GOVERNMENT
COMMUNICATIONS
SECURITY BUREAU
TE TIRA TIAKI

Speaking Notes for Speech to the New Zealand Institute of Intelligence Professionals by Una Jagose, Acting Director, Government Communications Security Bureau

Friday 27 November 2015

Auckland

40 min + Q&A

[Thanks etc].

I am Una Jagose, the Acting Director of the Government Communications Security Bureau. I started at the GCSB in late February this year, coming from my role as Deputy Solicitor-General, Crown Legal Risk at the Crown Law Office. I'll be in this role until the beginning of February 2016.

I thoroughly enjoy this role: the GCSB, and the New Zealand Intelligence Community, is a great place to be working. Our people are fantastic. I have learnt a lot, and I can say that the work we do is vitally important to New Zealand.

Today, I will be talking about cyber security and GCSB's role in that. But I also want to take the opportunity to do a bit of "myth-busting" about the GCSB – what we do and what we don't do. I know you're all intelligence professionals, but there might be different levels of insight into GCSB, so I want to make some things clear from the outset.

The week I started in the Bureau, a new wave of media attention started, alleging things about the Bureau's work, based on stolen, classified and misinterpreted documents.

There was also some underlying truth. It was alleged through the media that the Bureau may conduct surveillance in foreign countries, and may assist in counter-terrorism work. It should not come as a surprise to anyone that New Zealand's foreign intelligence organisation ... collects foreign intelligence; the statute that we operate under tells you as much. As does our website.

To be clear, our three functions are:

- Gathering and analysing foreign intelligence in accordance with the Government's requirements about the capabilities, intentions, and activities of foreign persons and foreign organisations;
- Information assurance and defending and protecting critical information infrastructures (our cyber security role, which I am going to talk about a bit later); and
- Assisting other agencies (Defence, Police and the NZ Security Intelligence Service)

Of course it's not so "newsworthy" to talk about the great work we do, the value we provide, or the extraordinary people we have who do cool things to deliver high quality cyber defence and foreign intelligence for the Government of the day – our statutory functions.

It also seems to be forgotten that the GCSB is a government department, delivering on the Government's priorities, answerable to Ministers, and subject to significantly more independent oversight than most agencies (appropriately so).

I agree that there are legitimate questions to be asked about our intelligence gathering activities. But there is also a risk of doing real harm to New Zealand's interests if the way those questions are attempted to be answered is by simply revealing selective details from stolen – and classified – documents, trying to interpret technical intelligence-speak from them, trying to draw threads about what is going on, and blithely publishing documents without context. Why? Because that approach could reveal to adversaries what our targets or capabilities are, or are not – and, accordingly, what our vulnerabilities are.

If the question was put, who benefits from those sorts of allegations and that sort of coverage .. the answer would not be New Zealand and New Zealanders. Anyone, and everyone but.

That would make us vulnerable to those who do not have New Zealand's best interests at heart – and I'm sure you all understand better than many that they are not imaginary!

We, New Zealand, have interests we want to protect and secrets others want to steal. And we want New Zealand to be able to flourish and prosper.

I do acknowledge that we – the GCSB - can be better at being more open with the public. We see the benefits in increasing the public understanding, and therefore the mandate, for what we do in protecting New Zealand and our interests.

And we are talking about this more, with interest groups like this one, politicians and the general public via media and our website (which we are continuing to work on).

But there can be a real tension here because complete openness with New Zealanders is also openness to adversaries; and that weakens, rather than strengthens, New Zealand interests.

We do not think that we can simply assert that we need to operate in secrecy and all will be well. I don't think any of us can. The public wants and expects openness from its Government.

So, what do we do about that?

The tension has to be managed in a way that provides appropriate levels of security to allow for both effective, legislatively-mandated intelligence operations (and therefore protection of New Zealanders and our interests) and public assurance (of lawfulness, of understanding and adequate protection of rights).

I think that a significant answer to these inherent tensions lies in the system itself. It lies in the legislative controls and external, independent oversight of the intelligence agencies. That oversight is crucial for assuring the New Zealand public that our security agencies are acting properly.

