**Speaking Notes**

**Presentation to the Transparency International New Zealand Board**

**13 February 2017**

# The role of Government in protecting New Zealand's important information

Andrew Hampton, Director, GCSB

Kia ora koutou

Thank you for the invitation to talk with you today and address the question of who looks after New Zealand's cyber defence, and to provide some background and context to the work of the Bureau.

Helping protect New Zealand's significant information and information systems is a key part of the role of the GCSB, and I welcome the opportunity to talk with you today about that.

I will also take the opportunity to talk more broadly about the functions of the Bureau and how we ensure we work in the best interests of New Zealand and New Zealanders.

## Our objectives and functions

GCSB is a New Zealand public service organisation. We are accountable to the Government of New Zealand and act in the interests of New Zealand and New Zealanders. While the nature of our work is sensitive, and often classified, it is important that we are as transparent as possible and that the public are confident that we are operating within our mandate and the law.

Everything we do needs to be in accordance with New Zealand law, our international human rights obligations, and we are subject to a high level of independent oversight and scrutiny.

Our legislation specifies three objectives for the Bureau:

- National security of New Zealand
- International relations and wellbeing of New Zealand, and
- Economic wellbeing of New Zealand

In fulfilling its objectives, GCSB has three functions.

We collect and report on foreign intelligence in accordance with Government's National Intelligence Priorities. By finding out about the interests, intentions and capabilities of foreign parties we help inform Ministers and government decisions.

We provide cyber security and information assurance services to organisations of national significance, both public and private sector. This includes:

- The National Cyber Security Centre – located in the GCSB,
- The CORTEX programme, which uses cyber threat information – including inputs from our international partners - to help protect public and private sector organisations, and
- Our regulatory role under the Telecommunications Interception Capability and Security Act to ensure national security risks are not introduced into telecommunications networks.
- All our cyber security services are provided with the consent of the organisations involved.

And, thirdly, we assist Defence Forces, New Zealand Police and New Zealand Security Intelligence Service (NZSIS) to undertake their lawful functions. This includes counter terrorism and support to military operations. In 2015/16 there were seven instances of us providing assistance to the NZSIS, and two to the New Zealand Defence Force.

In order to perform these functions we can exercise some intrusive, but warranted or authorised, powers on behalf of the State. It is therefore important that we are as transparent as possible about the nature of the threats New Zealand faces, our role in countering them, and how we are held accountable.

Importantly we are not an enforcement agency, we provide intelligence to others to inform their decisions.

Nor do we set our own priorities; these are set by Government and everything we do needs to be in accordance with these priorities.

A summary of the Bureau's activities for 2015/16 can be found in our annual report (link to GCSB external website).

## Authorisation and oversight

As I've mentioned, everything we to do to deliver our three functions needs to be in accordance with New Zealand Law and our international human rights obligations To ensure this, there is a strong authorising and warranting regime in our legislation. This involves a responsible minister and an independent commission of warrants – currently a retired Court of Appeal Judge. They need to be satisfied that what we are seeking to do is legal, necessary, reasonable and proportionate. There is also clear internal policy which guides the delivery of our intelligence and cyber security functions.

We are also subject to rigorous independent oversight which includes:

- A dedicated parliamentary oversight committee
- An Inspector-General of Intelligence and Security – with Commission of Inquiry powers

Our activities are also subject to the Ombudsman, the Privacy Commissioner, and the Auditor General. I suggest that we, and the NZSIS, are subject to more rigorous oversight than any other government agency.

And, we are meeting our obligations.

The Inspector General of Intelligence and Security has reported that GCSB has a strong culture of commitment to legal compliance and certified our systems and processes as compliant for the past two years.

Staff are also able to make protected disclosures directly to the Inspector General of Intelligence and Security if they have concerns about the Bureau's activities.

## Public scrutiny

There is a range of commentary about the role of the Bureau, and our functions and capabilities. The fact that anyone can make comment about what we do and how we do it is an important part of an effective democracy – however there are times when this commentary stretches beyond informed comment and into the realm of myth and misconception. I would like to take this opportunity to briefly address some of the most common of these "myths".

*First up, that the GCSB is part of a shadowy intelligence sharing partnership called the Five Eyes.*

That's actually true. It's just not that shadowy. To be effective, intelligence agencies do need to undertake much of their activity in secret. However, the fact that New Zealand is part of the Five Eyes and derives significant benefit from it is on our website!

As the Cullen/Reddy report states, for each foreign intelligence report the GCSB produces we get ninety-nine from our partners.

As with all of our activities, any sharing of intelligence with partners needs to be in accordance with New Zealand law and our international human rights obligations.

*That leads to the next common myth about the GCSB, that we are a law unto ourselves.*

I have to say, it doesn't feel like that when I am meeting with Ministers two or three times most weeks, seeking their authorisation and briefing them. I have been struck by the strong culture of legal compliance in the Bureau and the steps that are taken to ensure everything we do is properly authorised.

