1/7/08

OPENING ADDRESS – WARREN TUCKER

SiD SUPERSTRUCTURE GROUP INTELLIGENCE SEMINAR

WELLINGTON, 23 MAY 2007

Ladies and Gentlemen, Friends and Colleagues,

It is my very real privilege to be here with you this morning to provide the opening keynote address for this New Zealand Intelligence Seminar. I must say that I was both delighted and honoured when Lyndsay Gault asked me to do this. I met with Lyndsay and Bob Chambers shortly afterwards, and was impressed by their vision and enthusiasm for this seminar. I would like to take this opportunity to thank Lyndsay and his team at the Superstructure Group for their commitment to this vision, and for their efforts and energy in organising today's events.

I think that the organisers have been very canny in selecting the theme for today. "Cooperative Intelligence" is sufficiently broad in its compass to enable a very full range of issues, case studies, and presentations to be covered. It is also very salient in today's world, with its demonstrated and very real threat of international terrorism in particular forcing some very real changes in the way we intelligence practitioners work and collaborate. This is particularly true for our closest partners –especially in the UK and the US – but it also applies here in New Zealand.

I'd like to pick up a number of separate strands which each link back in different ways to today's theme. My intention is that by the time I gather these various strands together I'll have set the stage for the rest of today's speakers and the events which follow.

Cooperative Intelligence. It seems intuitively obvious that it ought to be a "good thing" to cooperate in the collection, analysis, and dissemination of intelligence. Indeed, most of you will have read the public criticisms of the failure to share critical intelligence across the US Intelligence Community which resulted from the various reviews and enquiries following the shattering and tragic events in New York, Washington DC and Pennsylvania on September 11, 2001.

R - File + attchs.

But intelligence by its very nature is secret. It is collected covertly from those who do not wish us – the authorities – to know of their intentions or capabilities. This applies whether the subject of the intelligence collection activity is an individual or small group of individuals (as is the case with the terrorist cell), or whether it is the intentions or attitude of a foreign government. So, given the inherently secretive character of secret intelligence, there is immediately a tension between the need to maintain the secret, on the one hand, and sharing the secret – or operating in a more open and collaborative manner – on the other.

At the heart of this dilemma lies the paramount need to protect and preserve the sources and methods which are used to collect and render usable this secret intelligence.

This applies whether the source is a human agent, a covert technical operation, or a product of a larger more integrated system such as a signals intelligence collection capability. Sometimes it is the very fact that a capability exists at all which must be protected, rather than merely its detail.

Within one's own country there are further impediments to collaboration in intelligence matters. In the domestic security intelligence field, it seems self-evident that sharing and collaboration is necessary between the intelligence and security services and the law enforcement agencies. But the law enforcement agencies are geared towards making arrests and bringing prosecutions. So, the attitudes, expectations, and indeed the organisational cultures of the law enforcement agencies are quite different from those of the intelligence and security agencies. These differences can be profound inhibitors of collaboration.

And when one adds to all this the international dimensions of sharing very sensitive secret intelligence across national boundaries between different nations, with different legal, judicial, and policy environments, then it is very clear that collaborative intelligence is not actually as self-evident or as straightforward in practice as might first appear to be the case.

So - given what I've just said – what are the drivers which are forcing the changes we see today towards an "imperative to share" rather than a "need to know" approach to secret intelligence?

What are the fundamental differences between our global situation today and that which prevailed during the 40 years of the Cold War?

What are the key drivers of the intelligence process for New Zealand today?

And how do we in New Zealand "measure up" against the benchmarks of best international practice as we know it?

Are there any structural or process gaps which, if addressed, would likely lead to improvements in the way we do our intelligence business here in New Zealand?

And how does all this fit within the framework of broader Government initiatives, such as the e-Government programme and indeed the wider goals for the State Services at large?

These, then, are the various strands which I want to address this morning under my broad heading of "Cooperative Intelligence".

So, in what ways have things changed over the past decade or so in the way we approach the intelligence business, and what are the drivers pushing us towards greater collaboration and cooperation?