Mass surveillance is a term that has been bandied about by people critical of our agencies. It is not a term that we use ... it is a myth. It creates an image of random information collection, without purpose, without control, and then the conspiracy theorists use that as the basis for allegations about rights to privacy. We do not simply randomly hoover up information and rummage through it, hoping to find something useful. It's simply not true.

The truth is quite the opposite: where our foreign intelligence work requires access to infrastructures that would otherwise be unlawful, it is conducted under Ministerial warrant or authorisation.

The GCSB Act sets out how the system works: the reason for the access or intercept must fit within the Government's requirements, and be justified. The Minister responsible must receive an application that sets out the reasons why the particular access is sought, how the proposed outcome justifies the access or intercept, whether the outcome can be achieved another way. The Minister must be satisfied that there are controls put in place to make sure that the Bureau only does with the information that which is needed for its proper performance. Overall the process is about ensuring that the access is lawful, reasonable and proportionate.

These are high hurdles. In addition, the Minister of Foreign Affairs must be consulted before any authorisation is granted, and the Minister responsible may impose any conditions he or she thinks fit. The Commissioner of Security Warrants – a former Court of Appeal judge – must also agree if a New Zealander's communications are to be targeted (New Zealanders' personal communications are not to be targeted, but there are exceptions if a New Zealander is, in the words of the Act, "an agent of a foreign power or foreign organisation").

There are built in internal checks and authorisations, and compliance training and exams, required before information can be accessed, and all accesses are fully auditable.

None of these steps is taken lightly. Furthermore, in the time I have been at GCSB I have been impressed at the internal oversight exercised day-to-day by the leadership team. My observation is that everyone involved takes very seriously the intrusive powers we exercise. We have a strong system of compliance within the Bureau to add to the independent oversight of our activities outside of the Bureau.

One of the most significant and independent forms of oversight is the Office of the Inspector-General of Intelligence and Security (the IGIS – we love our acronyms).

The IGIS oversees the work done in the Bureau (and the NZSIS). All our work – including everything to do with warrants and authorisations - is available to the Inspector-General at any time and it must be fully auditable. She has direct access to the building, to the systems, and to us.

The IGIS conducts audits, reviews and regular inquiries, and reports to Ministers and, as we have seen, to the public. The IGIS can initiate inquiries herself or based on a complaint from the public. Members of my staff can make complaints directly to her and have full protection from any employment consequences if they do so. She has full inquiry powers to examine people under oath, to call for and see any relevant material.

In the last few weeks, the IGIS has released her annual report for 2013/14 and certified the GCSB's compliance systems as sound. We have come a long way since the Kitteridge Review into compliance which was released in 2013 (a little before we were ready for that release).

As GCSB is a government department, the Privacy Commissioner, the Ombudsman and the Auditor-General also have oversight roles. And, finally, the Intelligence and Security Committee, a parliamentary committee, has an important role in holding the agencies to account for what they do. I. Along with the NZSIS Director, will be appearing before the Intelligence and Security Committee, in public, in the next few weeks.

So, that tension I mentioned: it is managed here, in this system of control and oversight. We cannot be entirely transparent to the public about what we do. But we must be – and we are - utterly open with the oversight bodies. Their reports on us are intended to reassure the public that what goes on is lawful and done with New Zealand's interests at heart.

This process of warrants and authorisations, and internal and external oversight that I've outlined – it simply does not allow for such wide-ranging, uncontrolled conduct such as "mass surveillance". And, what's more, it also doesn't allow us to just listen in on people's private communications!

Oversight is very important and we welcome it. It is necessary for a credible and resilient security and intelligence service for New Zealand. It is the platform for a strong public mandate that I intend to continue building in my time as Acting Director.

