

Speech given by Director to Hutt Valley Chamber of Commerce
Evening of Monday, 1 December 1997
Invited by Michael Ramanos by letter

INTRODUCTION

Thank you for your welcome. As you have noted this is the first time that I have spoken to such a business group, although I have spoken to other Service organisations in the Wellington/Hutt Valley area.

The NZSIS was established over 40 years ago in 1956, at the time of the Cold War, and it has continued to operate in an environment of constant change. During that time not much has been known about us, largely because we declined to comment on matters of national security. If we did get publicity it was often unfavourable - our successes are seldom acknowledged but it seems our problems always are! That is the nature of our responsibilities and even today I will have to protect detailed information about the SIS in the interests of national security.

As a consequence the Service has developed a reputation as a secretive and even a slightly "spooky" organisation which lives in the past, and watches New Zealanders in a slightly intrusive way. Today I hope to provide a level of insight into our business which raise your level of understanding and confidence in who we are, what we do, and why we do it.

As I have mentioned there is a further perception that we never answer questions. It seemed to me therefore that the best approach today would be to pose myself the questions most often asked about the SIS BUT on this occasion to go further by actually answering them. So, to coin a phrase, its off with the trench coat and dark glasses and here we go with the first question.

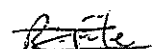
1. **WHY DOES NEW ZEALAND NEED A SECURITY SERVICE, APART FROM ANYTHING ELSE, DOESN'T IT CONTRAVENE OUR HUMAN RIGHTS ANYWAY?**

My answer, put simply, is that we need a security service because, even today in New Zealand, we do face very real threats to our security. The Security Intelligence Service is a fundamental and important part in the basic framework which has been set in place by Government to properly protect our democratic institutions. I hope that after my 20 minutes or so, I might have convinced you of this proposition.

As for the second part of that question about our human rights, I am not a lawyer and so I venture into the complex topic of human rights with some trepidation. Nevertheless let me comment briefly on the legal basis for the Service.

- International convention accepts that a democratic state has a right to protect itself using such mechanisms as Police, Defence and Security Services which are properly described in the law of the land. It also accepts that in certain circumstances they may have pre-eminence over some individual freedoms. It is also a well accepted principle that exceptions to Human Rights provisions should themselves be established in law.

- For us, that necessary law is in place. The NZSIS Act 1969 (one of the earliest in the Western World) and amendments in 1977 and 1996 describe not just our functions and how we will perform them, but also the limitations which are to be applied to our activities. For example, in our most intrusive activity, the exercise of an interception warrant, the value of the



Information must justify the interception or seizure of a communication and must not be likely to be obtainable by any other means. Those tests, to which I must attest in a sworn affidavit, are rigidly applied.

Last year further limitations were passed into law stating that:

.. "...it shall not be the function of the Service to further the interests of any political party";

In this case the new law confirmed an already existing practice. Furthermore, to preserve the apolitical nature of our activities it has been a long established convention that the Director of Security brief the Leader of the Opposition as well as the Prime Minister on important security issues.

And finally, but no less importantly, the Act was also amended to affirm that the Act does not:

.. "...limit the rights of individuals or organisations to engage in lawful advocacy, protest or dissent."

This leads to the second question:

**2. HOW DO WE KNOW THEY OPERATE WITHIN THE LAW?
THEY ARE NOT ACCOUNTABLE IN THE WAY OTHER GOVERNMENT
DEPARTMENTS ARE!**

It is the nature of national security that to make information available publicly and in detail is to debilitate the security mechanism you have established. Nevertheless strong action has been taken to ensure that we are properly staffed and accountable!

- First, our employment policy is designed to ensure that the NZSIS is not staffed by "a bunch of cowboys" or zealots although we get some outlandish enquiries for recruitment from people with such diverse skills as black belt in judo, hunting and shooting skills and expert in cultivating carnivorous plants. In fact our staff are very ordinary, very loyal and very committed New Zealanders. I can attest that should I or a senior officer seek to breach or circumvent the law our immediate conscience would be our own staff. They are our first line of control and protection.

- Secondly, our systems of operation are subject to our own extensive internal control and review procedures designed to confirm legality, propriety and financial probity.

- And overarching those internal procedures and mechanisms there is now a comprehensive range of effective oversight and review mechanisms which give genuine reassurance of the legality, propriety and cost-effectiveness of the Service. The Service is subject to full and detailed audit of its accounts and its operations by Audit NZ. New oversight provisions, which were clearly overdue, were also passed into law last year establishing a Committee of Parliamentarians on Intelligence and Security and an Inspector General. They were designed, after extensive review of overseas mechanisms, to meet our own circumstances.

I can assure the critics who say that these arrangements are Government "window-dressing" that this is far from the case. I have now appeared before the new Committee and I can affirm that appearance before such a senior group of MP's involved a most demanding review of policy administration and expenditure of the Service. And the Inspector General, who has widely based authority to review legality and propriety of our activities and to investigate complaints, will see everything relating to his investigation except where a ministerial certificate specifically declines him access. In my view, no Minister would lightly sign such a certificate limiting the

G who is a High Court Judge in his investigation except, maybe, at a time of vital national security concern.

3. WHAT DO YOU DO NOW THAT THE COLD WAR IS OVER?

Believe me, there is plenty to do - probably more than in the 1960's and 70's when the NZSIS focus both by law and by circumstances was very much narrower. Security was defined in the Act as "protecting New Zealand from espionage, sabotage and subversion and terrorism" and the most significant security issue was the Communist Bloc and the threat its member countries were seen to pose. In those days, our concern was to protect "New Zealand's safety, security and defence" to quote the Crimes Act in its definition of espionage. The threat was a serious one and, by the way, SIS activities were most successful. The Service was responsible for the advice which led to the Government's expulsion of foreign spies from the country on several occasions.

We are a smaller and tighter Service than we were a decade ago, but the focus has broadened considerably. Last year the definition of security was expanded to include "the making of a contribution to protecting New Zealand's international or economic wellbeing". Our security vulnerabilities are seen as being much more closely related to our own foreign and trading policies, to the protection of the products of our own R & D and of our intellectual property. Of course, we must continue to give due attention to the protection of those "safety, security and defence issues" of the definition I quoted. And, at the same time we must have real and continuing concern about the threat of terrorism.

Of course, these comments lead straight to the next most often asked questions about the NZSIS.

4. WHAT HAS NZ GOT THAT IS WORTH PROTECTING?

Events of recent months have been helpful in offering an answer to this question. While I don't want to join the media flurry about whether it was theft or souveniring or whether or not an arrest should have resulted, the 'Pacific Rose' apple bud case at Auckland Airport amply illustrated the delicate balance we have to keep in maintaining good international trading relationships, while at the same time protecting our national advantage.

There should be no doubt that our R & D and its resulting technology is worth stealing. NZ scientists in research institutes around the country are developing leading edge products, especially in the agricultural and horticultural sciences. These products, because of the commercial advantage they give to our industry, obviously contribute to NZ's economic wellbeing.

But it is not just the trading advantage which we stand to lose. In some cases dual use technology is involved (that technology which, though developed for a benign purpose, could be re-deployed for more sinister use, especially as chemical or biological warfare agents). We must also accept the responsibility to ensure that inappropriate access is not provided to such agents.

The "well-being" amendment to the NZSIS Act last year, which I have just mentioned was motivated to a significant degree by this need to provide more effective security protection in these areas of NZ's vital national interests where economic espionage is being practised and can be to the nation's serious disadvantage.

At the same time the Act was broadened to allow the Service to retain and to communicate to the Police or other appropriate authorities information for the purpose of preventing or detecting serious crime. That amendment makes good sense and will allow us to assist in areas such as money laundering, international crime and even drugs when we find intelligence helpful to

Whoever is the lead agency in these areas. Under old legislation we could not provide such assistance.

And the other question that my earlier comment on today's role for the Service raises is:

5. WE LIVE IN THE SOUTH PACIFIC, WHY SHOULD WE BE WORRIED ABOUT TERRORISM?

We have been relatively lucky, and I hope that continues to be the case. But it would be folly to become blasé.

There have been many examples of the international dimension of terrorism in today's world and some closer to home than is comfortable. Of course, there was the Rainbow Warrior and more recently, for example, the Aum Shimryko sect responsible for the Japanese subway gas attack was identified as having set up in West Australia, to test the chemicals they were developing, on sheep.

Here in New Zealand, immigration has given us an ever more diverse society which brings with it some significant advantages. But, at the same time, it can occasionally raise new security concerns, especially when our new residents have come from an unstable home environment and have not totally disassociated from the intimidation of the extremist groups they had hoped to leave behind. We don't accept that fund raising and other support activity for international terrorism should occur unchecked in New Zealand.

Our relative isolation is no guarantee of immunity from terrorism. Modern transportation and communications have closed the gaps. Prospective targets exist in New Zealand as elsewhere - For example, a foreign mission or dignitary may be seen by the dedicated terrorist to be at their most vulnerable here in New Zealand. Equally, unscrupulous extremists may see a means of gaining their world wide objective is to mount a terrorist attack during a major international event here. The APEC leaders conference or the America's Cup both in 1999 spring readily to mind.

We need, and we have a well established Government mechanism for combating a possible terrorist threat which foresees a closely integrated inter-departmental response. Central to that response is the availability of up-to-date and accurate intelligence, to protect our borders and to reduce our vulnerability to terrorist action here and, if there is an incident, to provide the essential information which will assist sound decision-making at the time of an incident. The Security Intelligence Service is a key player in providing that intelligence.

6. HOW DO YOU SPIES ACTUALLY OPERATE?

I will pause briefly to explain that we do not consider ourselves to be "spies". We don't really enjoy that description - we feel that those who work covertly against New Zealand interests are spies. I would describe us as "officers" or "officials" of the Government undertaking our legislated protective security role.

That said, let me answer the questions anyway. In general terms we employ two major techniques in undertaking our responsibilities. Firstly, we mount active operations to collect intelligence on security which we then analyse and distribute appropriately to the Minister or other authorities.

Most people would be surprised to be told that even in this operational role the large majority of our work is done openly. Having identified a threat, NZSIS officers will make an approach, identifying themselves by name, showing an ID card and explaining the Service's role, before inviting comment from an individual or organisation who can help us in the matters at hand. In my six years in the Service I know of only a few occasions when such an approach has not

resulted in a positive response.

Other more covert methods are used by the Service where they are warranted by the seriousness of the security concern and where the law allows it, but a covert option is only employed after extensive analysis of all options for gaining the needed intelligence. And I have to admit it doesn't always go to plan. On one occasion one of our surveillance vehicles parked in a quiet cul-de-sac near a shopping centre triggered a full armed offenders alert because of concern that they were bank robbers. The result - two very shaken hand-cuffed SIS officers and improved liaison with the Police.

Only in the cases of major concern do we employ an interception warrant and, as I said earlier, the Act is very explicit on the legal steps we must take in making such an application to the Minister. Furthermore, with the new legislation even these decisions are reviewable.

Alongside the operational approach we have developed a relatively wide ranging security advisory role which is the basis for the physical and personnel advice we provide to those government departments and agencies who ask for it. On the personnel side, we conduct individual security vettings (always with the candidate's full knowledge and consent) and we advise the appropriate chief executive of our conclusions on the candidates trustworthiness to handle classified material.

We also provide physical security advice on request to other departments and agencies. This can range from security briefings for officials travelling or posted to sensitive posts off shore, to physical security reviews of locations where classified and sensitive material is to be held. We have developed and are providing specifically designed security awareness briefings for departments or agencies where sensitive or classified material which is an attractive target for others is developed, managed or stored. In our view this is an important facet of our role, the preventative or pre-emptive action in support of national security.

CONCLUSION

And so, to conclude, I reassert that there is an important place in our democratic structure for the Security Intelligence Service. We have a peaceful country where the threat is low - our job is to keep it that way. Our role is protective in nature and though some people are less than well disposed towards some of our activities they are well founded in law and are subject to rigorous control and oversight. I have given brief responses to the six questions we most frequently face. In the interests of covering the ground I have kept the answer short and, obviously, in the interests of security, I have avoided comment in areas involving sensitive intelligence issues. I am happy to answer your questions on that same basis. Thanks

File

INTRODUCTION

Thank you for your welcome.

