OFFICE OF THE INSPECTOR-GENERAL OF INTELLIGENCE AND SECURITY

Cheryl Gwyn – Inspector-General of Intelligence and Security

Speaking notes for Women in International Security (WIIS)

30 November 2015

Thank you for the invitation to speak to you this evening.

I would like to talk about some of the challenges for intelligence and security oversight in what is an increasingly complex environment, but first I thought it might help to tell you a little bit about my role and the work that my office does. Everything that I am going to cover is information already in the public domain.

ROLE OF THE INSPECTOR-GENERAL OF INTELLIGENCE AND SECURITY

In New Zealand, as in other jurisdictions, the framework of oversight for the intelligence and security agencies has a number of elements and layers. Here, it includes the Directors of the agencies, the responsible Minister, the Ministry for National Security and Intelligence, the Commissioner of Security Warrants, the Intelligence and Security Committee and, more generally, the Auditor-General, Privacy Commissioner and Ombudsmen.

The principal external oversight body is my office, the Office of the Inspector-General of Intelligence and Security.

The role of the Inspector-General was significantly strengthened in late 2013. Previously the Inspector-General had to be a retired Judge. He (my predecessors were all men)

worked part-time; they had no investigating staff. Under the amendments it became a fulltime role, not confined to former Judges, and the powers and resources of the office now more closely match the mandate.

I think the agencies may sometimes feel that my office is a vehicle for public criticism of what they do – they perhaps think that I'm out to "ping" them and tell the world about it.

In fact the role of the Inspector-General under the Inspector-General of Intelligence and Security Act 1996, is to "assist the Minister" to ensure that each of the New Zealand Security Intelligence Service (NZSIS) and the Government Communications Security Bureau (GCSB) complies with the law. (I don't have jurisdiction over any other government agencies even if they have intelligence and security functions.) To that extent I have a common purpose with the agencies – to ensure they act lawfully and properly.

But I also see it as my role to shed as much light as possible on what the agencies actually do. It's important that the public understand the powers and activities of the intelligence agencies – and the limitations and controls on those powers – and see independent oversight working in practice.

While it's not for me to increase public confidence in the agencies, I would hope that over time, if the public sees that there is robust oversight and that the agencies respond to criticisms and recommendations, then public confidence will increase.

As well as assisting the Minister, I'm also required by the IGIS Act to independently investigate complaints.

In practice my staff and I:

- Review all of the GCSB interception warrants and access authorisations and all NZSIS domestic and foreign intelligence warrants, including the new visual

surveillance warrants and any authorisations by the Director of Security for urgent surveillance without a warrant (under the new powers, introduced under urgency late 2014). We select some of those warrants and authorisations for deeper analysis – a comprehensive check of the process and path by which the application for the warrant was formulated, from the feasibility paper, ie what was the intelligence case, to the application for the warrant signed by the Minister (and Commissioner of Security Warrants where required), through to review and cancellation/non-renewal or renewal of the warrant, and what intelligence was collected under it.

Our role is primarily *ex post facto* – that is, after particular operations have concluded. The underlying rationale is that oversight bodies should review, but not direct or approve in advance, the management and operational decisions of the intelligence services. This approach does not preclude the agencies briefing me on planned or ongoing operations. Although it is not my role to approve operations in advance, there are situations where prior discussion with my office can help to ensure clarity about the legality and propriety of any planned activity.

- Investigate complaints from members of the public and from current or past employees of the NZSIS and GCSB. Complainants must show they have been or may be "adversely affected" by any act, omission, practice, policy or procedure of the GCSB or NZSIS. We receive a range of complaints – from complaints about the outcome of the NZSIS security clearance vetting process; complaints of surveillance or interception of communication by the agencies. A current example of the last of these is from New Zealanders who were living/working/on holiday in the South Pacific at the time that the Snowden documents suggest that GCSB was intercepting electronic communications.

- Initiate my own inquiries into any matter that relates to GCSB and NZSIS's compliance with the law or into the propriety of particular activities they are engaged in. "Propriety" isn't defined in the legislation but is clearly intended to have a broader reach than pure legality. A current example of an own-motion

inquiry is one into the allegations that the GCSB misused its powers to assist Trade Minister Tim Groser in his bid to become Director-General of the WTO.