I've been impressed with the people at the Bureau. As I'm sure you're aware, there is thorough vetting before people can work for us: aside from comprehensive psychological tests, people undergo reviews of their financial background, what they do in their spare time, personal relationships, online habits, any other habits ... it is a very intrusive process. That's the level of commitment our people have to their work. Our people have very high levels of integrity and loyalty. They share a real sense of the burden and the privilege of the material they work with, and the importance of what they do, day to day. No doubt you have that too.

As I mentioned earlier, one of our core activities is cyber security, and this is one area that we've recently become more open about and that I want to elaborate more on today.

The Bureau's cyber security mission, conducted by our National Cyber Security Centre, is to ensure the protection, security, and integrity of communications and information infrastructures of importance to the Government of New Zealand. This includes identifying and responding to cyber threats or potential cyber threats.

So what are these threats?

Threat stems from the rapidly changing nature of the internet, which was not designed with security in mind. The more we are connected to, and holding data on, internet facing systems, the greater our vulnerability to attack. The scale and pace of growth is almost unimaginable, and it means vulnerabilities are constantly being introduced, protected against, then reinvented and rediscovered; and on it goes.

Connectivity to the internet is everywhere: crossing national and international boundaries and time zones, and allowing previously disparate groups to connect.

A couple of years ago there were as many internet connected devices in the world as there were people. Current growth trends point to there being three times as many internet devices as there are people in the world by 2017. Nearly 2 billion people use the internet as preferred means of communication.

It's a scale that offers massive opportunities, both for those who have good intentions, and those who do not.

On the not-so-good side, the trend is moving from just simply stealing data to manipulating or destroying it. For example, the much publicised Sony hack. And more recently the United States Office of Personnel Management (OPM) security clearance computer system database of personal information relating to military and security officials was inhabited by hackers. Millions of US government workers' private details were taken. And the hack was not discovered for more than a year, giving the adversary ample time to steal as much information as it wanted.

In the New Zealand context:

- In the 12 months to 31 December 2014 there were 147 incidents recorded by our National Cyber Security Centre.
- In the first six months of 2015 we had already recorded 132 incidents and expect that by the end of 2015 this figure will be in excess of 200.
- Of the incidents recorded so far in 2015, 79 were reported by government agencies and 33 by private sector organisations.
- A further 20 incidents were reported to us by our cyber security partners where the nature of the organisation was not identified.

These incidents range in seriousness from the targeting of small businesses with "ransomware" and attempts to obtain credit card information through to serious and persistent attempts to compromise the information systems of significant New Zealand organisations.

Some of these threats come from well-resourced, foreign adversaries. While at times they are directly targeting significant New Zealand organisations, we are also seeing them use (and attempt to use) New Zealand based systems as a "jumping off point" to host malware that is used to target overseas networks.

Part of our response to the more sophisticated and advanced types of these threats is the CORTEX project that you might have heard about.

CORTEX's sole purpose is to counter cyber threats to organisations of national significance. Those organisations are chosen because of their significance to New Zealand – both public and private sector – through criteria determined by Government, independently of the Bureau.

Included are government departments, key economic generators, niche exporters, research institutions and operators of critical national infrastructure.

We do not talk about which organisations are receiving CORTEX protection. Doing so may disclose where New Zealand's most valuable information is held and allow more focused attention from cyber-attacks.

Through CORTEX the Bureau is developing technical capabilities to both detect and disrupt malware in order to protect those selected organisations.

There is a double gate authorisation for CORTEX capabilities being provided to organisations:

1. First, the capability must be authorised by the Minister, and the Commissioner of Security Warrants, under the GCSB Act.
2. But, also, the organisation obtaining the CORTEX capability must consent to receiving it – and agree to a number of conditions (for example, each recipient must conduct the highest level of basic cyber-hygiene, advise those who interact with their computer systems (staff, customers) that their communications may be accessed for cyber security purposes, and maintain confidentiality about the services it is receiving).

So, what does CORTEX deliver?

We provide a range of protections, including:

- an ability to detect threats to networks, and to tell protected organisations about those threats so that they can respond to them;
- targeted advice from our experts about the prevention and mitigation of advanced and other cyber threats (we share what we learn from specific instances with a wider pool);
- an ability to identify vulnerabilities in computer systems and networks that advanced threats might exploit; and
- an ability to actively block advanced malware directly.