"The SIS really cares and understands - and that's a huge comfort" - Dame Pat Evison says that about SIS insurance but we like the philosophy and subscribe to it.

The NZSIS was established over 40 years ago in 1956, and it has continued to operate in an environment of constant change. During that time not much has been known about us, largely because we declined to comment on matters of national security. If we get publicity it is often unfavourable - our successes are seldom acknowledged but it seems our problems always are!

We have a reputation as a secretive and slightly "spooky" organisation and one which lives in the past. We are working to change that view. Last year we produced a public booklet on the Service and I have taken on talking commitments such as today's. I hope I can provide an insight which will raise your level of understanding and confidence in who we are, what we do, and why we do it.

Generally, it is said that we never answer questions. I hope to change that view too. I intend to ask those questions we hear asked most often about the SIS BUT to go further and actually answer them. So, here we go.

Question 1. WHY DOES NEW ZEALAND NEED A SECURITY SERVICE / DOESN'T IT CONTRAVENE OUR HUMAN RIGHTS?

Put simply, we need a security service because, even today in New Zealand, we do face very real threats to our security. The SIS is a fundamental and important part in the basic framework which has been set in place by Government to properly protect our democratic institutions. You can judge after my 20 minutes or so, whether I have convinced you of this proposition.

But does the SIS contravene your rights? Is it legal? I am not a lawyer but here's my attempt at an answer.

- A democratic state has the right to protect itself using such mechanisms as Police, Defence Forces and Security Services but their powers, authorities and responsibilities should be well defined in law.

The need for that protection can sometimes involve activity which would otherwise infringe upon individual freedom. Again such exceptions should also be established in law.

- For us, law is in place in the form of the NZSIS Act 1969 with its amendments. Where the Court of Appeal proposed it was deficient in its December 1998 findings the Government has moved quickly to amend the law to make it explicit. Two amendments will pass into law this year to ensure this is the case.
- Amongst other things the law:
 - defines "security" precisely
 - is very specific about when we can employ our most intrusive activity, the interception warrant - "the value of the information must justify the interception and must not be obtainable by any other means"
 - protects people involved in legal protest, advocacy or dissent - they are not our business
 - states that it will not be a function of the Service to further the interests of any political party. - In the latest amendment we will be required by law to be politically neutral.

Question 2. HOW DO WE KNOW THEY OPERATE WITHIN THE LAW? AREN'T THEY A BUNCH OF ZEALOTS WHO ARE NOT ACCOUNTABLE IN THE WAY OTHER GOVERNMENT DEPARTMENTS ARE!

Most people will understand that a national security agency cannot make all its information available publicly and in detail. To do that would be to totally debilitate the security mechanism we have established. Nevertheless strong action has been taken to ensure that the SIS is properly staffed and accountable!

- First, our staffing. We are very careful not to employ "a bunch of cowboys" or zealots. We do get some outlandish enquiries for recruitment from James Bond type people with such diverse skills as black belt in judo, hunting and shooting skills and, in one case, expert in cultivating carnivorous plants. But the reality is that our staff are very ordinary, very loyal and very committed New Zealanders. There is a very careful selection process to ensure this is the case. Importantly, should I or a senior officer seek to breach or circumvent the law our immediate conscience would be our own staff. As concerned New Zealanders themselves they are our first line of control and protection.

- Secondly, our systems of operation are subject to our own extensive internal control and review procedures designed to confirm legality, propriety and financial probity.

- But, overarching those internal procedures and mechanisms there is now a comprehensive system of effective oversight and review which gives genuine reassurance of the legality, propriety and cost-effectiveness of the Service. For example:
 - The Service is subject to full and detailed audit of its accounts and its operations by Audit NZ.

 - New oversight provisions, which were clearly overdue, were also passed into law in 1996 establishing a Committee of Parliamentarians on Intelligence and Security and an Inspector General. They were designed, after extensive review of overseas mechanisms, to meet our own circumstances.

To the critics who say that these arrangements are Government "window-dressing" I say that having appeared before that Parliamentary Committee of senior MP's from both sides of the House it involves a most demanding review of policy, administration and expenditure of the Service. And there is also the Inspector General. Anyone who has a problem with what the SIS has done has a right to lay a complaint before the IG. He has widely based authority to review legality and propriety of our activities and to investigate complaints and will be given all files and information relating to his investigation.

Question 3. WHAT DO YOU DO NOW THAT THE COLD WAR IS OVER?

Believe me, there is plenty to do. Security is defined, in part, in the Act as "protecting New Zealand from espionage, sabotage and subversion and terrorism" and the most significant security issue of the 1960s and 70s was the Communist Bloc and the threat its member countries were seen to pose. The threat was a serious one and SIS activities were most successful.

Now, we are a smaller and tighter Service than we were a decade ago, but at the same time the focus has broadened considerably. We must continue to give due attention to the issues of espionage, as we did previously. And now we must also have real and continuing concern about the threat of terrorism.

But the definition of security was expanded in 1996 to include "the making of a contribution to protecting New Zealand's international or economic well-being". Our security vulnerabilities are seen as being much more closely related to our own foreign and trading policies, to the protection of the products of our own R & D and of our intellectual property.

That statement usually invites the next question :-

Question 4. WHAT HAS NZ GOT THAT IS WORTH PROTECTING?

A simple example. The 'Pacific Rose' apple bud case at Auckland Airport two years ago amply illustrated the delicate balance we have to keep in maintaining good international trading relationships, while at the same time protecting our national advantage. There have now been several attempts to steal this product of NZ R & D worth millions in international trade advantage to NZ.

There should be no doubt that our R & D and its resulting technology is worth stealing. NZ scientists in research institutes around the country are developing leading edge products, especially in the agricultural and horticultural sciences. These products, because of the commercial advantage they give to our industry, are worth stealing and do contribute to NZ's economic well-being.

But it is not just the trading advantage which we stand to lose. In some cases dual use technology is involved (that technology which, though developed for a peaceful purpose, could be re-deployed for more sinister use, especially as chemical or biological warfare agents). We must ensure that these agents don't get into the wrong hands.

Let me assure you that this type of economic espionage is being practised now and can be to the nation's serious disadvantage.

The Act has also been broadened to allow the Service to retain and to communicate to the Police or other appropriate authorities information for the purpose of preventing or detecting serious crime. Now, we can assist in areas such as money laundering, international crime and even drugs when we find intelligence helpful to whoever is the lead agency in these areas. Under old legislation we could not provide such assistance.

And the other question that my earlier comment on today's role for the Service raises is:

Question 5. WE LIVE IN THE SOUTH PACIFIC, WHY SHOULD WE BE SERIOUSLY WORRIED ABOUT TERRORISM?

We have been relatively lucky and I hope that continues to be the case. But it would be folly to become blasé.

There have been many examples of the international dimension of terrorism in today's world and some closer to home than is comfortable. Of course, there was the Rainbow Warrior and more recently, for example, the Aum Shimryko sect responsible for the Japanese subway gas attack was identified as having set up in West Australia to test the chemicals they were developing on sheep. And there have been the recent bombings of US Embassies in Nairobi and Dar Es Salam and the emergence of Usama Bin Laden as the new international terrorist threat. These groups do not seek short term definable objectives eg, the release of prisoners; - they are extremely difficult to identify or trace - they are prepared to cause major destruction and casualties (including the innocent) AND THEY DO NOT operate within national boundaries!!

Here in New Zealand, immigration has given us an ever more diverse society which I acknowledge brings with it real and significant advantages for the country. But, at the same time, it can occasionally raise security concerns, especially when our new residents have come from an unstable home environment. There are instances where they have not totally disassociated from the activity and intimidation of the extremist groups they have left behind. We don't accept that intimidation of NZ residents or citizens to promote fund raising and other support activity for international terrorism should occur unchecked in New Zealand.

And in the technological era our relative isolation is no guarantee of immunity from terrorism. Modern transportation and communications have closed the gaps. Prospective targets exist in New Zealand as elsewhere -

For example, a dedicated terrorist may see a foreign mission or dignitary to be most vulnerable here in New Zealand. (Usama Bin Laden will target US interests anywhere in the world). In September NZ hosts State Visits by Presidents Clinton, Jiang Zemin and Kim Dae-jung (Korea).

- Equally, unscrupulous extremists may see that a means of gaining their world wide objective is to mount a terrorist attack during a major international event here. The forthcoming APEC leaders conference in September where we host 21 Pacific Rim leaders, including the world's most influential, or the America's Cup, or Olympics 2000 in Sydney spring readily to mind.

We need, and we have a well established Government mechanism for combating a possible terrorist threat which foresees a closely integrated inter-departmental response. Central to that response is the availability of up-to-date and accurate intelligence, to protect our borders and to reduce our vulnerability to terrorist action here and, if there is an incident, to provide the

essential information which will assist sound decision-making at the time of an incident. The Security Intelligence Service is a key player in providing that intelligence.

Finally the question you all wanted to ask:

Question 6. HOW DO YOU SPIES ACTUALLY OPERATE?

There have been many books which propose to tell how spies operate - from John Le Carre to Tom Clancy - now is the time to dispense with the fiction and talk the plain and often mundane facts.

Let me start by reminding you the SIS has no enforcement authority at all.

- Our primary role is to collect intelligence on security which we then analyse and distribute appropriately to the Minister or other authorities. Most people would be surprised to be told that the large majority of this work is done openly. Having identified a threat, NZSIS officers will make an approach, identifying themselves by name, showing an ID card and explaining the Service's role, before inviting comment from an individual or organisation who can help us. In my eight years in the Service I know of only a few occasions when such an approach has not resulted in a positive response.
- Other more operational methods like surveillance are used by the Service where they are warranted by the seriousness of the security concern, where the law allows it and when other options are exhausted. And I have to admit it doesn't always go to plan. Many years ago one of our surveillance vehicles, parked in a quiet cul-de-sac near a shopping centre, triggered a full armed offenders alert because of alert shopkeepers' concern that they were bank robbers. The result - two very shaken hand-cuffed SIS officers and improved liaison with the Police.
- Finally, it is only in the cases of major concern that we employ our most intrusive mechanism, an interception warrant which must be authorised by the Prime Minister and Commissioner of Warrants (shortly).
- We have a wide ranging security advisory role for those government departments and agencies who ask for it. On the personnel side, we conduct individual security vettings (always with the candidate's full knowledge and consent) and we advise the appropriate chief executive of our conclusions on the candidates trustworthiness to handle classified material.

We also provide physical security advice on request to other departments and agencies. This can range from security briefings for officials travelling or posted to sensitive posts off shore, to physical security reviews of locations where classified and sensitive material is to be held. We have developed and are providing specifically designed security awareness briefings for departments or agencies where sensitive or classified material which is an attractive target for others is developed, managed or stored. In our view this is an important facet of our role, the preventative or pre-emptive action in support of national security.

CONCLUSION

And so, I conclude, by asserting that there is an important place in our democratic structure for the Security Intelligence Service. We have a peaceful country where the threat is low - our job is to help keep it that way. Our role is protective in nature and though some people are less than well disposed towards some of our activities these are well founded in law and are subject to rigorous control and oversight. I have given brief responses to the six questions we most frequently face. In the interests of covering the ground I have kept the answer short and, obviously, in the interests of security have not touched on sensitive issues.

And another quote to finish:

"Espionage is the world's second oldest profession and just as honourable as the first."