- Review the SIS and GCSB systems (including carrying out unscheduled audits). For example, we have just completed a review of how the NZSIS holds, uses and audits access to, the repository of hugely personal and sensitive information about people that it collects when it is "vetting" them for a security clearance (health, financial, political, sexual, etc).

- "Certify", on an annual basis, whether the agencies' compliance systems are "sound".

In order to be able to effectively do these things, my staff and I have a right of access to the Bureau and SIS's premises (including the GCSB's H/F radio interception and direction-finding station at Tangimoana and the satellite communications interception station at Waihopai); their ICT systems, documents and employees.

The flip side of that privileged access is that we are subject to the same constraints on holding and using classified information as GCSB and SIS staff. My staff and I must all be security cleared to the highest level. We work in a SCIF (secure compartmented information facility) and follow the same security measures as agency employees.

Maintaining security and being bound by the rules around classified information does sometimes make it difficult to report publicly on issues as fully as I would like. I have asked the Directors of both agencies for their full cooperation to assist me in making as much information public as possible when I come to report on the various inquiries into their agencies.

When I'm carrying out an inquiry I have powers similar to those of a Royal Commission: I can compel the production of documents and information, issue notices to attend before me to answer questions and to give evidence under oath or affirmation. My proceedings, reports and findings are challengeable only for lack of jurisdiction.

I have recommendatory powers only, in the same way that the Ombudsman does. To date, I don't think that is a problem.

THE CHALLENGES IN AN INCREASINGLY COMPLEX ENVIRONMENT

I'd like to touch on three issues that I see as posing a challenge to effective oversight:

- "the accountability deficit" that arises from increased intelligence sharing and cooperation across borders
- the rise in terrorist activity and consequent calls for greater powers for the agencies
- technological change

Intelligence and security agency cooperation

Cooperation between selected western states in certain areas of intelligence operations (particularly signals intelligence) is longstanding. However, since 9/11 there has been a significant increase in the scope and scale of intelligence cooperation.

The collaboration has increased both in terms of the volume of information shared and the number of joint operations. The scope of cooperation has broadened to include a greater range of states and a wider variety of intelligence activity.

The UKUSA arrangement – the Five Eyes: USA, UK, Canada, Australia, NZ – is the most public example of transnational intelligence collection and distribution through international intelligence sharing arrangements.

Broader and deeper cooperation between intelligence and security agencies represents a growing challenge to accountability. International information-sharing arrangements vitiate completely privacy requirements and generally elude intelligence oversight.

I spoke recently at an international Data Protection conference and I was reminded of the extent to which privacy regulation is conducted on a national basis, creating an uneven pattern of privacy laws, some more demanding than others. Likewise, national intelligence oversight and review structures were designed for a different era and are, in the main, ill-equipped to deal with intelligence cooperation across borders. Cooperation between intelligence and security agencies has not been matched by cooperation between national oversight and review bodies.

This increasing accountability deficit presents perhaps the most significant oversight challenge in the field of national security today[1].

National oversight of intelligence cooperation

The extent to which national oversight bodies can cooperate, share information, perhaps even carry out joint inquiries, is seriously limited. In some jurisdictions, the legislation governing oversight bodies specifically prevents such cooperation. In others – such as New Zealand – the issue is not specifically addressed in the oversight legislation. I would argue it is implicit in my powers that I can look at how the agencies for which I have oversight responsibility share information and resources, including with foreign partners, but the principle of "the third party rule" or "originator control" (ORCON), which shields information supplied to an agency by intelligence partners in other countries from attribution, has the potential to impede such oversight. The rule stipulates that information shared with a foreign intelligence service or government should not be transmitted to third parties (domestic or foreign) without the prior permission of the service which originally shared the information.

The prohibition on the further dissemination of information is widely interpreted as applying to the recipient services' oversight, considered to be third parties. The practical

---

[1] Born, Leigh and Wills, *International Intelligence Cooperation and Accountability* (Routledge, 2011) is a very useful resource on this topic.

consequence is that oversight bodies may be precluded from accessing large volumes of information and correspondence held by intelligence services.