When I was in the UK a few weeks ago, I heard a BBC Radio interview programme, entitled "Secrets and Mysteries". This brought together, in a very thoughtful way, discussion with a number of recently retired but very senior and experienced British Government officials. It dealt with the UK's strategy designed to counter the threat of radical Islamist terrorism, and very usefully raised a number of associated issues. These included the differences between the dangers which the UK faces today compared with those of the Cold War era, and also the way in which they differ from the experience of three decades of terrorism in relation to Northern Ireland. If anyone wishes, I have a transcript and would be happy to pass on details afterwards.

One of the participants was Sir David Omand , who is a former Director of GCHQ, former Permanent Head of the Home Office, and most recently the Co-ordinator of Security and Intelligence in the British Cabinet Office – now retired.

Sir David was asked to describe the biggest shift between Cold War intelligence and today's intelligence priorities for the UK. Couching his reply in terms of "secrets and mysteries", he rather neatly summed up the essential differences in the following way:

Quote:

The principal secret in the Cold War was the capability of our adversary. That our intelligence services were able to describe with some considerable degree of accuracy. But what were their intentions? What would they do with their military capability? And that, of course, was the great mystery. In today's world, it's the other way round. Today, we know all too well what the intentions are of those who intend to harm us. But what are their capabilities? Where are they hiding? What weapons do they have? These are mysteries and it's that task, of course, that our security service and our police services have to cover.

Unquote.

Sir David went on to elaborate:

Quote:

And there's one other fundamental difference between then and now. The Cold War was a secret war. Most of the preparations made by the British government were kept from the public because they had to be kept from the enemy. Today it's very different. Today, countering terrorism is a matter for all of government and local government and the voluntary sector and private industry. And the public has to understand what is being done in their name to keep them safe.

Unquote.

Implicit in this, of course, is the notion of cooperation and collaboration, and a "whole-of-government" approach to tackling the very difficult problem of international Islamist terrorism. I'll come back to this a little later.

So now to pick up the question of what are the other drivers which are impelling us towards a more cooperative approach in intelligence.

First, intelligence work is not done in a vacuum. It is shaped and conditioned by the whole context of government's work, and by the international environment. In this respect the international response to the reality and the threat of international Islamist terrorism has been key. On 28 September 2001, just a couple of weeks after the attacks of September 11, the United Nations Security Council unanimously adopted Resolution 1373, which binds all member states.

Resolution 1373 provides a framework for the international response, and calls on all states to take action to prevent and suppress the financing of terrorist acts; to prevent their country from being used to support or facilitate terrorism; to improve co-ordination and information flows between countries; and to set up effective border controls to prevent the movement of terrorists and terrorist groups.

In Resolution 1373 the Security Council also noted with concern the close connection between international terrorism and transnational organised crime, illicit drugs, money-laundering, illegal arms-trafficking, and illegal movement of nuclear, chemical, biological and other potentially deadly materials, and explicitly emphasised – and I quote – "the need to enhance coordination of efforts on national, subregional, regional and international levels in order to strengthen a global response to this serious challenge and threat to international security."

Other drivers for us, beyond those led directly by the UN, result from work undertaken by international organisations of which New Zealand is a member. These include, for example, the World Customs Organisation (WCO), the International Maritime Organisation (IMO), and the International Civil Aviation Organisation (ICAO). And there are other drivers which flow on from specific initiatives by countries such as the United States – for example the Container Security Initiative, and the Proliferation Security Initiative.

Taken together, New Zealand's response has been comprehensive, and includes a raft of legislation as well as specific actions in regard to improved shipping and port security, airport and aircraft security enhancements, and measures such as the implementation of a common global standard on advance passenger information, adopting a biometrics standard, moves to a strengthened passport with electronically secure embedded information, and reform of immigration service policies, processes, and legislation. Many of you will be better acquainted with the detail of this work than I. The essential point, though, is that underpinning all this lies the expectation that New Zealand government departments and agencies will work together in a collaborative and "joined up" manner, rather than taking a narrow departmental viewpoint.

For its part, Government has invested significantly in a number of key areas to provide the wherewithal and resources to give effect to these initiatives. Notable, from my perspective, is the growth in the budgets of the key intelligence and law enforcement services – the NZSIS, the GCSB, New Zealand Police, and New Zealand Customs Service in particular since 2001.