Michael Barrett (1984)

Speech to Serious Fraud Office staff

Background

Date	12 June 2017
Timing	1100–1145 20 minute presentation, 10 minutes of questions from the audience
Topics	<ul style="list-style-type: none"> • You, and the NZSIS • Challenges of being a small organisation • Trends – the need for transparency and accountability

Speaking notes

Introduction

- Good morning everyone. Thank you very much for asking me to come and speak with you. Julie first made contact with me at the end of last year about coming to talk to the team. I am sorry it has taken me so long to get here. I am really pleased to finally meet you all. It's a shame Julie is away today – I will do my best to cover off the information she asked me to talk about.
- So, today I would like talk a little about me and the NZSIS. I would also like to talk about the topic Julie asked me to consider: the challenge of being a small organisation and some of the trends you might want to consider.
- I will make sure I leave some time for questions at the end, but I am also keen for this to be a conversation, so please feel free to ask questions as we go along.

You and the NZSIS

- I have been the Director of the New Zealand Security Intelligence for three years. It is a role that I absolutely love. A lot like your work here at the Serious Fraud Office, we do a job that is challenging and difficult at times. It is also vitally important to the fabric of New Zealand society.
- I started my career as a lawyer in public practice though. I joined the public service when I joined the Cabinet Office and immediately felt an affiliation with the concept of public service – and I have never really looked back. The last role I held there, after spending some time at Foreign Affairs, was Cabinet Secretary - a senior leadership role. That cemented my passion for public service and for upholding the democratic system in New Zealand even further.
- The NZSIS is a civilian government agency. We aim to achieve three main outcomes:
 - New Zealanders are safe,
 - New Zealand's key institutions are protected, and
 - New Zealand's national advantage is promoted.
- To achieve those outcomes, we work alongside other agencies in the New Zealand Intelligence Community and with our international partners to maintain New Zealand's national security.
- There are three main aspects to the NZSIS's work.

Security intelligence

- We use a wide variety of sources and methods to identify, and provide advice to counter threats to national security to New Zealanders at home and abroad.
- The threats include terrorism and violent extremism, espionage conducted by other states, the proliferation of weapons of mass destruction, and hostile cyber activities.

- We work closely with partners such as the New Zealand Police, the New Zealand Customs Service, the Department of Internal Affairs, Immigration New Zealand and the New Zealand Defence Force to prevent threats to security progressing to acts of violence or espionage.
- This role consumes the greatest part of the NZSIS's resources.

Foreign intelligence

- Foreign intelligence in the NZSIS context primarily relates to regional security in the Pacific and includes understanding what others are doing or intending to do.
- Foreign intelligence, and the assessment of it, is vital for knowing what is going on in the world, whether it is strategic challenges, political or economic instability, or security issues.
- Based on the information we gather, we provide advice to other government agencies such as NZDF or the Ministry of Foreign Affairs and Trade or to our international partners.
- In this role, the fundamental business of intelligence is about helping decision makers manage risks to New Zealand's interests.

Protective security advice

- The NZSIS's role is about providing advice and support to New Zealand state sector agencies and to outline the Government's expectations of the public sector for managing personnel, physical and information security, and supporting agencies to better manage risks and assure continuity of delivery.
 - This area includes our vetting services which you will have come across when you applied for a security clearance.
 - My agency also screen people visiting or seeking residency who may pose a risk to national security. We do this by gathering information about them from police records, travel information, interviews and other sources
-
- We have a big and challenging job to deliver for the country.

Challenges of being a small organisation

- Julie asked me to talk with you about the challenges of being a small organisation.
- The NZSIS has approximately 200 staff is growing quite quickly as a result of additional funding we received in Budget 2016. So I will reflect, instead, on my time as Cabinet Secretary where I led two different functional areas - the Cabinet Office and Government House. Both of these had teams of around 30 people.
- There are three main challenges I think smaller organisations need to overcome:
 - Depth
 - Resilience
 - Flexibility and agility.
- Depth is the first area I think can be challenging in a smaller organisation. With a small number of staff there often isn't capacity in the system to enable more than one or two people to hold expertise in any one area. This often also applies to key working relationships, where one staff member holds the relationship with an important stakeholder. This creates 'key person risk' where if that person was away for a long period of time or left the organisation work programme or relationship is at risk of falling over.
- Resilience is another area where I think smaller organisations can face challenges. A small workforce means that there are a limited number of people to deliver the organisation's work. In busy sectors, with important work and challenging deadlines, this can create fatigue. Staff can get burnt out, they might experience more sickness and their

overall productivity and motivation can decrease. As I mentioned in my first point, with limited depth, there aren't always people available and able to step in – it can then become a never-ending circle.

- Which brings me to the final difficulty I think smaller organisations face - being flexible and agile. All of the best planning and intentions in the world cannot foresee all of the issues that might be coming down the chain. Natural disasters, changing ministerial priorities, security problems, and world events. These are just a few of the things that could come up at any moment and could need to be a priority within the organisation. That means an organisation needs to have the flexibility and agility to respond and reprioritise – which can be challenging given my first two points about depth and resilience.
- None of these challenges are unsurmountable. By identifying them and building mitigations into your organisational strategy they can be addressed where resources allow. This could include things like stakeholder planning, good prioritisation, developing a succession plan, and focusing on staff wellbeing and resilience skills.
- On the other side of the coin, are the many strengths that come from being a smaller organisation. Three areas come to mind:
 - Interpersonal relationships
Straightforward communications
 - Clearer line of sight between work programme and mission and vision.
- First of all – interpersonal relationships. With a smaller staff group people tend to have the opportunity to get to know everyone else a little more than in a bigger organisation. That is a really positive thing. The better people know each other and understand each other's talents and style – the easier it is to work productively together. At a really simple level, you can all fit into a meeting room for staff meetings! I think that something a lot of bigger agencies would envy!

- This leads on nicely to the next strength of smaller organisations – straightforward communication. With a smaller staff group, internal communications is a lot more straightforward. You can do a lot more face to face communication. Less staff means it's easier to communicate to everyone in a timely way – that is without big gaps in time between talking to one group and other due to sheer size of an agency. You can also tailor your communication better because you know people better.
- Finally, clearer line of site between the work each person does and the mission and vision. With fewer layers in a smaller organisation, there is often a shorter and therefore clearer line between the work someone does and the organisational mission and vision. This can be a powerful motivator for staff as you can absolutely see the difference you make and how it contributes to the greater purpose of the agency you work for. The line of site also helps an organisation prioritise its effort –which can help overcome some of the challenges I discussed earlier.
- Of course, none of these strengths are a given. They still require sound organisational strategy, development and leadership. But all things being equal, they can really set an organisation apart.

Trends – transparency and accountability

- Julie also asked me to talk about trends we are seeing that you might want to consider for the future. I have taken that theme quite broadly and what I would like to discuss is the increased public demand for transparency and accountability.
- These are issues that are really key for us at the NZSIS where it is vital to have the trust and confidence of the public in order to be able to do our job well. Given your role I believe it is equally important for you.

- NZSIS's vision is to be ahead of the curve: providing indispensable security and intelligence services underpinned by high public confidence and trust.
- We know that to be successful, we need the support of the New Zealand public. Our domestic and international partners also need to understand and value our work. The NZSIS cannot be successful in our mission if we operate in isolation.
- As a security agency, we face increasing public demand for transparency, oversight and accountability, and media demand for more detailed and frequent information. The proliferation of round-the-clock news coverage compounded by the vast reach of social media really drives and fuels these demands.
- So we need to balance the need to respond and to maintain transparency and trust, with the need to maintain security of information. Our ability to do our job depends on it.
- Our new legislation, the Intelligence and Security Act 2017 was enacted in March this year. As a result, there is now increased transparency and oversight of our security and intelligence agencies, all the while ensuring that we are able to protect New Zealand and New Zealanders.
- The Act explicitly sets out the agencies' powers and activities more clearly than ever before. It also enables Ministers to enter into agreements for direct access to information datasets held by other government agencies. These agreements are published online for anyone to read.
- The Act is the most significant reform of the agencies' legislation in New Zealand's history. Importantly, it protects the privacy and human rights of New Zealanders.

- It also brings the GCSB and NZSIS closer into the core public service which also increases our overall accountability and transparency. From my perspective, being more open transparent can only be a good thing, for agencies and for the public.
- To optimise the benefits of the new Act, we are actively trying to be more open. Our public engagement is part of that.
- We have increased our efforts to engage more with the public and media. I have been available for interviews and briefings with media and I have spoken at a number of functions and conferences across the country.
- Some of those media interviews have been about things that haven't gone so well for us. We believe in fronting up and owning our mistakes. If we are really seeking the public's trust then that is the only way to approach stuff ups.
- This presentation, and presentations like it, is all part of helping to tell the story of what we do and the positive contribution that we make to New Zealand. Again, this helps people have trust in the work that we do to keep them safe.

Closing

- I hope that has been useful. I've traversed a few different topics which I hope has been interesting.
- As I said, talks like this are one of the ways that NZSIS helps increase transparency about our work. So, thank you again for inviting me.
- I am really happy to answer questions.

Hugo Group speech

Background

Date	25 August 2017
Address	Queenstown
Timing	Lunch time address 20-25 minutes with 10 minutes for questions from the audience
Audience	22 senior CEs from the private sector and their partners, plus other speakers
Topic	Political, economic and technological change and how we manage associated risk, SIS, IC and its work, protective security considerations

Hello everyone

It's my pleasure to be here with you today. Looking at the Retreat programme, you have already had some very thought-provoking conversations – with more to come. I hope to contribute some further thoughts and considerations from a security and intelligence perspective.

Over the last few years, following my appointment as Director of Security, I have given many presentations with the aim of making the work of the NZSIS, and the wider New Zealand Intelligence Community more open, transparent and visible. Part of the reason for doing that is to build trust and confidence with the New Zealand public who rightly feel that they have a role in the security discourse.

Another reason I have been actively engaging with communities, including leaders like yourselves, is that the impact of the security threats we face as a country and as part of the global community, are potentially devastating to us all. And, there are things that we can all do to protect ourselves and our organisations. So, some of the things I will talk about today are areas, like protective security, that you should be thinking about as leaders.

Today I'm going to cover a few different areas

- Who the NZSIS is, the work that we do to make a difference for New Zealand and New Zealanders, how we work within the New Zealand Intelligence Community
- What we are seeing in terms of the changing threat environment we operate in
- Security areas I think it is prudent for leaders and organisations to consider.

While I know that you operate under Chatham house rules, much of the work the NZSIS does is sensitive and so there are some areas where discussing them would compromise security or the ability for us to do our job well. So, the examples I will use today are unclassified.

I'll begin with a bit about me and the NZSIS.

I have been the Director of the New Zealand Security Intelligence for three years. It is a role that I absolutely love. We do a job that is challenging and difficult at times. It is also vitally important to the fabric of New Zealand society.

I started my career as a lawyer in public practice though. I joined the public service when I joined the Cabinet Office and immediately felt an affiliation with the concept of public service – and I have never really looked back. The last role I held there, after spending some time at Foreign Affairs, was Cabinet Secretary - a senior leadership role. That cemented my passion for public service and for upholding the democratic system in New Zealand even further.

The NZSIS is a civilian government agency. We aim to achieve three main outcomes:

- New Zealanders are safe,
- New Zealand's key institutions are protected, and
- New Zealand's national advantage is promoted.

Our work can be broadly split into three areas:

- We provide protective security advice and vetting services:
 - The NZSIS provides advice and support to New Zealand government agencies and outlines how the Government expects them to keep themselves secure.
 - We carry out vetting checks on people who need security clearances to carry out their work in government. That includes gathering information from police records, travel information, interviews and other sources to determine whether a person is suitable to gain access to classified material.
- We are a Security Intelligence Service:
 - We use a wide variety of sources and methods to identify threats, collect intelligence, and provide advice to counter threats to the national security of New Zealand and New Zealanders at home and abroad.
 - Threats include terrorism and violent extremism, espionage conducted by other states, the proliferation of weapons of mass destruction, and hostile cyber activities.
 - We work closely with other agencies such as the New Zealand Police, the New Zealand Customs Service, the Department of Internal Affairs, and Immigration New Zealand to prevent threats to security progressing to acts of violence or espionage.
- We provide Foreign Intelligence advice:

- Our foreign intelligence work primarily relates to regional security in the Pacific and includes understanding what others are doing or intending to do in our region.
- Foreign intelligence, and the assessment of it, is vital for knowing what is going on in the world, whether it is geostrategic shifts, political or economic instability, or international security issues.
- In this role, the fundamental business of intelligence is about helping decision makers make informed decisions and manage risks to New Zealand's interests.