The third party rule is reflected in New Zealand, as in some other jurisdictions, in the freedom of information legislation, here the Official Information Act (OIA) (s 6).

Such restrictions make it difficult, if not impossible, to scrutinise what foreign agencies do with intelligence provided by our national agencies. Who has access to that intelligence? what controls are there on that access? is it used only for lawful purposes? Similarly it is difficult or impossible for the national service to assess whether the intelligence it receives from foreign partners was collected lawfully.

What can be changed at a national level? The process and responsibility for the authorisation of all intelligence cooperation agreements and activities should be more clearly articulated in national laws. We can seek statutory requirement for cooperation agreements to be sanctioned by the executive government, whether generally or specifically.

Intelligence services could be legally obliged to share cooperation agreements with their oversight bodies (as in Canada)[2] and/or the agencies could be required to brief oversight bodies on particular types of intelligence cooperation activities.

It may be that national oversight bodies can – subject to the possible constraints already mentioned - initiate inquiries into the cooperation of agencies with foreign services. By way of example, my Dutch colleagues have two investigations underway into the cooperation of the Dutch intelligence and security services with foreign services.[3]

---

[2] Canadian Security Intelligence Service Act 1985, s 17(2).

[3] Review Committee on the Intelligence and Security Services, Annual Report 2014/15, p 17.

International oversight

International accountability is also under-developed. Hardly surprisingly, states have not to date agreed to international oversight of their national intelligence agencies and seem unlikely to do so.

International monitoring institutions struggle to fill the gap, for example at the United Nations, European Union and Council of Europe levels.

There are rare examples of international organisations conducting inquiries into aspects of international intelligence cooperation: the inquiries conducted in 2006-2007 by the European Parliament (EP) and the Parliamentary Assembly of the Council of Europe (PACE) into the secret detention and unlawful transfer of suspected terrorists on European territory.

International accountability could take the form of either or both of an international body or networking and cooperation between national oversight bodies. The recently appointed UN Special Rapporteur on the Right to Privacy will certainly have a role, given his extensive mandate, and his stated focus on surveillance oversight.

As to oversight cooperation, to date, national investigations have built on each other, rather than being coordinated across jurisdictions. For example, my office is currently undertaking an inquiry which entails an analysis of the GCSB's bulk data collection capability. My work is assisted by, eg from the United Kingdom, the Intelligence and Security Committee's report,[4] the RUSI report,[5] the report from David Anderson QC, the UK Independent Reviewer of Terrorism Legislation;[6] and from the USA, the Privacy and Civil Liberties Oversight Board report on s 702 of the Foreign Intelligence Surveillance Act

---

[4] Intelligence and Security Committee of Parliament, *Privacy and Security: A modern and transparent legal framework*, March 2013.

[5] The Royal United Services Institute, *A Democratic Licence to Operate - Report of the Independent Surveillance Review* (July 2015).

[6] *A Question of Trust – Report of the Investigatory Powers Review*, June 2015,

and the United States National Research Council report to the President on technical options regarding bulk collection.[7]

Similarly, my office is currently undertaking an inquiry into whether the New Zealand intelligence and security agencies had knowledge of/cooperated with the Central Intelligence Agency (CIA's) programme of detention and interrogation, including torture, as detailed in the US Senate Committee on Intelligence report released in December 2014. Although my inquiry was precipitated by the Senate Committee report, I am assisted by the inquiries into the same or similar issues already undertaken in other jurisdictions such as the United Kingdom. (As I have said publicly, my decision to commence an own motion inquiry does not suggest or presuppose that NZ agencies or personnel were in any way connected with the CIA activities).

Inquiry reports from oversight bodies in other jurisdictions are useful at a number of levels – they may provide an explanation of technical processes which are largely universal; a published description of operational activities in one jurisdiction reduces the ability of agencies in other jurisdictions to deny or decline to comment or to try to prevent the oversight body from publicly describing the same or similar activities.

These kinds of public reports are forcefully negotiated, with the oversight/review bodies pushing the agencies to make as much information public as possible, rather than assert that it must remain classified for security reasons. That is essential to maintaining public confidence.