Usually it involves a layered set of technical capabilities– layering provides better coverage and is more likely to detect sophisticated malware that might be able to avoid detection at some levels.

Organisations may receive just one layer, or several layers of capability.

CORTEX is not about replicating existing defences used by organisations but is focused on countering foreign-sourced malware that is particularly advanced in terms of technical sophistication and/or persistence. This type of malware is not adequately mitigated by commercially available tools.

So, how does CORTEX work?

At the heart of the capabilities is the detection of advanced malware. Detection mainly occurs through automated means – i.e. machines looking for indicators of malicious activity using information about previous successful or attempted cyber-attacks.

In some cases the capabilities also involve 'active defence'. This involves putting in place systems that can identify and disrupt sophisticated cyber threats in near real-time. These systems are given 'signatures' – patterns of data that identify particular, known threats – for them to use to distinguish between benign and malicious internet traffic. When malicious internet traffic is identified by its signature, the system prevents it from reaching its destination.

Roughly 0.5 % of the data analysed through GCSB's CORTEX capabilities has a signature associated with some form of cyber threat.

Each month the GCSB and our international cyber security partners identify around 900 new signatures. Where possible this information is used to assist others to avoid the threat and help identify the source of the threat – although attribution can be a very complex matter to determine, and our focus is really on defending systems regardless of where the threat comes from.

In some cases (so far our experience tells us that is less than 0.005% of the total data analysed), a human GCSB analyst would need to review the data when the machine analysis throws up malicious cyber activity that it is unable to resolve – perhaps because it's a new form of attack.

Just as in our foreign intelligence work, technology assists in ensuring oversight of the CORTEX capabilities for compliance with the law and with the specific terms of the authorisation, and to provide reassurance that the capabilities are being used for their authorised purpose and nothing else.

The system itself provides strong and comprehensive oversight of the use of CORTEX data. The data is categorised according to how it should be handled, and the rules about what can (or cannot) be done with it.

These rules specifically limit the number of our people who can access the data, all of them cyber defence specialists, with a clear understanding of the rules.

And of course the IGIS is able to view it all – including a complete log of what occurred, the reasons for any activity taken, and what was done with the data.

The CORTEX capability is only used for cyber security.

And it's going really well.

In the first 10 weeks of 2015, we resolved more cyber security incidents than we did in all of 2014. We think it's more likely that that's not because of an increase in the volume of incidents so much as our improved capacity to identify and resolve incidents promptly.

Some recent examples of what we have seen or been involved in responding to include:

- The targeting of several officials from a key government agency through email and web site exploits in an effort to gain access to personal information and potentially compromise the agency's network. This attack was detected and mitigated before important information could be lost or compromised.
- The use of a malware package to target six significant New Zealand organisations. The threat was detected and mitigated through systems and support provided via our CORTEX capabilities.
- These capabilities also helped us identify and trace the source of a new cyber- attack method from a known major foreign threat source. The attack targeted several CORTEX customers. The "signatures" of this new cyber-attack were able to be passed on to our international partners, helping to reduce global vulnerability to this particular attack.

We have also helped:

- an Auckland firm whose computer network was attacked by an overseas-based criminal group
- a major IT firm resolve a long-term compromise
- a telecommunications provider respond and strengthen their systems after seeing suspicious, overseas-sourced activity on their network
- private sector organisations suffering ransomware and denial of service attacks.

New Zealand government and private sector entities are targets and victims of malicious actors. We cannot be complacent about it.

Some incidents require our assistance, others can be resolved with some advice, and others again are managed by the entities themselves when they are aware of what's going on in their systems.

GCSB typically does not currently provide direct assistance to smaller businesses or to individuals; however, we may assist with evaluation of cyber incidents if they fit within our authorisation criteria.