To deliver on our mission and keep New Zealand and New Zealanders safe, we work alongside other agencies in the New Zealand Intelligence Community, including the GCSB and the Department of the Prime Minister and Cabinet, and with our international partners.

Considering the geopolitical uncertainties and the significance of the security challenges facing New Zealand, it is essential the NZSIS and the other agencies in the New Zealand Intelligence Community maximise our impact by working together within our legal framework.

We all play a specific role in relation to National Security.

- The NZSIS focuses on human intelligence. That is, gathering intelligence through people.
- The Government Communications Security Bureau (GCSB) focuses on signals intelligence. They work in the electronic sphere.

- The intelligence collection from both agencies helps the National Assessment Bureau within the Department of the Prime Minister and Cabinet (DPMC) to make assessments to inform Government decision-making.

So, what is the environment we are dealing with?

New Zealand faces security threats, like any other country.

Terrorism and the threat from violent extremism continue to be of very real concern internationally, and New Zealand is not immune. There are groups and individuals who actively seek to unsettle our democratic values and way of life using a variety of means – including the impact acts of terror have on the national psyche.

While the terrorism threat level in New Zealand remains at 'low', the international environment continues to evolve. The threat from the so-called Islamic State, or Da'esh, al-Qaida and related extremist groups continue to be of concern.

Some key changes that have impacted on the New Zealand environment are:

- the increasingly sophisticated and pervasive social media presence of extremist groups, but in particular Da'esh and its ability to reach and influence individuals across the world;
- the nature of the messages from those types of groups. Those messages include encouraging individuals to travel to Syria or Iraq, and if that is not possible, to commit attacks in their own countries; and
- the nature of attacks, which looking across the spectrum, have become increasingly unsophisticated. For example, in recent

months we have seen attacks committed overseas using just vehicles and knives.

The threat of espionage persists and the distinction between state intelligence activities and commercial theft has become increasingly blurred. Some countries commit state-sponsored commercial espionage.

State actors continue to conduct cyber operations to acquire sensitive information and those types of activities are becoming increasingly difficult to detect. Defending against espionage and cyber attacks is now a crucial activity for public and private sector agencies alike, and is a key focus for us.

Threats to New Zealand's national security have historically been characterised as either domestic or international in nature. In reality, an increasing number of security issues do not respect national boundaries.

Technological developments such as drones and encryption also create real challenges.

As a result of all of this, New Zealand's national security agenda is more broad and complex than ever before.

I thought it might be useful to talk about some of the areas I think leaders and organisations should consider in terms of your own protective security

As I already mentioned, The NZSIS provides protective security advice to government by implementing and promoting the Protective Security Requirements for managing personnel, physical and information security.

That includes providing formal guidelines and ongoing support so that agencies can better manage business risks and assure continuity of service delivery.

This is an area where I think as New Zealanders we can be a bit naive and don't always realise how vulnerable we can be. Security matters – and not just for organisations that hold classified information. Whether we work for government agencies, private sector companies or academic institutions, others may find us a lot more interesting than we think.

I'm not sure why we find it hard to believe that we may be targeted and exploited in the course of our work. In our personal lives we know we may be targeted by scammers, ransomware, and so on. In reality, as well as ordinary criminals, there are state-sponsored actors who are actively trying to steal information from us in our places of work and study.

Here are a few facts.

- Foreign Intelligence services in many countries screen and monitor incoming visitors.
- Business and government travellers from New Zealand regularly report that their hotel rooms and belongings have been searched while they were overseas.
- Electronic equipment is easily compromised in these circumstances.
- Business and government travellers are also targeted by Foreign Intelligence Services either through personal contact or through spear phishing.

I will give a couple of examples of how this plays out – the stories are real but the facts have been changed.

Example one

A senior manager had a job in a high-tech organisation. She was on Linked-In, which provided a lot of information about her professional role. She also had a personal Facebook page that was visible to the public, which showed she loved gardening. She had devices that she used for both private and professional purposes.

One day she received an email advertising a garden show. She clicked on a link, which installed and executed malware.

Example two

An upper-level manager and his lead negotiator received an invitation to a three-day trade conference in a foreign country. Neither of them intended to take or discuss classified material, so they did not seek travel approval or a travel briefing from their Security Officer or the NZSIS before departing.

They both took their private and work electronic devices overseas with them, including their cell phones and laptops. Before leaving New Zealand, they deleted information on their devices they considered sensitive.

The pair knew there would be foreign delegates present at the conference so decided to leave their devices in the safes in their hotel rooms. However, while they were out, foreign intelligence officers accessed their hotel room and installed malware on their devices that automatically logged all activity on the devices, even once the pair had returned to New Zealand.

The officers also cloned the hard drive of the laptops and recovered not only the deleted classified documents, but also intellectual property and sensitive information relating to the trade negotiations.

If the manager and negotiator had sought proper advice before departing, they would have been given a briefing that would have helped them to avoid some basic traps.

They would have been told to take as few electronic devices as possible, leaving their personal devices at home and maybe just taking a “burner” or temporary device without all their personal and work data on it. They would have known that deleted material can still be accessed. They would have been told to keep their electronic devices with them at all times.

The kind of naive trust that they showed is probably pretty typical of New Zealanders travelling overseas. And I do understand that – our national values and character include trust and integrity – and it can be a shock to discover that we are fair game in other countries.

We provide a suite of practical information about protective security for public and private agencies online at www.protectivesecurity.govt.nz – do take some time to have a look. And, if you want to, get in touch.

And for you to think about, here are a few tips which might seem a bit basic but are really important:

- Be sceptical of offers of help and favours being offered by foreigners.
- Minimise personal information that you reveal about yourselves, especially on social media.
- When you’re travelling, be very careful with electronic media. In some countries you might not want to take your devices (take burner devices instead). Don’t leave devices in hotel safes. Don’t use hotel Wi-Fi. Don’t use hotel shredders.

Insider threat

The other aspect of protective security is the concept of insider threat. An ‘insider threat’, or ‘insider’, is a current or former employee, contractor or business partner who intentionally or unintentionally misuses their legitimate access to harm an organisation’s customers, assets, capabilities, partners or reputation.

Common insider acts can include:

- unauthorised disclosure of official, private, or proprietary information
- fraud or process corruption
- unauthorised access to ICT systems
- economic or industrial espionage
- theft.

An insider's motivation is often because of a combination of factors and pressures, such as:

- revenge against an employer or colleagues
- uncertainty about their continued employment
- greed or financial gain
- political or religious ideology
- ego or notoriety
- coercion, manipulation, or exploitation from an external third party.

Sometimes internal security breaches can be unintentional – but none the less have a big impact on your organisation through staff being vulnerable to exploitation.

There are a couple of well documented private sector examples here in New Zealand that demonstrate how important this area is.

The first is the Tag Oil NZ intellectual property case where one of their production managers accessed a computer and stole geotechnical data from the company's computer. The stolen information was worth millions to the New Zealand Energy Corp (NZEC).

The second example is the ASB investment advisor who stole \$17.8 million from customers and said he found committing that fraud “easy”.

Protecting from insider threat is also an area of concern internationally, and it’s something we’ve seen play out very publicly in different parts of the world.

The majority of organisational security initiatives focus on perimeter defences. That means that insider threat events often go undetected. A 2016 survey conducted by Gartner found that only 18 percent of enterprises have a formal insider threat programme in place. And in fact, insider threat remains an area that many organisations see as an urban myth.

There are practical organisations can implement to mitigate insider threat. The big one is creating a security culture.

Organisational culture has a direct impact on security. Even with the best security processes and tools your organisation will still be at risk if your people have a poor attitude toward security.

There are six steps we recommend to help create a positive and sustainable security culture, and reduce the personnel security risks facing your organisation.

1. *Show commitment from the top*

To embed effective security practices and procedure, you need to show your commitment and model best practice.

2. *Build security awareness*

People are much more likely to engage in your security culture if they understand the credible security risks that face your organisation. Increased awareness will help people understand that they have important security responsibilities and know what those responsibilities are.

3. Publish clear communications about security

Everyone needs access to clear policies and procedures that:

- explain the reasons for your organisation's security instructions
- outline legal, regulatory and compliance requirements
- ensure people understand their responsibilities.

4. Support staff wellbeing

Provide people with access to support, such as a confidential employee assistance programme. Encourage them to report and deal with personal issues before they become a serious problem.

5. Manage concerning behaviour

Managers need tools and policies to identify, support, and manage people who display concerning behaviour to do with security, poor performance, or unacceptable conduct.

6. Avoid a blame culture

Organisations need to have robust policies about 'whistleblowing' to encourage staff to raise legitimate security concerns.

It needs to be safe for people to report emerging concerns or near misses as a way of helping colleagues who might be at risk, rather than getting them into trouble.

People who speak up should be seen as good corporate citizens rather than troublemakers.

The Ombudsmen has done some interesting work in this area from a public sector perspective. There is some useful information and good resources online at www.ombudsman.parliament.nz

Again, there is more information on the protective security requirements website so do have a look.

Before I finish, I'd also like to draw your attention to the tools that the GCSB provide around cyber security.

If Andrew Hampton was here today he'd probably tell you that basic information risk management has been shown to prevent up to 85 per cent of the cyber attacks seen today.

He'd talk to you about things like:

- managing user privileges – limiting the number of privileged accounts and monitoring their use;
- having policies about mobile working; and
- the importance of staff training so that your people understand cyber risk and their role in preventing it.

There is some great information online about managing cyber risk including some of the cyber threats out there. I recommend checking out www.ncsc.govt.nz and www.cert.govt.nz

Close

I have covered quite a bit of ground on security and intelligence today.

I am really happy to take questions.

Speech to Ombudsmen Association conference – 21 May 2018

Tena koutou, tena koutou, tena koutou katoa.

Thanks for asking me to speak today. I am a real believer in the importance of the work of ombudsmen. Ombudsmen shine a light on the workings of governments and industries around the world in support of openness, accountability, and integrity. You help to tip the scales of power back in favour of individual people.

Those are values in which I have strongly believed all my life. They are values that my parents instilled in me, and they have been areas of specific focus for me in my professional life – particularly when I worked in the Cabinet Office as constitutional adviser, Deputy Secretary, and as Cabinet Secretary. In those roles my work involved advising on the operation of democracy, considering ethics and propriety in relation to the conduct of executive government, supporting open and accountable government under the Official Information Act, and ensuring sound decision-making processes.

And yet here I am, the Director-General of the New Zealand Security Intelligence Service, an organisation that carries out covert intelligence-gathering activity, much of which is necessarily secret. This shift in roles has required me to think deeply about the power of the state, and the rights of the public in terms of: security, physical safety, transparency, privacy, freedom of expression, and political protest.

In New Zealand – as in the rest of the world – there has been a very active debate over the last few years about whether we have correctly struck the balance of these human rights, which is ultimately a debate about the extent of state power. My assessment of where that debate has landed in this country is as follows:

- People know there are national security threats to guard against. They want to be safe and they want their country to be secure.
- Most people understand that to achieve the mission of keeping them and their country safe the security and intelligence agencies need intrusive powers and need a level of secrecy.
- Most people are happy to allow those powers and that secrecy if they have a pretty good understanding of what the agencies are doing and confidence that they are behaving properly.

- People also want to know that there are effective and transparent mechanisms to continuously check that the agencies are not abusing their powers.

The intelligence agencies in New Zealand have been on a real journey to achieve this point, and today I will walk you through that journey so you can see how strongly the dial has been shifted in favour of individual human rights and openness. At the same time the intelligence agencies have been given legislative tools to be more effective in their work, so to my mind this really is a “win/win” situation.

It’s easiest to tell this story by telling you about my own involvement in the New Zealand Intelligence Community, because that covers the relevant time period.