As just one example, my former agency, the Government Communications Security Bureau, more than doubled its budget during the seven years I was Director. The GCSB also had its authorities strengthened and put onto a legislative basis through the enactment of the GCSB Act 2003.

In looking at all these responses to the drivers which followed September 11, it is important to not overlook the New Zealand Defence Force. Significant decisions have been taken in recent years by Government in respect of the Orion fleet upgrade and the Navy (through Project Protector) in particular, as well as the wider range of Army and air transport capabilities which flow from the Long Term Defence Plan.

As an aside, I'd like to mention in passing one outcome of these drivers – which was a result of the Maritime Patrol Review in late 2001. The establishment of the National Maritime Coordination Centre (NMCC), located with Headquarters Joint Forces at Trentham, stands out in my mind as an example which epitomises collaboration and cooperation across a range of quite diverse departments and agencies, and spans the civil/military divide.
The NMCC was established under shared governance and club funding arrangements, under the leadership of Customs, and staffed though secondments from participating departments and agencies. These collaborative arrangements enabled the concept of the NMCC to be validated, and proved the viability of the pilot project under which it was established. The NMCC has recently become formally part of Customs, but the underlying spirit of collaboration and sense of shared purpose remains.

I'd like now to focus in on the framework and the mechanisms – both formal and informal -for the coordination of our intelligence and security work here in New Zealand.

First, it must be said that New Zealand is blessed with some fundamental advantages which result from our small size and our history. The most significant is that we have a unitary system of government, and national Police, Fire and Customs Services. This simplicity of structure confers substantial benefits in enabling collaboration, in implementing security policies, and in responding to events.

Underpinning this is the DESC structure. This is described in some detail in the report by the Controller and Auditor-General entitled "Managing Threats to National Security" of October 2003, which is referred to and quoted from in the brochure publicising this Seminar. I don't want to repeat all that, but having been part of the DESC system for more than a decade now, let me give my perspective on it.

First, a brief description. DESC stands for Domestic and External Security Coordination, and the present DESC system was established in 1987 to replace and broaden the scope of the Intelligence Council and the Committee of Controlling Officials which were its predecessors. Sitting at its head is the Cabinet Committee on Domestic and External Security Coordination (DES), through which key Ministers coordinate and manage the national response to domestic and external security issues affecting New Zealand. At its centre is the Officials' Committee for Domestic and External Security Coordination (ODESC), which coordinates both advice to Ministers and the actions of the various departments and agencies involved. ODESC comes in several flavours, of which for us in this seminar the ODESC(I) – which deals with intelligence coordination matters – is the most relevant. Supporting ODESC is a small but growing Secretariat – DES Group – based in the Department of the Prime Minister and Cabinet, and increasingly taking a leadership role in advancing critical issues.

ODESC(I) membership comprises the Chief Executives of: the Department of the Prime Minister and Cabinet, the Ministry of Foreign Affairs and Trade, the Ministry of Defence, the Chief of Defence Force, the Treasury, the Commissioner of Police, the NZSIS, the GCSB, and the Director EAB and Director DES Group.

To me, the ODESC(I) works very well because it operates in a very collegial manner, with all participants well known to each other and with frequent interactions outside the formal ODESC(I) meetings. It operates at both the strategic level and at the level of specific issues or crises affecting New Zealand. Strategically it examines broader policy questions relating to the work of the New Zealand Intelligence Community, and the NZSIS and the GCSB in particular; examines budget and resource issues; reviews the Statements of Intent and the Annual Reports of the Agencies; and ensures that advice to key Ministers is coordinated in an inter-departmental manner. In this regard it acts informally as part of the web of oversight as well as coordination arrangements for the New Zealand Intelligence Community as a whole and the Agencies in particular.

ODESC(I) also is responsible for ensuring the processes for interdepartmental coordination of the Foreign Intelligence Requirements and Priorities (which in their high-level form are signed off by Ministers via the DES Cabinet Committee); for the National Assessments Committee which meets weekly to provide interdepartmental scrutiny of and debate on the national intelligence assessments usually drafted by EAB; and for the Interdepartmental Committee on Security which provides policy and doctrine on a full range of protective security issues for government departments and agencies.

I should note here that the Foreign Intelligence Requirements process is currently undergoing a process of review and re-invigoration.