---

[7] United States National Research Council *Bulk Collection of Signals Intelligence: Technical Options* (2015), defining (at S1) "bulk collection" as any collection of communications signals where "a significant portion of the data collected is not associated with current targets" and concluding at S6-S7 that "[t]here is no software technique that will fully substitute for bulk collection", but that there was scope for better targeting and better automatic access controls.

International cooperation

There is however a case for more conscious collaborative oversight of different countries whose intelligence agencies are working closely together.

Craig Forcese, a Canadian academic, advocates what he calls "borderless review"[8]: that is, parallel investigations, undertaken by oversight bodies in two or more states to examine in a given case the role of their respective services. That however would likely require some form of international agreement between participating institutions, to provide the legal framework for such cooperation. In some jurisdictions that may be prevented by current national legislation.

Counterterrorism focus – call for new powers

The second "challenge" to effective oversight that I want to mention arises from the increase in terrorist activity and the consequent increased emphasis of the agencies on counterterrorism. In the wake of events such as the *Charlie Hebdo* shootings in January this year and the ISIS murders in Paris in November, it's not surprising that the call – from intelligence and security agencies around the world, not just those in France - almost immediately becomes "we need more powers". For example, in the US and the UK the agencies have renewed their calls for technology companies like Apple and Google to have to build backdoors into their devices and software to make it possible for intelligence and security and law enforcement agencies to decode decrypted messages the companies' customers send and receive.

Yet it is generally acknowledged that all three perpetrators of the *Charlie Hebdo* massacre were "known" to French authorities and, likewise, the problem in stopping the Paris attacks was not a lack of data, but a failure to act on information the authorities already had. It wasn't, as some have suggested, a result of the terrorists using sophisticated encryption technology.

---

[8] Born, Leigh and Wills ibid n 1, chapter 4.

In Canada, Bill C-51, now the Anti-terrorism Act 2015, highlighted another issue – the call for security agencies to have powers that potentially cross the line between intelligence and law enforcement. The Canadian Security Intelligence Service (CSIS) now has more power to disrupt suspected terrorist plots, rather than just collecting information about them. If they have reasonable grounds to think a terrorist threat exists, CSIS can now, eg interfere with travel plans and bank transactions of suspected terrorists.

The challenge for legislators – and for the public – is to ask the question that logically comes prior to a consideration of new powers: what is the effectiveness, or lack thereof, of the agencies' existing powers? It must be convincingly demonstrated that new powers are necessary because the current powers are insufficient.

Further, any new powers must be commensurate with the scale and resources of the agencies, to ensure that they can properly utilise such powers.

While it's not my role to comment on current or proposed government policy, I think that oversight bodies have some legitimate role in informing the debate on proposals to amend the legislation that governs the intelligence and security agencies.

All the oversight in the world can't compensate for poor legislation. As Sir Michael Cullen and Dame Patsy Reddy carry out their review of the New Zealand intelligence and security agencies, their legislation and the oversight legislation, it's useful to look at "*A Question of Trust",*[9] where David Anderson said:

> *"Each intrusive power must be shown to be necessary, clearly spelled out in law, limited in accordance with human rights standards and subject to demanding and visible safeguards."*

---

[9] Ibid, n 6.

As the Anderson report recommends, a transparent legal framework should include:[10]

- the types of data collection measures undertaken by intelligence agencies [I'll come back to this question of the need for clarity around exactly what it is the agencies do]
- who can exercise them
- what the objectives are
- who might be subject to them
- the threshold and procedure for justifying their use
- the duration of the warrant or authorisation
- the procedures regarding retention, deletion and disclosure of data
- sharing parameters
- oversight and review procedures.

Technological developments

A third challenge is coping with technological changes. Developing technologies pose challenges not just for the agencies themselves but also for effective oversight.

The Anderson report devotes a whole chapter to technology. He points out that any new law must be couched in technology-neutral language, but those who make and enforce the law – and those who have oversight responsibility – must have some understanding of the relevant technology.