I became interested in the Security Intelligence Service in about 2010. At that time I was the Secretary of the Cabinet, and the NZSIS was suggested to me as a next step. I remember thinking “What do they actually DO at NZSIS?” I knew about the protective security functions, like vetting for security clearances, but apart from that I knew almost nothing about them – only what I had read in the media, which over many years had been relentlessly negative. As Cabinet Secretary I had a good understanding of other government agencies, but this one was opaque. On the rare occasions when I dealt with staff at the Service, the people I spoke to wouldn’t even give their last names. I was intrigued.

So I was already interested in the New Zealand Intelligence Community when I was asked to carry out a review of compliance at New Zealand’s signals intelligence agency, the Government Security Communications Bureau. This compliance review was prompted by some events that had huge media coverage in New Zealand at the time. GCSB had been revealed as acting unlawfully in supporting a police raid on a high profile individual.

I knew nothing about GCSB and had absolutely no idea what to expect when I embarked on the review. I imagined that the staff of GCSB would be suspicious of me, but they could not have been more open and welcoming. I realised the truth of the statement that these agencies have “high external walls but low internal barriers.” Once you have your TOP SECRET SPECIAL clearance, then people will freely share with you what you need to know.

It was a real privilege to work in GCSB at such a time of organisational distress. I saw people who were proud of their work, who were passionate New Zealanders, and who were motivated to do what Parliament had mandated them to do in the way that Parliament had intended. They knew that they were in difficulty and they were horrified about it. They were not at all defensive about working with me to identify the root causes.

During that time I got my first real view of the work of New Zealand's intelligence community, and how the intelligence cycle works. I was very impressed with the calibre of the staff and how clever they are at their work. Not that I would claim to understand the technical side of what they do at the Bureau – maths has never been my strong point. But I developed a very high regard for the signals intelligence professionals and the others who work at GCSB.

By the time the review was completed I was really interested in the role of Director of the NZSIS. Interestingly, even though the Service had co-located with the Bureau in Pipitea House, I still had very little idea about what its people did. I did not “need to know” about the NZSIS for the purposes of the GCSB compliance review, and so I was not told.

When the NZSIS Director role was advertised, I applied and started preparing in earnest. I knew that the Service was an agency that specialised in human intelligence.” I didn't have many sources of information about the work of the Service. There was of course popular fiction. The works of John Le Carre, James Bond films, and programmes like Homeland gave me some pretty weird ideas about what might be going on at the NZSIS.

So, being a lawyer, I turned to what promised to be a more reliable source of information: the New Zealand Security Intelligence Act 1969. And that told me almost nothing. It described the functions of the NZSIS in general terms – to collect intelligence, to provide protective security advice, and so on – but most of the focus of the legislation is on intelligence warrants. If you just relied on the 1969 Act to form a view of the scope of the intelligence collection activity of the Service, you would think that all we do is intercept private communications under the authority of a warrant.

In reality the Service has always conducted a range of human intelligence collection activities, including physical surveillance in public places, and obtaining information from human sources.

I learned about these other activities after I got the job as Director. And I realised that these activities were not included in the legislation because they were not unlawful. The Service started out its life in New Zealand when the Police Special Branch was turned into a stand-alone agency, and at that time it had no legislative basis whatsoever. As with other security agencies in similar countries, officers of the Service simply undertook a range of activities in carrying out their work in the interests of national security.

The 1969 Act represented a great step forward when it provided a legislative basis for activities such as intercepting telephone calls and installing listening devices.

But the 1969 Act did not in any way refer to any activities undertaken by the Service that were lawful, such as physical surveillance. A great deal of what the Service did – such as obtaining information about individuals from telecommunications companies and banks - depended on a broadly expressed exemption to New Zealand's Privacy Act. None of that was referred to in the 1969 Act either.

From a strictly legal point of view, this was fine. There is a strong line of argument among jurists that legislation should only be used when required to authorise activity, and should not purport to regulate activity that is already lawful. Under this argument legislation should not authorise physical surveillance, for example, because it is already lawful to follow and watch a person in a public space.

The problem with this argument in relation to the Service was that the social contract was changing. By "social contract" I mean on the one hand the licence given by the public to intelligence agencies to conduct covert activity in order to keep the country safe, and on the other hand the level of information the public expects to know about intelligence activities in return. There are several reasons why the social contract has shifted.

First, the changes in the threatscape around the world – particularly in relation to foreign interference by state actors, and terrorist attacks by non-state actors – has raised public awareness that security agencies need to be equipped properly to counter those threats. That is the case even in a country as peaceful and geographically remote as New Zealand, where there is a growing public understanding that we are not immune from national security threats.

Second, changes in technology have given security and intelligence agencies more opportunities and more challenges, with greater privacy implications for New Zealand citizens. Bulk data, artificial intelligence and encryption are just some examples.

Third, as transparency in government has increased, the public's expectations have changed. People expect to know what the agencies of the state are doing. The public pays for the intelligence agencies and Parliaments elected by the people provide the scope of our powers. There is an expectation that the public will have a say in our activities and how they are conducted.

The outcome of the public debate that has occurred in New Zealand and in other liberal democracies is that there is a new point of balance between the public's right to know and the agencies' need to keep operational activity and capabilities secret. And that is very healthy.

Being more open about what we do reduces the risk that staff will want to expose operational activity that they feel the public should know about. Ultimately it strengthens public trust.

There will always be a point at which we need to keep operational information and capabilities secret. Our targets and adversaries are watching and listening closely to learn how to evade or penetrate us. But in western liberal democracies around the world more information about the security and intelligence agencies is being made public without seriously compromising those agencies' ability to carry out their work.

In New Zealand the government recognised the need to recalibrate the social contract when it decided in 2015 to conduct a comprehensive review of the legislation governing the two intelligence agencies and our oversight bodies. Dame Patsy Reddy and Sir Michael Cullen, two very distinguished and highly regarded individuals, were selected to undertake the review.

Their Report, and the legislation that was based upon it – the Intelligence and Security Act 2017 – intentionally created a level of transparency and openness about our work that had previously not existed.

In fact, the reviewers stated in the Report's introduction that they saw the review as an opportunity to raise public awareness about the intelligence and security agencies' work.

The Report was unclassified and was made publicly available. It gave people access to information about what the Service and the Bureau do, why we do it and how we do it, which in many cases had not previously been described publicly. For example, the Report talked about the NZSIS's human intelligence activities – also referred to as HUMINT. That was the first time that HUMINT had been referred to publicly.

The Report is a great example of the balance that can be struck in providing the public with information about the nature of intelligence activity without compromising that activity.

The Intelligence Community contributed to the review and the subsequent legislative public consultation process by providing a number of case studies. Those case studies were a mix of actual cases and hypotheticals, which helped to give people a clear understanding of the context in which we might need certain powers or functions, and how we might conduct ourselves. They were unclassified and were published on the Department of Prime Minister and Cabinet website.

The case studies really shone a light on specific aspects of our work for the first time. For the first time, we gave examples of our counter-espionage work. Espionage is the act of obtaining confidential information by covert means. Espionage is traditionally associated with states stealing secrets from other governments, but the Report revealed that espionage is now also being conducted against New Zealand businesses.

We described a case concerning some undeclared foreign intelligence officers working in New Zealand, who had displayed an enduring interest in a prominent New Zealand private sector entity. The entity had been the subject of both traditional human and cyber espionage by the foreign intelligence service. NZSIS had engaged the New Zealand entity to provide a defensive briefing and had discussed with them the espionage threat posed by foreign intelligence service. GCSB had also provided advice and support.

That is just one of many case studies included in the Report. The Report therefore represented a significant flinging open of the doors of the agencies, and the Intelligence and Security Bill maintained that approach. The Bill was referred to the Foreign Affairs, Defence and Trade Committee of Parliament (rather than the secret Intelligence and Security Committee) and followed a normal select committee process, including the consideration of public submissions.

Interestingly there was a very small number of public submissions – I think fewer than 60 – which suggests that the public was broadly comfortable with the explanatory information they had been given and the overall balance of powers and constraints provided in the legislation.

On 28 March 2017, the Intelligence and Security Act was passed and came fully into force in September.

Some important principles have been carried forward from our earlier legislation (although in some cases these provisions apply for the first time to the GCSB):

- For example, section 16 continues to state that the agencies are not law enforcement agencies.
- Section 17 continues to provide that the agencies must act in accordance with New Zealand law and all human rights obligations recognised by New Zealand law; independently and impartially; with integrity and professionalism; and in a manner that facilitates effective democratic oversight.
- Section 18 provides that the agencies must be free from improper influence and be politically neutral.

- Section 19 states that the activities of the agencies must not limit the right of freedom of expression in New Zealand.
- Section 20 continues the obligation on the Directors-General of the agencies to keep the Leader of the Opposition regularly informed about matters relating to the functions of the agencies.

The Act sets out our objectives and functions in a more transparent way. The Service and the Bureau have almost identical national security objectives, functions and powers.

We contribute to the protection of New Zealand's national security, its international relations and well-being, and its economic well-being.

We achieve these objectives by collecting, analysing and communicating intelligence to those who need to know it. We provide protective security services, advice and assistance. We cooperate with other public authorities (such as Police, and NZDF) to facilitate their functions.

While NZSIS's and GCSB's objectives and functions are largely the same, the Act makes clear that we deploy different and complementary capabilities in relation to those objectives and functions. In the case of the Service, we deploy human intelligence capabilities, and in the case of the Bureau, signals intelligence and cybersecurity capabilities.

The ISA provides a much clearer authorising framework. The Act states more clearly what we do under a warrant, including any human intelligence activity that would otherwise be unlawful.

The Act makes it easier for people to understand the two different types of warrants we use, and the approvals that are required.

Type 1 warrants relate to New Zealand citizens or permanent residents. To obtain a type one warrant, there is a 'triple lock' process. The warrant is issued by the Minister and a Commissioner of Intelligence Warrants. It is then reviewed by the Inspector-General.

Type 2 warrants relate to foreign citizens. A type two warrant is issued by the Minister alone, and is also reviewed by the Inspector-General after it is issued.

You may recall my earlier comment about why statutory authorisation should not be provided for activity that is already lawful. The reviewers came up with a clever mechanism for regulating our activities, including some of our lawful activities. That mechanism is the Ministerial Policy Statement – or MPS.

The ISA provides that the Minister must issue MPSs across a range of operational activities. An MPS sets out the Minister's expectations and guidance for the agencies as to how certain activities, necessary for us to perform our functions under the Act, should be carried out.

We must apply the guidance and principles articulated in the MPS when we plan and carry out the activities to which each MPS relates. That in turn provides the framework for good internal decision making and assists the Office of the Inspector-General with its oversight function.

The MPSs were drafted for the Minister by the Department of the Prime Minister and Cabinet, after consultation with NZSIS and GCSB. DPMC also consulted the Inspector-General of Intelligence and Security, the Office of the Ombudsmen, the Privacy Commissioner, and other relevant agencies such as Ministry of Foreign Affairs and Trade, the Ministry of Justice, and the New Zealand Police.

Eleven MPSs are now in effect. Very briefly, they provide guidance as to the conduct of the following activities:

- Conducting surveillance in a public place
- Conducting surveillance activities in accordance with an exemption from the Land Transport (Road User) Rule 2004
- Requesting information from other agencies, both in the public and private sectors
- Requesting information lawfully from agencies or individuals when we do not have a warrant and we are therefore asking people to share information voluntarily
- Obtaining and using publicly available information (for example, open source information that is available on the internet)

- Creating and maintaining a legal entity such as a company without revealing its connection to NZSIS
- Our staff acquiring and maintaining assumed identities to give them cover so that they can undertake their work
- Our staff making false or misleading representations about being employed with an intelligence and security agency (which is also about our staff maintaining cover)
- How information obtained by GCSB and NZSIS is managed, including the retention and destruction of that information
- How the New Zealand intelligence and security agencies cooperate with overseas public authorities (in particular, to ensure that we meet our human rights obligations under New Zealand law)
- How GCSB provides information assurance and cybersecurity support to an organisation, with the consent of that organisation.