Underpinning the formal framework are other, less formal arrangements. For example there are regular meetings bilaterally between the NZSIS and GCSB Directors and – separately - their key operational and intelligence staff, between myself and the Police Commissioner, with key seniors in the Defence Force, with the Comptroller of Customs. The Heads of all the intelligence agencies – NZSIS, GCSB, EAB, and Defence Intelligence, together with Director DES Group, meet periodically in informal session to discuss a range of common issues and concerns.

And sitting alongside ODESC(I) is the Combined Law Agencies Group (CLAG) which meets regularly at both senior (Chief Executive) level and at working level, both in Wellington and in the regions, to share knowledge and understanding of common issues and to coordinate and collaborate while respecting statutory roles and constraints. Many of you will be familiar with CLAG, and we will be hearing more about this later today.

In short, the frameworks, mechanisms, and arrangements – both formal and informal – which exist within New Zealand do, in my view, serve us well to facilitate the sharing and co-ordination of intelligence and domestic security information more generally. Critically, in my view, these mechanisms also enable the respect, trust, and confidence in integrity which are fundamental pre-conditions to fulsome collaboration in the intelligence arena. There are however several ways in which I think these arrangements could be further improved, and I'll come back to this later.

I'd like now to shift gears, and turn our focus to some specifics relating to intelligence – as distinct from the wider security arena and the drivers and processes which govern what we do.

New Zealand is a small, geographically remote country with global interests through its international trade and its strong sense of identity as a good "international citizen". We are strongly committed to working multi-laterally – through the United Nations, for example – and to the rule of international law. We play our part in a wide range of international forums. Through our Defence Force we contribute – albeit in a small way – to a considerable number of international peacekeeping and other endeavours. Our recent deployments to East Timor, Solomon Islands, and Afghanistan are notable examples, although these do not do justice to the actual spread of our Defence Force personnel in various UN and other missions around the globe.

Our Foreign Service is also small by many benchmarks, but our diplomats are active and highly respected for their professionalism, and we have a good spread of diplomatic Missions around the globe also.

So, our small size and geographic remoteness do not mean that we are in any sense isolated from world affairs or the forces of globalisation. Our foreign intelligence interests are, commensurately, broad in their scope. It can be said that our access to global sources of high-quality intelligence through our long-standing and close intelligence partnership arrangements compensates for our small size and lack of intrinsic global reach, and enables New Zealand to be a more active player on the world stage than would otherwise be the case.

But – as I've said publicly on other occasions – New Zealand does not take for granted its access to the very considerable benefits conferred by these long-standing intelligence partnerships. We do play our part, and make important contributions which are valued by our intelligence partners. This dynamic, which has endured for more than 50 years, is underpinned by the fact that each partner sees real net benefit to itself as a result of the partnership, and is therefore committed to collaboration and cooperation in a way which continues to grow the relationship. These arrangements were forged in the crucible of the Second World War, which directly threatened the very existence of the partner nations, and therefore made the imperative to collaborate outweigh and overcome the inhibiting factors which I mentioned earlier, and which would likely have otherwise dominated. So, in a sense, the collaboration with our closest intelligence partners abroad is a consequence of catastrophic world events some 60 years ago, but which has survived and indeed flourished because a self-perpetuating dynamic has been established which encourages and fosters that collaboration through the mutual net benefits which these arrangements confer.

Again – as I've said publicly on previous occasions – I reject categorically any suggestion that the intelligence relationship which we have with any of our partners abroad is in the nature of master-servant, or that we are in any way the "lackeys" of the larger partners.

That, I think, deals with our foreign intelligence needs and arrangements in about as much detail as is appropriate in an open forum such as this. Turning now to the needs and drivers of our domestic intelligence business, I should note that from an NZSIS perspective it is in the public domain that we currently focus our security intelligence efforts on counter terrorism, counter proliferation, and counter espionage. To this I would like to see added counter serious organised crime, particularly serious transnational organised crime. That is a discussion and debate we will have in coming months, as NZSIS undergoes the fundamental transformation and re-organisation on which we are now embarked.

