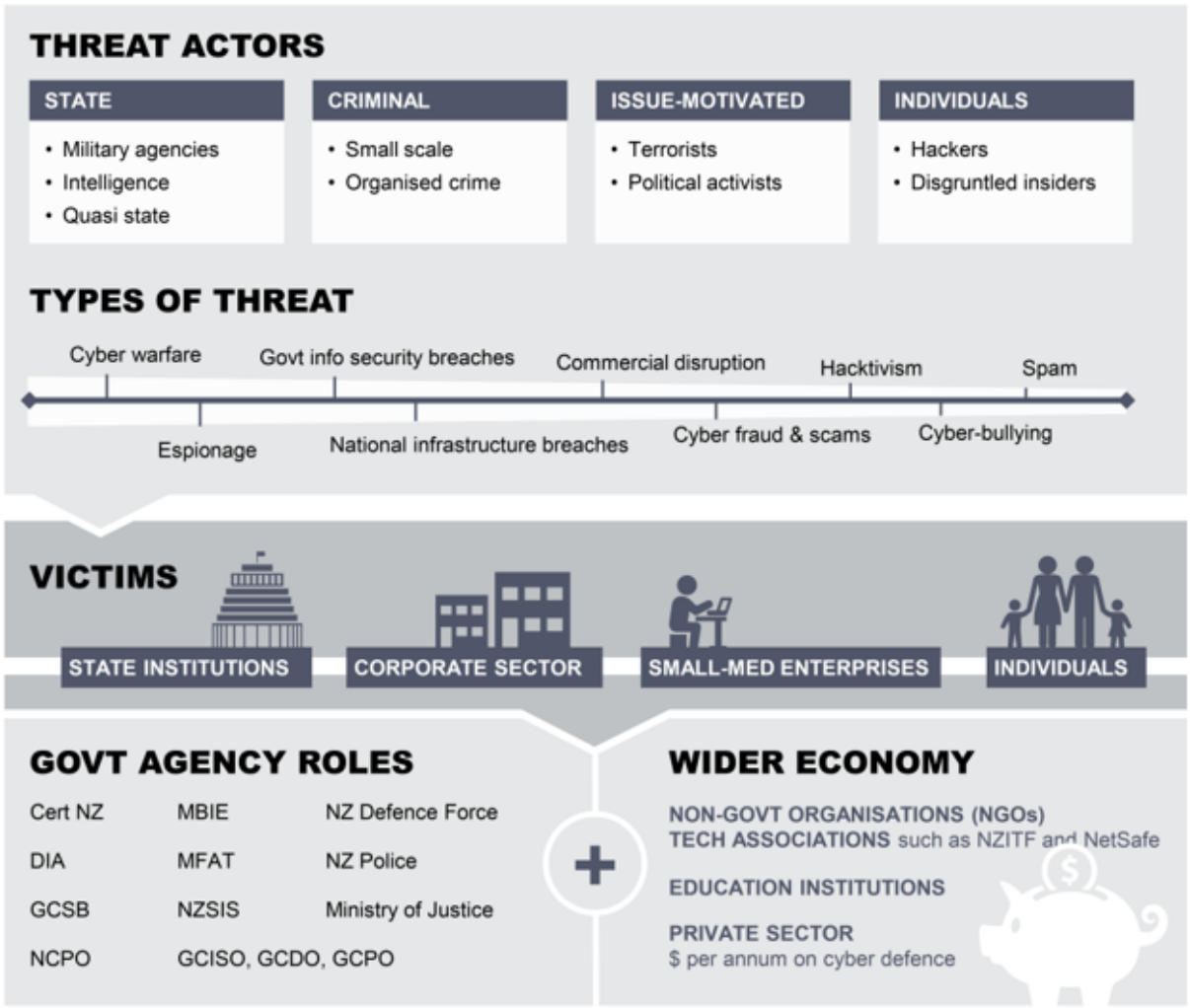
Accession would:

- complement existing mutual assistance laws, boosting capacity for international cooperation to deal with increasingly sophisticated and diverse forms of computer-related criminal activity;
- have significant reputational value for New Zealand; and
- enable New Zealand to better participate in mainstream international work on cybercrime.

In June 2020, the then-Cabinet agreed 'in principle' to accede to the Budapest Convention subject to further consultation and detailed advice on legislative changes required for, and financial implications of accession. An eight-week public consultation period closed in September. This included targeted consultation with Māori, civil society, and the telecommunications and data storage industry. Officials are now completing analysis of the submissions and will provide you with a briefing summarising the responses received during the consultation. A draft Cabinet paper and National Interest Analysis are under development.

Attachment A: Role of other Ministers and agencies

The diagram below provides a brief overview of the cyber security landscape.



Three Ministerial portfolios currently have direct policy responsibility for cyber security matters:

- The **Minister for National Security and Intelligence** has overarching responsibility for the national security and intelligence system and setting the overall policy for that system.
- Responsibility for CERT NZ and cyber security policy matters within the National Security and Intelligence portfolio are delegated to the **Minister for the Digital Economy and Communications**.
- The **Minister responsible for the GCSB** has responsibility for the oversight of the GCSB and its cyber security functions, as set out in the Intelligence and Security Act 2017.

There are a number of agencies that do work which touches on these three Ministerial portfolios:

- **DPMC**, through the National Security Group, leads advice on matters for national security for the: Prime Minister (who is the Minister for National Security and Intelligence); the Minister for the Digital Economy and Communications (on matters associated with cyber security policy through the NCPO); the Minister responsible for the New Zealand Security Intelligence Service; and the Minister responsible for the Government Communications Security Bureau (in the context of the Intelligence and Security Act 2017). DPMC provides advice on the Intelligence and Security Act 2017. DPMC also leads on advice for the Five Country Ministerial meeting, attended by the Minister of Justice, which often includes cyber security related topics.

- The **Government Communications Security Bureau** (GCSB), through the **National Cyber Security Centre** (NCSC), provides cyber security services, including raising cyber resilience through threat reporting, advice and guidance; incident response capabilities and support to major events; the provision of detection and disruption services to consenting organisations. The focus of the NCSC is on nationally significant organisations, or where there is a risk of high national impact.

- The Director-General GCSB is the **Government Chief Information Security Officer** (GCISO) and is the functional lead for information security across government. Along with the GCISO functional leadership, the GCSB maintains the New Zealand Information Security Manual, which is a mandatory component of the Protective Security Requirements for agencies. The GCSB also has a regulatory function, administering the network security provisions of the Telecommunications (Interception Capability and Security) Act 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.

- The **Department of Internal Affairs** Chief Executive is the Government Chief Digital Officer (GCDO). This digital functional/system role is responsible for implementing the Strategy for a Digital Public Service, with a focus on trusted digital government and using all of government contracts to build a more secure digital system. DIA also implements the Unsolicited Electronic Messages Act 2007 and the Films, Videos and Publications Classification Act 1993. The latter focusses on addressing online sexual exploitation of children, and violent extremism online.

- The **Ministry of Justice** works on the rule of law and justice sector policy, including oversight of the Harmful Digital Communications Act 2015 and the Privacy Act 1993.

- The **Ministry of Business, Innovation and Employment** (MBIE) has 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 the Digital Economy and Communications (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 is a branded business unit within MBIE.

- The **Ministry of Foreign Affairs and Trade** 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.

- The **Ministry of Defence** 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.