These MPSs cover some very significant ground. They are unclassified documents, which are publicly available through our website, the GCSB website and the New Zealand Intelligence Community website.

As well as the Ministerial Policy Statements, there a number of other operational activities that are either new to us or that are articulated and made public for the first time.

The first is Direct Access Agreements. Direct Access Agreements allow an intelligence agency to access information from other agencies directly, so they are very important. The ISA provides that Ministers may agree to allow direct access, but they must sign a Direct Access Agreement, setting out in detail the constraints and procedural requirements governing the access.

Two Agreements have been entered into so far, relating to Customs and Immigration New Zealand databases. The Agreements are available on our website and the website of the relevant agency.

The Act also introduces a new regime for intelligence agencies to obtain business records from telecommunication and financial service providers. Previously, those companies provided information to us on a voluntary basis. They understood that we needed the information for the purposes of investigating threats to national security, and that they could provide the information properly under an exemption to the Privacy Act. Nonetheless the voluntary approach was becoming more and more difficult to sustain. The telcos and banks were trying to balance the competing interests of national security and customer privacy. The Act resolves this difficulty by enabling an intelligence agency to compel a telecommunication or financial service provider to release certain records, with the approval of the Minister and a Commissioner of Intelligence Warrants. This provision formalises the basis on which information is provided and makes the process much more transparent to customers and the public generally.

For the first time, our legislation provides for NZSIS to use cover and assumed identities to carry out our work. Although people have probably been aware that the NZSIS would use cover identities, this essential practice had no legislative basis until now.

The ISA made amendments to the Protected Disclosures Act 2000 as it relates to the disclosure of classified information and information about activities of an intelligence agency. Such disclosures are commonly referred to as "whistle-blowing."

The amendments mean that for disclosures of classified information, or information relating to the activities of an intelligence and security agency, organisations are required to put in place a number of internal procedures.

The provisions make clear that the Inspector-General of Intelligence and Security is the only "appropriate authority" for protected disclosures relating to the intelligence agencies. The provisions also ensure that disclosures are made to people who have the appropriate security clearance and who are authorised to have access to that information. The ISA also continues the existing protections for employees who bring any matter to the attention of the Inspector-General.

These provisions are extremely important to the agencies, as well as the public. They mean that if a staff member has concerns about any aspect of an intelligence agency's work, there is a route to raise the concerns that is independent, effective, safe to the staff member, and at the same time protects national security equities. We regularly remind our staff that they can make protected disclosures to the Inspector-General if they have any concerns about the lawfulness or propriety of any of our activity.

This brings me to oversight. The new Act continues to provide strong oversight of both intelligence agencies.

Most information about our work, by necessity, is classified. We do not reveal a lot of what we do publicly in the same way as most other public sector agencies. In these circumstances, effective oversight of our activities is essential to provide New Zealanders and the government with confidence that we are conducting ourselves lawfully.

There are three types of oversight of the agencies.

- The Office of the Inspector-General of Intelligence and Security (or the "Office of the IGIS" as it is sometimes known) is the key oversight body of the New Zealand intelligence agencies. The IGIS inspects key documents, and reviews the activities of the agencies on a continuing basis. The office also investigates public complaints about the activities of the intelligence agencies.

The IGIS has full, direct access to our information and records, both operational and corporate. The intelligence agencies provide information and resources to support IGIS investigations and queries.

The Inspector-General always produces unclassified versions of her reports on our work, which are published on her website for anyone to read.

The agencies meet regularly with staff from the Office of the IGIS to discuss issues. We involve them early on as we design processes, systems, and authorising documents, to ensure that the balance between security needs and human rights is struck in a way that we all accept. There is some natural tension in this process, which is healthy. It requires a culture where all are willing to listen and understand each other's point of view. Where we cannot reach agreement, we seek a definitive view from the Solicitor-General, who provides a binding opinion. This process, to my mind, involves a mature exchange of perspectives that results in a well balanced outcome.

- The second oversight body is the Intelligence and Security Committee, which provides parliamentary oversight of the intelligence agencies. The Committee examines issues like organisational efficiency and efficacy, budget, expenditure and policy.

The Committee is made up of members of Parliament representing both the Government and the Opposition - all parties.

- Thirdly, like all public service agencies, the NZSIS is subject to the Ombudsmen Act, the Official Information Act and the Privacy Act.

When NZSIS receives requests for information we try to be as open as possible without compromising security. Due to security and privacy concerns, we cannot always be forthcoming with information. When we cannot release material, we try to provide as much information as possible and clearly explain why we have given a particular response.

Under the previous Act NZSIS was exempt from nearly all of the Information Privacy Principles under the Privacy Act. We are now subject to more Privacy Act provisions than we have been previously. We are still exempt from some provisions, for national security reasons, but the exemptions are much more limited.

We continue to have the ability to give a “neither confirm nor deny” response in relation to requests for information under the Official Information Act and the Privacy Act. Such a response is sometimes necessary from a national security point of view. NZSIS has, in the past, been the subject of orchestrated requests from people of security concern who are trying to find out more about NZSIS-specific areas of investigation. NZSIS does not always know who is making a bona fide request and who is not.

The Office of the Ombudsmen and the Office of the Privacy Commissioner provide important oversight of the work we do. If a member of the public is not satisfied with the NZSIS’s response, they may seek a review from the Ombudsman or the Privacy Commissioner. The Chief Ombudsman and the Privacy Commissioner and a number of their staff have TOP SECRET security clearances, and I really appreciate the thoughtful and constructive approach they bring to our issues. In particular, I am grateful that they understand that we are a busy, complex, operational agency and that their recommendations need to balance practicality and workability with principle.

The last thing I will mention about the new legislation – but by no means the least – is that under the ISA, the NZSIS has become a public service department.

We had been behaving like one as much as possible already (for example, my appointment process was managed by the State Services Commissioner, who also reviewed my performance), but now, like Pinocchio becoming a “real boy,” NZSIS is a “real public service department.” The Public Service Code of Conduct applies to us now. My staff can belong to a union, and they can pursue employment grievances through the Employment Court.

I’m sure you can see that the journey that we have been on, as it relates to transparency and openness, has been very significant indeed.

The media and the public now have access to a lot of information about us and our work, through documents like the Independent Review, the legislation, and the websites of the agencies and the Inspector-General. GCSB's Director-General Andrew Hampton and I are committed to continuing to speak publicly and to make ourselves available, as appropriate, to the media. Our intention is to be as open and accountable as possible.

As I have said, there are limits to what we can say. And that brings me to one other aspect of power imbalance, from the perspective of an intelligence agency. One enormously frustrating aspect of our work is that mostly we cannot put the details of the work we do into the public domain. When we provide critical intelligence to Police that helps to disrupt aspiring terrorists, the fact of our involvement cannot be revealed because it would compromise our equities. When we warn agencies that they are the targets of foreign espionage or covert influence operations, that must remain secret.

We are sometimes criticised unfairly in public, generally because only partial information is available. Sometimes the inaccuracy of the information trotted out by commentators is quite breathtaking. Unfortunately, we often cannot respond at all, especially on speculation concerning alleged targets or operations, let alone throwing open the classified files that would give the true and complete picture – which I would often love to do!

So secrecy cuts both ways and often does not work in our favour. While secrecy might be seen as protecting the agencies from public scrutiny, it can also prevent us from demonstrating our value and our professionalism to a partially informed public.

This is another area where independent oversight bodies such as ombudsmen can be really helpful. When independent oversight bodies see good work and best practice in agencies, you can describe what you see. Where it is deserved it rewards the agencies for the efforts we make to be lawful and compliant, and has the effect of building public understanding and confidence at the same time.

Finding the right balance of secrecy, openness, and oversight will be an ongoing process in liberal democracies like New Zealand. But there is no doubt in my mind that we are at a good point in the journey. My successor will have a much easier time working out what kind of organisation he or she is applying to lead. It will be evident to him or her that an episode of Homeland is not a very true reflection of the Service's work, and that James Bond would be unlikely to get a job with us.

More importantly, the people of New Zealand are now much better placed to participate in the ongoing discourse about the work of intelligence and security agencies. That can only be positive for the intelligence community and the public.

Our journey demonstrates that the checks and balances can and should be reviewed and recalibrated from time to time. Public information, transparency and oversight are critical in this process.

In our case we have achieved an outcome that is:

- good for the public, which is better informed;
- good for the intelligence agencies, which are better equipped to deal with national security threats; and
- ultimately good for New Zealand, because the country has become more secure without the compromise of our values.

Thank you.

The Role of Security Intelligence Agencies – Some Reflections

Address by Rebecca Kitteridge, Director-General of Security
Wellington Rotary Club
29 April 2019

Introduction

On Friday the 15th of March, New Zealand suffered a terrorist attack that was unprecedented in this country and sent shock waves around the world. The slaughter of innocent people praying peacefully in the Masjid al-Noor and Linwood Mosques – those beautiful places of worship – devastated scores of lives and caused a profound outpouring of grief.

In the immediate aftermath of the attacks, the obvious questions were “How could this happen? Could it have been stopped? Did anybody know about the attacker?”

A Royal Commission of Inquiry has been established to ensure that those important questions are answered fully and independently. I was one of the agency heads who requested such an inquiry. I knew that it was the only way that the families and the public would be assured that all the hard questions would be asked and that light would be shone into every corner. Such independent scrutiny matters hugely to an agency like ours, because we depend on public confidence, understanding and democratically sanctioned legal authority to do our work.

Except for the information that is already in the public domain I will not be saying anything today about work of the New Zealand Security Intelligence Service before the mosque attacks, or what we knew or could have known about the alleged attacker. Those matters are squarely within the Terms of Reference of the Royal Commission of Inquiry, and the information is largely classified in any event.

There are, though, some things I can say today.

- I can tell you a bit about the New Zealand Security Intelligence Service – or NZSIS as it is known.
- I can explain in general terms how intelligence agencies conduct their security intelligence investigations and some of the challenges we face in countering threats in a challenging technological landscape.
- I can talk at a high level about NZSIS’s role in the aftermath of the Christchurch terrorist attacks, and some of the challenges we have faced. (I note that our response post-attacks does not fall within the ambit of the Royal Commission.)
- And I can touch on the challenges and opportunities with which intelligence agencies in western liberal democracies are grappling, particularly in the area of emerging technologies.

What is NZSIS?

First, by way of context, let me tell you a bit about NZSIS.

- NZSIS is a “human intelligence” agency, which means we work primarily through people. By way of contrast, the Government Communications Security Bureau is a “signals intelligence” agency, and works primarily in the electronic sphere.
- Our statutory objectives are to contribute to the protection of New Zealand’s national security, the international relations and well-being of New Zealand, and the economic well-being of New Zealand.
- Our functions include investigating, collecting and reporting on issues relating to New Zealand’s national security, such as counter-terrorism, espionage, foreign interference, and regional stability. We provide this intelligence to a range of customers on a “need to know” basis, including NZ Police, the New Zealand border agencies, the Ministry of Foreign Affairs and Trade, and the New Zealand Defence Force.

- NZSIS also hosts and manage CTAG, the Combined Threat Assessment Group. This multi-agency group constantly scans classified and open source information from both domestic and international sources to produce assessments about the threats of terrorism around the world. Its assessments provide the basis for setting the New Zealand national terrorism threat level, which went from LOW to HIGH following the Christchurch attacks, and is now at MEDIUM.
- NZSIS provides protective security services, advice and assistance to government and key decision makers, with the goal of lifting the overall security culture and capability across government.
- We provide security clearance vetting services across government, to ensure the suitability of government employees to access classified information. We completed 6,150 clearance recommendations last year.
- NZSIS, with GCSB, also conducts national security risk assessments for activities under the Outer Space and High Altitude Activities Act 2017.

So you can see that NZSIS, which has about 335 full time equivalent staff, is a busy and complex little organisation.