However, in NZSIS our role in the security intelligence field is not confined to merely producing security intelligence reports and passing these on to others for their use as they see fit. Government expects that in this arena, we will produce actionable intelligence which is actioned. We will assess and provide commentary and advice on the implications for security of the issues we deal with. We will provide the pre-emptive secret intelligence which is the key to successful counter-terrorist action. And we will assist, cooperate, and collaborate with other agencies, such as the Police and Customs Service to the fullest extent practicable in order to achieve the public safety and security outcomes which are the responsibility of Government to strive for. We will facilitate and act as the gateway to our international partners for access to security-critical information and intelligence. An important example of this is the so-called Tip-Off database operated by the US' Terrorist Screening Centre, with which I signed a formal agreement for mutual access and sharing a couple of weeks ago in Washington DC.

If I seem to be dwelling on the threat of terrorism, at the expense of the other issues such as counter-proliferation and counter espionage which I mentioned a short while ago, let me elaborate briefly.

To remind, the threat of radical Islamist terrorism internationally is real and demonstrated. Since September 11, 2001, we have had – to name a few – bombings in Bali in October 2002, in Madrid on 11 March 2004, and in London on 7 July 2005. Embassies have been struck. A number of plots have been averted thanks to pre-emptive intelligence successes. Airline travel has been impacted through ever more intrusive security measures. Police with automatic weapons patrol the streets of London, and within the US security forces are visible and pervasive.

New Zealand has, mercifully, so far been spared the spectre of a serious terrorist attack on our soil. As has been said publicly before, we judge that the threat of terrorist attack directed against New Zealand is low, but it is rising steadily as we more systematically investigate a number of areas of concern. Our principal current concern remains to ensure that New Zealand does not become a staging point for a terrorist attack to be launched against others, either here or overseas. However, the overseas experience of the radicalisation of impressionable youth by Islamic extremists, and the implications for our own security in the context of international radical Islamist terrorism, should not be lost on us. The much shorter lead times involved in the radicalisation process which now seem to be the norm overseas is a particularly worrisome trend, because it means that the intelligence process has to be more agile and more focussed and more systematic. No longer can we rely mainly on stationing a set of "pickets" across key points in the domestic landscape to alert us to indicators of security concern. We must work closely and collaboratively with – in particular - the Police in order to gain a "rich picture" of understanding the local dynamics, issues, tensions, and warning signs within communities. The UK experience is that so far this approach has not yet reached its potential, with most prosecutions there having their origins in intelligence that came from overseas, from the intelligence agencies, or from technical means. Considerable effort is however being put into increasing the flow of intelligence coming from communities.

In a recent public lecture entitled "Learning From Experience – Counter Terrorism in the UK Since 9/11", the UK's Deputy Assistant Commissioner at the Metropolitan Police, Peter Clark, had this to say:

Quote:

So what has happened since 9/11? I think it is no exaggeration to say that there has been a complete change in our understanding of the terrorist threat. For 30 years or more we had been facing a deadly campaign of terrorism conducted by utterly ruthless people intent on wreaking death and destruction. But it was different to that which we now face.

Colleagues from around the world often say to me that the long experience that we have in the United Kingdom of combating a terrorist threat must have stood us in good stead. That the experience gained during some 30 years of an Irish terrorist campaign equipped us for the new challenges presented by Al Qaeda and its associated groups. To an extent that is true – but only to an extent. The fact is that the Irish campaign actually operated within a set of parameters that helped shape our response to it.

It was essentially a domestic campaign using conventional weaponry, carried out by terrorists in tightly knit networks who were desperate to avoid capture and certainly had no wish to die. The use of warnings restricted the scale of the carnage, dreadful though it was. The warnings were cynical and often misleading, but by restricting casualties, were a factor in enabling the political process to move forward, however haltingly.

I believe [said Peter Clark] that if you take the reverse of many of these characteristics, you are not far away from describing the threat we face today. It is global in origin, reach and ambition. The networks are large, fluid, mobile and incredibly resilient. We have seen how Al Qaeda has been able to survive a prolonged multi-national assault on its structures, personnel and logistics. It has certainly retained its ability to deliver centrally directed attacks here in the UK. In case after case, the hand of core Al Qaeda can be clearly seen. Arrested leaders or key players are quickly replaced, and disrupted networks will re-form quickly. Suicide has been a frequent feature of attack planning and delivery – a stark contrast with the Irish determination to avoid capture. There is no evidence of looking to restrict casualties. There are no warnings given and the evidence suggests that on the contrary, the intention is frequently to kill as many people as possible. We have seen both conventional and unconventional weaponry and to date, although perhaps this is not for me to judge [said Peter Clark], there has not been an obvious political agenda around which meaningful negotiations can be built.