We do provide the information we learn – declassified and at appropriate levels of generality – in advisories available on the NCSC website and other information sharing forums such as the Security Information Exchanges (SIEs) that we facilitate. SIEs are where sectors or industries meet as a group and discuss relevant cyber threats and mitigations, and all benefit from sharing information.

A recent Vodafone report tells us that 56% of NZ businesses reported a cyber-attack in past year. 45% of them self-report that they have inadequate tools and policies to face cyber threats.

Cyber security is something we all have to be aware of. It is not just a technical issue. We advise that cyber security should be approached as an enterprise wide issue.

I want to share with you some of the advice that we give to organisations and the public in general. Perhaps it will be of use to you and your organisation, or you can share it with friends and family – spread the cyber security word!

We tell organisations to not believe that they don't have anything of value or underestimate what information is of value. Data is valuable. Customers certainly think so, especially information about themselves.

We live in a global data economy and data can be stolen, changed, improperly used or even combined with other data sets to create commoditised information with commercial value.

New Zealand's geographical isolation traditionally has meant we are safer from some of the risks we see overseas – we cannot rely on this when it comes to cyber threats in particular. Connectivity to the internet knows no geographic boundaries, and, accordingly, there is global vulnerability.

We've also been advising organisations to not take a risk avoidance position. This is only successful if you can be sure to have better defence than every potential attack, and that's not likely. It is better to have a risk acceptance strategy: mitigate the risks and prepare resilience to those risks being realised at some point.

We also encourage organisations to see information security through a lens of people, places and systems:

- The people risk: an insider threat can be as damaging as a cyber-attack. And people can also be the cause of vulnerability – whether deliberately or by failing to follow security protocols.
- The places risk: premises need to be secure to prevent physical access. What are your organisation's boundaries? You have to think of them as more than the physical reaches of your organisation. What is the reach of your information and data sets? That's the boundary. Now think again: are you sure that boundary is secure?
- Following that, the systems risk is probably obvious, and doubtless your IT team or specialist can assure you of security of those systems. But have organisations considered outsourced IT service providers:
    - What are their security arrangements?
    - Is their resilience regularly tested?

Contracting out service delivery or responsibility won't prevent cyber-attacks.

We ask organisations to think of their information as a supply chain – from start to finish. It's only as secure as the weakest link in that chain. And are you or your organisation creating vulnerabilities for others?

The secret to cyber security is that the basics matter – but they are not as commonly implemented as you would think. Most cyber-attacks succeed because the basics aren't followed. Even though there are some adversaries who have access to the most sophisticated cyber-attack capabilities, they will always try the obvious first. After all, what burglar doesn't try for an unlocked window first, even if they can hack through your household security system?

So what are the basics? Our Australian counterpart ASD [Australian Signals Directorate] has some good mitigation strategies on its website. The top four are:

1. Patching systems and applications as patches become available
2. Ensuring people don't bring their own software to work, i.e. white-listing – only allowing approved software to run
3. Limiting administrator privileges
4. Strong control of passwords.

If this is something you're interested in, you can find out more at ncsc.govt.nz or google "catch, patch, match" for ASD's site and the comprehensive advice.

These basic actions provide a very solid basis for building and maintaining more secure systems and networks. The serious, high end, sophisticated threats to significant New Zealand entities and infrastructures require a more complex response, and CORTEX is an important part of that. I am looking forward to seeing CORTEX develop and provide even more benefits to New Zealand.

I hope today you are more informed about the role and functions of the Bureau, along with the important cyber security challenges we all face. This is part of our efforts to talk more openly about what we do, and attract the best people to come and work with us, share our knowledge and learnings ... and hopefully use that expertise for the greater good of New Zealand if and when they move on into organisations like yours.

So I want to finish by saying that GCSB, and the core NZIC, is a great, exciting place to work. Consider perhaps spending some time working in the NZIC. Or do you have staff that would benefit from such exposure and development? It’s not about us trying to poach – you’d bring new skills in and learn others to take back. The bigger and deeper the pool of intelligence expertise in New Zealand, the better for New Zealand.

Thank you very much for your time. I am happy to take a few questions.