*Another common myth is that the GCSB is staffed by "Cold War Warriors", stuck in the past.*

Most of the GCSB senior team are in their 30s and 40s. The Berlin Wall was long down before most of us started working. I'm also pleased to report that over 50 percent of our managers are women, a high proportion of our staff are from the private sector, and we attract some of the brightest new graduates in the country.

*The most common myth is that the GCSB is engaging in the "mass surveillance" of New Zealanders; that we are actively monitoring the phone calls, the emails and the internet traffic of large sections of the population.*

I can assure you, we aren't. The GCSB does not have the legal authority, the capacity or the interest to undertake such activity. But don't take just my word for it. Dame Patsy Reddy, Sir Michael Cullen and the Inspector-General of Intelligence and Security have all concluded that the GCSB does not do this.

## Cyber threats

I know that you have previously discussed the issue of cyber security and hacking. I have already touched briefly on the role of the Bureau and our National Cyber Security Centre (NCSC) in this regard.

New Zealand's prosperity and our way of life is built on us being an open and democratic nation, with the free flow of people, trade and information across our border. Yet with that connectedness comes new threats, often as a consequence of the huge growth of the Internet which is changing the way we live and work, and I'd say was never designed with security in mind.

Whereas in the past we could rely on our geographic remoteness to keep us and our information safe, our information and potentially our infrastructures are now open to threats in real time from anywhere in the world.

We will soon be releasing a report which provides an overview of the cyber threats recorded by the NCSC over the past year. These are threats which directly impact New Zealanders and New Zealand organisations.

Not only is the level of threat increasing – our NCSC recorded 338 cyber incidents in the 2015/16 year, compared with 190 in the previous year, the nature of the threats are becoming more complex and the sources of them more diverse.

In a typical month GCSB:

- detects through CORTEX seven cyber intrusions affecting one or more New Zealand organisations. For context: roughly 0.5% of internet traffic analysed by GCSB under CORTEX has a ‘signature’ of advanced malware associated with it; and each month about 900 new signatures of this type are identified either here in New Zealand or by our Five Eyes partners.
- we receive 12 new incident reports which are unrelated to CORTEX monitoring. The incidents in this case are typically self-reported by the organisation dealing with them, and
- we receive five requests for some other form of concrete cyber security assistance.

Over the last 12 months the requests have been as much from private sector firms as government agencies. The organisations in question have included financial institutions, ISPs and tertiary institutions.

The fact that we are increasingly being asked for our advice and input this reinforces the reality that cyber threats are very real, and that New Zealand’s relative geographic isolation offers no protection in our globally interconnected connected world.

### Cyber Defence

In part the increase in recorded incidents reflects increased detection of threat activity by our cyber defensive capabilities, particularly CORTEX.

CORTEX is a project to counter cyber threats to organisations of national significance – e.g. to operators of critical national infrastructure.

There is information about CORTEX and our information assurance functions on our website for those of you who would like to find out more, including the privacy impact assessment.

It involves GCSB implementing capabilities to protect these organisations against advanced malicious software ('malware'). In some cases malware is passively detected. In others it is actively disrupted or 'blocked'.

In terms of the types of incidents we are seeing, phishing – often clever, socially engineered email intended to make the recipient open an attachment or visit a website which contains a malicious file, and ransomware - which involves your files or systems being locked down until you pay a ransom - are some of common types of harm being reported to us or being detected by our capabilities.

Late last year we released details of the pilot of a cyber defensive initiative called - Malware-Free Networks. This involves GCSB trialling sharing of cyber threat information and technology with an Internet Service Provider (ISP) enabling them to mitigate malware that is targeting a small subset of its customers.

This kind of cooperation between the public and private sector organisations is an important part of our national strategy for increasing New Zealand's cyber resilience.

**My priorities**

I have spent some time talking about our functions, priorities as an organisation and how we go about delivering them.

I would like to finish by touching on my own priorities as a (still) relatively new Director of the GCSB.

My focus in in five key areas:

- Implementation of the new legislation which is currently going through Parliament,

- Continuing to build public trust and confidence – being more open and accessible through engagements like this is one of the factors which can contribute to this,

- Increasing the Bureau's effectiveness by working better with others, both internally and externally,

- Involving the customers of our cyber security, information assurance and intelligence products more in how we design, deliver and evaluate services, and

- Developing our people and their capabilities – with additional investment from Government comes the need to grow our people, both in number and building their capabilities. This also creates opportunities broaden the diversity of our staff so we can better reflect the community we serve and bringing a greater range of perspectives to our decision-making.

Thank you again for the opportunity to come and talk with you this afternoon, I look forward to taking your questions.

END