Unquote.

A sobering statement, and worth our while reflecting on.

Peter Clark goes on to address the question "So what impact has all this had on our response from a law enforcement perspective?" The simple answer, he says, it that it has changed everything.

Again I quote:

No longer can the police service feed off the crumbs falling from the intelligence table. In the past a case would sometimes come to the police after there had been a great deal of investigation by the intelligence agencies. Sometimes we would have little insight into what lay behind the case, and this was often deliberately the case – to protect the evidential investigators from knowledge that could lead them into difficulties when giving their evidence in court. This is no longer acceptable for very sound legal reasons, but it is also not acceptable in terms of public safety.

We can no longer wait until the terrorist is at or near the point of attack before intervening. It might give us the strongest evidence to do so – to capture the terrorist with the gun or the bomb. But the risk to the public in the age of suicide bombers and no notice attacks, is simply too great. So what we have done is to develop a new way of working. The police and the Security Service now work together in every case from a much earlier stage than would ever have happened in the past. The intelligence that is gathered and assessed by the Security Service is in large part the lifeblood of counter terrorism in the UK. Exploiting it is a shared endeavour. Setting joint objectives and agreeing investigative strategies is not exceptional. It has become the daily routine.

Unquote

Stirring words indeed, and very pertinent to today's theme of collaborative intelligence.

I'd like now to return to a couple of points I alluded to earlier, and then to finish.

I mentioned previously, when I was talking about the DESC framework, that there were a couple of areas where I thought we could improve the ways in which we worked. I mentioned one of these at the recent Police Seminar on radicalisation, and I believe strongly that we need to pick it up. Interestingly, in reviewing the key findings of the Auditor-General's 2003 report I see it there too, so I can't claim it as an original idea. However, having been directly involved in establishing the arrangements for setting our Foreign Intelligence Requirements and Priorities more than a decade ago, I came firmly to the view that a similar process would be appropriate for identifying and testing our Domestic Security Intelligence needs and priorities, and subjecting these to the rigour of inter-agency consultation and debate. I believe that while it would be important that NZSIS retain the final say on these, because of its clearly identified statutory responsibilities in this area, the end result of such a collaborative requirements-setting process would be more transparency and better understanding and "buy in" by other agencies such as Police and Customs, as well as arguably a better set of requirements. I know that ASIO moved to such a system about a decade ago when Denis Richardson became Director, because we discussed it during one of my visits to Canberra at that time.

The second area, in which there has been steady if unspectacular progress over the past few years, is in the establishment of a secure computer-based network for the sharing of information and intelligence across the New Zealand Intelligence Community. The so-called New Zealand Intelligence Community Network is designed to perform this role. So far, the focus has been on establishing the secure connectivity between the various agency and departmental networks, but the stage has now been reached where very real benefits are being achieved through secure analyst-to-analyst communication at the desktop. The next step will be to extend this beyond mere connectivity, and to provide for secure and controlled access to relevant data repositories. Experience elsewhere within government – especially from the e-Government programme and its supporting e-GIF framework which specifically focuses on frameworks for interoperability – is that a further step, to focus on collaborative and aligned business processes, will bring further benefits. Again, I note that the Auditor-General made specific recommendations in this regard in his 2003 report. And all this is fully consistent with the wider drive towards "trusted State Services" and "networked State Services" which is being championed by the State Services Commissioner, Dr Mark Prebble!

Taken together, I think I've made a pretty compelling case for continuation of the moves in recent years towards greater collaboration in the way in which we conduct our intelligence business here in New Zealand, despite the intrinsic tensions and difficulties which can impede this. I've quite deliberately set out to cover a fairly broad front, and to set my comments in an international rather than purely New Zealand context. I've sought to come at the topic from several different angles, each of which seemed to arrive at a common destination and which I think provide the reassurance of some degree of coherence in the overall arguments and conclusions. I hope I've set the scene for the rest of today's programme, and I'd be happy now to take any questions or to respond to any comments.