Chapter 4 of the report is an interesting survey of relevant technologies – compiled entirely from open-source material. I've touched on encryption – front doors and back

[10] "*A Question of Trust*" is in large part the basis for the new Investigatory Powers Bill just introduced into the UK Parliament. The IP Bill aims to consolidate and update all of the current legislation covering the UK intelligence and security agencies.

doors, but there is also, eg IMSI catchers or grabbers [devices which intercept signals between a mobile phone and a mobile phone base station, by mimicking the mobile phone base station), and equipment interference/computer network exploitation (CNE)/ hacking, as it's more usually known. CNE was first acknowledged – "avowed" – by the UK government only early this year. Similarly the use of s 94 of the Telecommunications Act 1984 (UK) for the bulk collection of communications data for the use of the intelligence agencies, was avowed for the first time simultaneously with the announcement of the IP Bill.

I understand that the avowals were seen as necessary by the UK government so that when Members of Parliament come to debate the proper scope of investigatory powers they are fully informed as to the scope of the powers currently used. At a time when many governments around the world are in the process of, or considering legislative change, this is an important message.

Effective oversight of the agencies' use of new technologies requires at least a basic understanding of those technologies by the oversight body, whether through the knowledge and expertise of our own staff or by access to external technical experts, so that we can assess that they are used within the scope of the relevant legal framework. In practice, for my office it's mainly a combination of reliance on agency experts to explain and our own (growing) knowledge. While the agencies – particularly the technical experts within the GCSB - are very generous with their time, it's important for our credibility and our ability to ask the necessary searching questions, that we acquire our own knowledge and expertise.

We also need to be able to explain these technical issues to the public - in so far as we able to do so consistent with national security requirements. A significant challenge for us is how we provide enough detail, framed in lay language, about what the agencies are doing to make it meaningful to the public. In a way, that in itself is a particular challenge of oversight in today's environment.

A "gendered" approach

Finally and briefly, my invitation to speak suggested that I might consider talking about whether there is merit or utility in a "gendered" approach to understanding intelligence and security issues. I confess I have not given the question enough considered thought, but there are some useful statistics that can help to get the discussion started.

The GCSB has 36% female and 64% male employees. In the NZSIS women comprise 40.5% and four of the nine roles in the NZSIS Senior Leadership team were held by women.[11] Of course, both Directors are women. This compares to the public sector average in NZ, in 2014, of 59% female and 41% male employees.

I don't have statistics for the New Zealand Defence Force or for the intelligence roles within the Department of the Prime Minister and Cabinet. In the IGIS office, of a total of seven, including IGIS and DIGIS, we have five women and two men.

Nor do I have statistics for racial and ethnic diversity in the intelligence agencies, though I strongly suspect that they are much worse even than the proportions of women.

The UK Intelligence and Security Committee of Parliament published a report in March 2015[12] (following a study led by the Rt Hon Hazel Blears MP, who was then a member of the Committee) on the position of women in MI5, MI6 and GCHQ. The report considered recruitment policy and practice; maternity-related issues, childcare and flexible working hours; career and promotion prospects; and cultural and behavioural issues.

Women currently comprise 37% of the workforce of the three UK intelligence agencies – compared to 53% for the UK Civil Service as a whole. They also comprise disproportionately more of the workforce at junior grades: on average across the three agencies women make up only 19% of the Senior Civil Service.

---

[11] Those statistics are taken from each organisation's Annual Report as at 30 June 2014.

[12] Intelligence and Security Committee of Parliament, *Women in the UK Intelligence Community*, March 2015.

The former US Secretary of State, Madeleine Albright, who conducted a similar investigation examining women in the CIA, commented on the UK report:

> "…diversity should be pursued – not just on legal or ethical grounds, important as these are in their own right – but because it will result in a better response to the range of threats that threaten national security."

The Chief Justice, Dame Sian Elias, said in her 2009 Dame Silvia Cartwright lecture to the Auckland Women Lawyers' Association: "… we need diversity on the bench and in all places where public authority is exercised … the effect of such representation is not only the visibility of difference. The life experiences of women and minorities are very different to the life experiences of the men who were judges when I [the Chief Justice] started in legal practice and who are still disproportionately represented on the bench. Elizabeth Evatt, the Australian Judge, thought that women and minority judges are more likely to realise how often claimed objectivity is marred by unconscious biases."

I'd be interested to know your views on whether and how greater diversity in the intelligence and security agencies would result in a better response to the range of threats to national security.

CONCLUSION

Thank you again for the opportunity to talk to you. I'm happy to answer any questions.