How intelligence agencies conduct security intelligence investigations

As I have said, investigating terrorism threats in New Zealand is a significant focus for NZSIS. Our work involves trying to detect threats before they manifest as physical attacks, so that they can be disrupted by the Police.

So how do we undertake our security intelligence investigations? I guess the first thing to say is that we do not look for threats by monitoring every New Zealander's internet usage.

In the weeks following the Christchurch attacks, I was surprised by how many people seemed to think that NZSIS or GCSB were, or should be, monitoring the entire internet. This expectation was surprising to me because, along with the Director-General of the GCSB, I have spent considerable time and effort in the last five years explaining in various forums that the New Zealand intelligence agencies do not monitor New Zealanders' internet usage across the board. To do so would constitute mass surveillance, and would exceed our current authorisations. The constraints on our powers are clear in our legislation, and the fact that we do not conduct mass surveillance of New Zealanders has been confirmed by independent reviewers Sir Michael Cullen and Dame Patsy Reddy.

In addition, consider the volume of data being posted on social media platforms globally. Twitter and Facebook, for example, each host hundreds of millions of posts per day. Even the smaller chatrooms, like 4Chan, host hundreds of thousands of posts per day. Those numbers are increasing exponentially.

Sometimes, though, a person will see a concerning post on the internet, and will refer that post to us. We call that a "lead." Every security investigation starts with a lead. A lead is the initial information that indicates a potential threat to national security. Leads come from a range of sources, including from other NZSIS investigations, from overseas partners, tips from members of the public, or members of various communities speaking to us about their concerns.

Every lead is inquired into, and an assessment is made to determine its credibility as a national security issue. It might be determined to be not credible. It might be referred to another agency, such as the Police. It might become an initial national security investigation, or a full national security investigation.

If a full national security investigation is required, we will conduct that investigation using the intelligence cycle.

- First, any NZSIS investigation must be within the scope of the security and intelligence priorities set by government. The intelligence agencies do not decide our own areas of focus. We investigate matters in accordance with our legislation and the priorities set by government. The details of these priorities are classified, but longstanding focus areas for NZSIS include counter-terrorism, espionage, foreign interference, and regional stability.
- Within these areas of work we have individual investigations. Those investigations aim to understand what particular actors are doing and to provide intelligence about those actors to agencies (like the Police) that can take enforcement action to mitigate the threat.
- The investigator begins by considering a number of questions, or "intelligence requirements", which in a counter-terrorism investigation will likely include intent, capability, access to weapons and credibility of information.

- An assessment will be made about the best and most efficient way to collect the intelligence that will answer the intelligence requirements. Intelligence collection can take various forms, including physical surveillance by specially trained staff, seeking information from human sources, engaging with communities, collecting publicly available information from the internet, obtaining information from partners (including New Zealand agencies and foreign intelligence agencies), and intrusive measures carried out under an intelligence warrant. We use the least intrusive investigative method necessary and proportionate to the threat we are investigating.
- If the only way to collect important intelligence means undertaking activity that would be unlawful (such as telecommunications interception or technical surveillance) we will first seek a warrant. The bar is set high; we do not seek warrants lightly. The warrant application must satisfy the legal tests set out in our legislation, and show that the action we seek to take is both necessary and proportionate. All warrants are issued by the Minister Responsible for NZSIS, and dependent on the type of warrant may have to be jointly issued by a Commissioner of Intelligence Warrants (a former High Court Judge). After they are issued, warrants are reviewed retrospectively by the Inspector-General of Intelligence and Security.
- As the intelligence is collected, it is compiled to create as accurate and comprehensive a picture of the threat as possible. This part of the intelligence cycle involves integrating, evaluating and analysing strands of available information, and distilling them down to the key issues and risks. This process can be very challenging, because usually our targets are actively keeping their activities secret. Through this process we often find that more information is required, in which case the investigator will develop further intelligence requirements for collection. At various points we will take the distilled information and write it up into an intelligence report.
- Our intelligence reports are rigorously reviewed, classified and given to those who have a need to know. Of course, if the intelligence raises

concerns about public safety we connect with the Police immediately so they can determine the next steps.

- Sometimes the agencies that receive our intelligence reporting come back with more questions. These questions may require further intelligence collection, so it is very much a cycle of intelligence collection, analysis, and reporting.

What I have described to you is the basic intelligence cycle, which is aimed at ensuring that we can detect national security threats and work with enforcement agencies to disrupt them.

For completeness, I should add that as well as investigating “known knowns” in accordance with the intelligence cycle, we also work to understand “known unknowns.” This work involves proactively assessing and understanding any areas of threat that may be trending internationally or emerging domestically. As has been said publicly, we had been conducting this kind of assessment in relation to violent right wing extremism, as well as other threat areas, over a nine month period before the Christchurch mosque attacks. That work will, of course, be scrutinised by the Royal Commission of Inquiry.

NZSIS’s role in the aftermath of the Christchurch terrorist attacks

The investigative work that I have been describing is designed to get ahead of threats, and to ensure as far as possible that they do not succeed. But when the thing we dread the most has happened, and an attack has occurred, what then is the role of a security intelligence agency?

I will answer that question in the context of the Christchurch attacks.

On the afternoon of 15 March, I received an urgent call from Mike Bush, the Commissioner of Police. The call from Commissioner Bush was brief but extremely concerning. He described an unfolding shooting situation with multiple fatalities at two Christchurch mosques.

I knew straight away that this was an event of horrific magnitude. And when I saw, a short time later, the attacker's so-called "manifesto," I knew we were dealing with a terrorist attack.

The "manifesto" was significant because of the first step in the intelligence cycle – determining whether NZSIS has a mandate to involve itself under its legislation and the government's security and intelligence priorities.

A mass shooting within New Zealand will not always be a legitimate focus of investigation for NZSIS. NZSIS will only have a role if the shooting is, or appears to be, an act of terrorism (which includes violent extremism). In summary, terrorism involves two elements:

- First: an act, or intention to conduct an act, that is meant to cause death or serious injury to persons (including through damaging property).
- Second: the act is intended to advance an ideological, political, or religious cause. Note, incidentally, that "intent" is ideology-neutral.

You will recall the massacre of 13 people committed by David Gray in Aramoana in 1990. David Gray committed horrible acts of violence, but he did not kill people in order to advance an ideology. Accordingly the Aramoana massacre was not a terrorist attack and was solely a law enforcement matter.

The killings in Christchurch were different. It was almost immediately apparent that there was the intent to advance an ideological cause, with the intent of creating terror in the populace. It was a terrorist act.

The situation in Christchurch was one in which terrible crimes had been committed, and there were ongoing issues of public safety. The Police, therefore, were the lead agency. But because the attacks fulfilled the definition of terrorism, NZSIS had a role to play. Our job in this situation was to provide as much intelligence as possible to support the Police and to detect any further attacks.

The immediate intelligence requirements were:

- What do we know about the alleged attacker?
- Is he working alone, or is he part of a group?
- Is this one of a number of planned attacks?
- Will this attack inspire or provoke other attacks?

You may recall that the situation was very confusing in the immediate aftermath of the attacks. There were reports of multiple attackers. A number of people were taken into custody by the Police, although all except the alleged attacker were later released. There were also reports of multiple attack sites, including stories about a gunman at Christchurch Hospital and a bomb scare at Britomart train station in Auckland.

NZSIS went into full-scale response mode, immediately. One of the most humbling and gratifying aspects of my role is the quality and commitment of the people who choose to work for NZSIS. They are highly motivated by the spirit of service to New Zealand, and the mission of keeping New Zealand and New Zealanders safe and secure.

The moment we learned of the attacks, NZSIS stood up a response team that worked shifts 24/7 starting that night. The investigations fell naturally into three areas:

- First, getting a complete picture of the alleged attacker, finding out everything possible about him and his plans, with an immediate focus on whether he was part of a group and whether any other attacks were planned.
- Second, reviewing everything we knew about extreme right-wing groups in New Zealand, to detect any "copycat attacks" inspired by the Christchurch attacks.

- And third, detecting any suggestion of a revenge attack either in New Zealand or against New Zealand interests offshore – and you may recall that ISIS quickly called for such revenge attacks.

In all of these areas, we have worked, and continue to work, extremely closely with our Police colleagues. We were supported in our work by GCSB, which assisted us through its technical capabilities and links with foreign intelligence partners. NZSIS too engaged with international counterparts around the world, partly because the alleged attacker was an Australian who had travelled widely before the attacks, and partly because the possibility of copycat or revenge attacks is an international issue.

Even though the alleged attacker was not a New Zealander, the Christchurch attacks prompted many New Zealanders to contact either the Police or NZSIS to report concerns about people who had expressed racist, Nazi, identitarian, or white supremacist views. In the days following the attacks NZSIS received hundreds and hundreds of calls and messages, as did Police. Each call was a lead that needed to be investigated, deconflicted with Police, and triaged into high, medium or low priority depending on the information to hand – a very challenging task given the level of public alarm and the sketchy nature of much of the information provided.

I can't speak highly enough of the selfless dedication of my staff, as they worked through this process day and night. It is stressful work to assess the significance of incomplete information. As they do every day, my staff bore the weight of potentially terrible consequences if they missed something or made a line call that turned out to be incorrect. But they are intelligent, conscientious people who are well trained and follow proper systems. They kept working through the leads.

At the same time as all of this was going on, there was an understandable demand for information from the media about what NZSIS knew or did not know about the alleged attacker, and what work we had been doing in the area of violent right wing extremism before the attacks. It is understandable that people were looking for certainty and

answers. In the immediate aftermath of the attack the country was in agony, and angry.

We were able to release some basic information – that the alleged attacker was not known as a person of national security concern to us, or to NZ Police, or our Australian counterparts; and that NZSIS had been looking specifically at violent right wing extremism for about nine months before the attacks. Anything further than that immediately took us into the realm of classified intelligence, which we could not disclose publicly.

Media reports assuming that there had been an intelligence failure were tough for me and my staff. I am a person whose default setting is openness, so it was frustrating to me that in these circumstances we could not put all the relevant intelligence into the public domain. Unfortunately, revealing information about our work would make us less effective in the future.

It is understandable that the information vacuum has tended to be filled with a range of speculative conclusions. But often those conclusions have been inaccurate, and dealing with that has not been easy for me or my staff.

Please don't get me wrong. I am not saying there was or was not a failure on the part of the Service or any other agency – that is for the Royal Commission to determine. But until the Commission issues its report it is not fair to make any assumptions.

In the case of the Christchurch mosque attacks, the alleged attacker was not known to us. But even where an attacker is known to an intelligence agency, experience in other countries has shown that that fact alone does not necessarily indicate an intelligence failure.

Every day around the world security intelligence investigators are sifting through strands of intelligence to build a complete intelligence picture of thousands of people who would do us harm and who are doing everything they can to avoid detection.

UNCLASSIFIED

This process is always challenging, but particularly so in the online world where lots of people espouse extreme ideologies. A surprising number of those people speak casually in favour of violence, but in almost every case it is just talk, or use of irony, or an unpleasant brand of humour – there is no indication of actual planning or preparation. Some use their real names; many do not. In the online world, identities and geographical locations may be obscured. And many people hide their most extreme rhetoric in encrypted chatrooms.

So even where an intelligence agency has a lead (such as an actual name or a user name) it can be very challenging to assess the extent to which a person is a national security threat. These kinds of situations require fine judgements about intent and capability based on often imperfect intelligence.

It is entirely possible that an intelligence agency might assess a person who espouses extremist rhetoric, and determine on the basis of all the available intelligence that the person is not a terrorist threat. Agencies cannot use their limited resources to monitor people who are just venting. Extremist rhetoric may be disturbing but there is a very high bar before it will be illegal, let alone constitute terrorism. Intelligence agencies like NZSIS do not have the legal justification or the resources to maintain warranted coverage over a person espousing extremist ideologies in the absence of a link to violence. In these circumstances we may conclude the investigation, although we may periodically review the case.

A subsequent attack by an extremist who has been assessed in this way by an intelligence agency will not necessarily mean there was an intelligence failure. Perhaps the extremist became inspired to commit violence after the investigation concluded, or perhaps the intelligence agency's understanding of the person was imperfect because critical intelligence was hidden from the agency. There have been many such cases around the world.

In these circumstances the intelligence agency is highly unlikely to be able to explain publicly everything it did to obtain intelligence about the person, and why the attacker was assessed not to be a terrorist. That kind of classified information would be invaluable to those who wish to evade detection. Instead there will generally need to be an independent review or inquiry, held in the classified domain, to assess the adequacy of the agency's actions.

At this time an intelligence agency will feel acutely a sense of agony that an attack has succeeded, and a sense of determination to apply any lessons so that similar attacks can be prevented in the future.

Lessons, challenges and opportunities

The importance of learning from an attack is hugely important. Attacks inevitably reveal vulnerabilities in our systems or societies. How far we go to tackle those vulnerabilities is a matter for public debate. The lessons to be learned from the Christchurch mosque attacks will form part of the report of the Royal Commission of Inquiry, and that will be invaluable.

Some of the challenges are already obvious. Encryption of sites, chatrooms, apps and other platforms (including gaming) is a huge challenge for all security and law enforcement agencies. The use of social media to spread extremist material and to recruit to terrorist causes is a worldwide issue. The widespread use of anonymised identities online makes assessing the credibility of threats extremely difficult. Compelling or encouraging technology companies to cooperate with law enforcement and intelligence agencies is an ongoing challenge – particularly where they are located in a foreign jurisdiction. And although it is sometimes possible to work constructively with larger providers in like-minded jurisdictions subject to the rule of law, that is not the case where content originates from less reputable locations.

These are global issues. Many jurisdictions and international bodies are debating the extent to which law enforcement and intelligence agencies should be able to require access to information online, including the so-

called “dark web,” encrypted sites and apps; and where to find the balance between state access and privacy. Right now the internet is like the Wild West in the 1800s – an expanding domain where application of law proves challenging to an extent that most of us would find completely unacceptable in the physical world. It remains to be seen whether the public will continue to tolerate the licence to operate afforded to criminals and terrorists by the online world. Global leadership is required to solve this global problem. Sadly, the attacks in Christchurch have given New Zealand a compelling and legitimate role in building support for a concerted push for change.

New technologies offer the intelligence agencies opportunities as well as challenges. An important policy area being worked through in other western liberal democracies concerns data sharing and data analytics. As we all know, commercial entities collect, analyse and exploit our personal data for financial gain. The intelligence agencies, with appropriate legal authorities, constraints and oversight, can use similar technologies to tip the odds further in favour of detecting terrorist and other national security threats.

As Andrew Parker, the head of MI5, said in a recent article in The Times:

“Used in combination with knowledge from our behavioural science experts, [data analytics and related technologies] will give us an earlier and richer picture of our cases. [Data analytics] could also help us spot more quickly when individuals known to us from the past re-engage with terrorism. We do not have the resources or the legal justification to actively monitor those ... individuals. The challenge we are addressing is how to detect signs of developing intent.”

These matters are within the terms of reference of the Royal Commission of Inquiry. Their consideration of the issues will be informed by a range of perspectives, and any recommendations they make will be a measured and useful contribution to the public discussion.

In the meantime, I have a lot of confidence in the commitment of my talented staff to continue to do everything within their power to keep New Zealand safe and secure. I hope I have left you with a better understanding of the way they do their work.

Conclusion

I have described to you some of the challenges we face, and I will finish with something of a challenge to you. It is about how you can help.

To some extent this means being a bit less complacent, and a bit more vigilant. As I have explained, NZSIS relies a great deal on the help and support of the New Zealand public, and every citizen can help us to keep the country safe by providing us with leads to investigate if they see activity of concern.

In the end, though, national security is a much bigger task than NZSIS – or indeed any government agency – can tackle alone. Every person in this country has the responsibility of ensuring that New Zealand is not just diverse, but truly inclusive. Taking active steps to build social cohesion in our communities is probably the best line of defence, and

UNCLASSIFIED

the most useful thing that you can do to help us to keep New Zealand safe.

Thank you.

UNCLASSIFIED



New Zealand
Security Intelligence
Service
Te Pā Whakamarumarū

UNCLASSIFIED

UNCLASSIFIED

Our Role

The NZSIS protects NZ and its people from harm and enhances NZ's economic security

We do this by working to ensure that:

- NZ's institutions are secure;
- The privacy and safety of New Zealanders is maintained;
- New Zealanders' democratic rights and freedoms are protected; and,
- We contribute to international security.

UNCLASSIFIED

UNCLASSIFIED

How we work

- The NZSIS is a 'Human Intelligence' ('HUMINT') agency
- HUMINT can be derived from:
 - members of the public willingly sharing information directly with us
 - a person actively seeking or sharing information at the behest of the NZSIS
 - interviews of people of security concern or vetting candidates
 - observations of the activities of a target



New Zealand
Security Intelligence
Service
Te Pihikete Takekōwhiri

UNCLASSIFIED

- We are adept at gathering intelligence from and about people as opposed to focussing solely on using technology to collect information. Our capability in this field distinguishes us from the NZDF and the GCSB in terms of how we gather security intelligence information.
- 'Human Intelligence' is about people interacting with people. It can be derived from members of the public sharing information directly with us, a person actively seeking information at the request of the NZSIS or from interviews of people of security concern.

UNCLASSIFIED

Partnerships are Key

- NZSIS collect and provide security and intelligence advice to the Government and public agencies
- International alliances are fundamental to our work

Importantly: Intelligence work is not law enforcement and the NZSIS is not a law enforcement agency



New Zealand
Security Intelligence
Service
Te Pū Whakamāramaru

UNCLASSIFIED

- We have extensive engagement with Police, NZDF, Customs, Ministry of Primary Industries Immigration and other agencies that is characterised by two-way sharing of intelligence, direct support for operational activities, and the sharing of capabilities and training. We also provide advice to other agencies on matters of security, including: providing protective security advice and security screening services to government, advising officials about the risks with being posted overseas and providing advice to other agencies about national security.
- The 5-Eyes partnership comprises our most significant intelligence relationships and provides NZ with access to advanced technology which New Zealand could never hope to emulate by itself. We also get access to the skills, training programmes, professional standards, free consultancy, and millions of dollars' worth of equipment.
- Collecting intelligence is about identifying threats to national security as early as possible and before they reach the threshold of criminal offending. We have no powers of enforcement; we communicate intelligence so others can take action.

UNCLASSIFIED

Threats to New Zealand

1. Terrorism



2. Espionage



3. Cyber Attack



4. Proliferation



5. Regional Instability



6. Arrival of an individual or groups of individuals of security concern



New Zealand
Security Intelligence
Service
Te Pū Wiriwhiri

UNCLASSIFIED

Terrorism: Terrorism is an ideologically, politically, or religiously motivated violent act intended to induce terror in the population and/or coerce a government or other authority. Terrorism events can threaten the safety of New Zealanders and New Zealand interests either on or offshore.

Espionage: Acts of espionage, covert interference, influence, sabotage, and subversion that threaten the security and effectiveness of NZ's Government and threaten NZ's economic interests and international well-being, and the integrity of business. These may be carried out, directed, and/or sponsored by foreign states or by non-state actors, both within New Zealand and offshore.

Cyber Attack: An activity that threatens or impacts the confidentiality availability and integrity of data and information infrastructure, and operations and services that depend on such. These acts may be carried out foreign governments, private sector company or individual.

Proliferation: Threats to New Zealand's interests from the development, deployment and use of weapons of mass destruction (WMD) and from the proliferation of relevant material and expertise. May include New Zealand actors unwittingly supplying highly sensitive technology to a foreign WMD development programme.

Regional instability: Political and social disorder in a Pacific state or across the region could threaten the security of the region and impact negatively on New Zealand's

interests. This could include a political crisis, such as a coup, that could create tension between states in the region, including New Zealand.

Arrival: An individual (or group) of national security concern (particularly terrorism) presents at the border and requires an immigration decision about eligibility to enter New Zealand

UNCLASSIFIED

NZSIS has three primary outcomes

1. New Zealanders are safe
2. New Zealand's key institutions are protected
3. New Zealand's national advantage is promoted

UNCLASSIFIED

UNCLASSIFIED

New Zealanders are safer

- Counter threats from extremism and terrorism
- Security screening to strengthen New Zealand's border
- Support for deployments and events



New Zealand
Security Intelligence
Service
Te Pū Whakamārama

UNCLASSIFIED

- We identify, and provide advice to other agencies about countering, a number of threats including: terrorism and violent extremism, espionage conducted by other states, the proliferation of weapons of mass-destruction and hostile cyber-activities. We work with other agencies, such as the Police, to prevent threats to security progressing to acts of violence or espionage.
- We work closely with partners such as the Department of Internal Affairs and Immigration New Zealand to screen those people visiting, or seeking residency or citizenship who may pose a risk to national security. We do this by gathering information about them from police records, travel information, interviews and other sources.

UNCLASSIFIED

Key Institutions are protected

- Mitigate espionage and hostile foreign intelligence threats
- Protect people, information and assets
- Security clearance vetting



New Zealand
Security Intelligence
Service
Te Pā Whakamārama

UNCLASSIFIED

- Through the Protective Security Requirements (PSR) we assist agencies to meet the Government's expectations of the public sector for managing personnel, physical and information security and supporting agencies to better manage risks and assure continuity of service delivery.
- The NZSIS also vets individuals seeking security clearances across government to ensure they are trustworthy not exposed to influence from other states. We do this by interviewing them, checking information they provide about themselves and by contacting referees.

UNCLASSIFIED

National advantage is promoted

- Enhance regional stability and security
- Contribute to international security
- Enable better policy and geo-political decision making



New Zealand
Security Intelligence
Service
Te Pū Whakassumatahi

UNCLASSIFIED

- We seek to identify those people or states which threaten our regional security, work out what they are doing or intending to do, and what their true agendas might be towards New Zealand or our partners. Based on the intelligence we gather, we provide advice to other government agencies such as the NZDF or the Ministry of Foreign Affairs and Trade or (where appropriate) to international partners.

Provide advice to other government agencies such as the NZDF or the Ministry of Foreign Affairs and Trade or (where appropriate) to international partners

Identify people or states which threaten our regional security

UNCLASSIFIED

New Zealand Intelligence Community (NZIC)

Goal: An agile, coordinated and customer-focused community that can sustainably meet the Government's protective security and intelligence priorities

The New Zealand Intelligence Community knows we have achieved this goal when....



New Zealand
Security Intelligence
Service
Te Pū Whakamārama

UNCLASSIFIED

UNCLASSIFIED

NZIC: What Success Looks Like

- Evolved into a highly customer-focused and responsive community
- Increased NZIC operational collaboration
- Capability investment transformation
- Collectively enhanced the security of the NZIC
- Enhanced the trust and confidence of New Zealanders
- Supported delivery of Better Public Service priority results #9 and #10
- Enabled continued access to world-wide intelligence relevant to New Zealand



New Zealand
Security Intelligence
Service
Te Pa Whakaitiaki

UNCLASSIFIED

- Evolved into a highly customer-focused and responsive community through the introduction of a new relationship management model, collaborative sector-wide approach to delivering New Zealand's intelligence priorities and better matching of customer intelligence demand with NZIC information supply
- Increased NZIC operational collaboration (consistent with legislative parameters) to meet more effectively the government's security and intelligence priorities
- Collectively ensured that any capability investment transforms the ability of the NZIC to meet government priorities through a sequenced growth plan and effective governance and performance oversight
- Collectively enhanced the security of the NZIC
- Enhancing the trust and confidence of New Zealanders, including through implementation of changes arising out of the 2015 legislated review of the intelligence agencies
- Supported delivery of Better Public Service priority results #9 and #10 through leadership of the Protective Security Requirements initiative and project CORTEX
- Enabled continued access to world-wide intelligence relevant to New Zealand's prosperity and security through the use of strategic partnerships