National Security System in 2016

Howard Broad, Deputy Chief Executive – Security and Intelligence Group, DPMC

Massey University National Security Conference, 30 August 2016

Introduction

(1) National Security matters. The first duty of Government is to protect the people. Our recent experience in national security has been a story of earthquake, mine disaster, the Rena maritime grounding and a 1080 thread to food security. More lately we have become worried about international terrorism, cyber attack, superpower rivalry is back with us and our neighbourhood still has a bunch of problems. National security is a broad church of risk.

(2) And so we define the national security outcome as: "… the condition which permits the citizens of a state to go about their daily business free from fear and able to make the most of opportunities to advance their way of life."

(3) We have been going about our daily business lately largely free from fear. And we have been steadily making the most of our opportunities. Our world, though, is changing. You only have to look around you. How we communicate, read and get entertainment, do our banking, shop, and perform so many of our everyday functions – has been upended over the course of half a generation.

(4) The world continues to come to us. We are much more a multi-cultural society with links all over the globe. We look and act differently.

(5) Grasping opportunity means trade. International trade is no longer just about exports and imports. Increasingly global commerce is interlinked and inter-dependent, with rapidly expanding global value chains. Ideas may be born here, with manufacturing elsewhere, drawing on imports from yet another place, - and sales in a further location. Economically we are not an island.

(6) A fast growing segment of our economy is what we term 'commercial services': that component of our services sector which is not tourism/travel and education. Commercial services are services such as legal, accounting, IT, architecture, engineering, film and digital services - to name but a few. Fast growing? Now earning over $4 billion in export revenue. What is significant is that much of this commerce is via the internet. "Security" in this context, is less about traditional barriers such as tariffs or non-tariff-barriers and more about broadband speed and confidence on-line.

(7) And the point? Our global inter-connected-ness means our security is increasingly linked to the security in other countries. Meaning security is not island shaped either.

Threats - Enduring

(8) There's more. The nature of conflict and the way we think about it is changing as well. The identifiable domains of conflict are not two or three - but seven: land, sea, air, space, cyber, money, information. Each of these areas is potentially contested, and in each of them any government needs to be able to clearly and carefully think through its national security posture and response.

(9) Some conflicts in the world appear distant. There are security problems in the sea-lanes around Asia, tensions remain in the Ukraine, the "zone of conflict" that has captured attention running through North Africa, the Middle East and into South Asia, now spawns terrorism elsewhere and has propelled a

major refugee crisis in Europe. In our own South Pacific region we observe risk factors including the impact of climate change, resource depletion, political instability and population movement. The Pacific is family – we can't shirk our responsibilities here. Further south the Antarctica ban on resource exploitation nears an end in 2048 and competition potentially causing conflict may ensue. We watch closely the marketing of New Zealand as a substitute illegal migration destination now that Australia is closed.

(10) Our economic zone (you know, the fourth largest EEZ in the world) is resource rich and difficult to protect. New Zealand companies with valuable intellectual property are vulnerable to theft, vandalism, and commercial espionage. There are many interested in our assets in order to obtain trade and other advantage. Organised crime, with its off-shore links, threatens in several ways.

(11) Terrorism is something that worries us. On traditional grounds the risk is low. Yet is it? Some terrorist conflicts are long standing – think of the PKK, the IRA, and Hezbollah – each seeking legitimacy in Westphalian terms.

(12) Then there is ISIL/Dae'sh – a terrorist venture sourced in a mix of intra/inter-national and sectarian disputes. On the one hand ISIL/Dae'sh seeks a fight to gain and hold ground. On the other it seeks a fight with non-Islam values and people wherever. Thus it inspires extremists to "come join them". Or sends extremists back home to carry the fight there. Now also we seem the self-inspired vulnerable mind just looking for a cause to attach their death wish. Finally, as ISIL/Dae'sh "state" comes under increasing military pressure we see and worry about its ideologically linked seeds growing around the world. Let's be clear we critically understand the point of terrorism; an asymmetrical engagement intending that we change our system of democratic system of government or the policies that we agree upon. To us, this is unacceptable.

Risk Analysis

(13) So what do we make of our risk environment? The first point is that "**states still matter**". The rise of religiously based extremism, or security threats delivered to a nation state by private actors, may tempt us to look away from the actions of nation states as threat actors. These remain a concern. While the world is no longer bi-polar as it was during the Cold War, or unipolar as it was following the Cold War, new actors are emerging to convey threats. Just think of the risks of a nuclear armed North Korea or the concern to trade routes arising from competing claims to the South China Sea. What is true is that an ability to interpret the motivations behind the conduct of international relations is as important as ever.

(14) Secondly, "**geography still matters**". Building on the first theme, the excitement around hyper-connection and globalisation tend to crowd the fact that the issues of most concern are influenced by geography. Conflict in the Middle East connects with people flows into Europe drive concerns about the security of trade links there. Tensions in the South China Sea destabilise confidence in trade routes and markets in North and South East Asia. Political instability and climate change influence security in

our near region. The point is that New Zealand has interests in all these global risk centres of gravity and the accumulation of risk to us is of concern.

(15) Thirdly – "security threats to New Zealand are, in the main, **externally driven**". They may manifest as an internal problem but the ones of most concern are driven by external factors. Putting to one side the geologic and meteorological issues unique to New Zealand, almost all of the major risks we face link in some way to external factors – risks ranging from corporate espionage, cyber attack, or regional instabilities, have their gestation off-shore.

(16) Fourthly **- Complexity rules**; where the connected world does impact seriously, is in the system wide linkages that have developed. When adversity in one part of the system strikes – the flow on effect can be rapid and highly unpredictable, with major consequences resembling a new "black swan" event, (which as you know, is a completely unforeseen event) serving to additionally challenge responders. All crises, all risks, have some aspect of this phenomenon to some extent. We try, therefore, to lift the risk management sights of enterprises from agency specific issues (which are important no less) to system wide effect. Crucially, the maintenance of system sight on common capabilities is a significant success factor. Whether of strategic or operational character, some capabilities are broadly beneficial to our national security. I don't limit this thought to public sector assets - it is complementary that high standard business continuity and redundancy standards apply right through business and non government enterprises.

(17) Fifthly, an **open society** such as ours enhances resilience. But our open economy, free movement of people, capital and goods exposes us to threats. It provides us with key strengths – the mobilisation of a free society committed to common humanitarian standards is one of the majesties of democracy – but is a weakness in that such mobilisation generally waits until threats are clear and present – or in other words "too late".

Our Objectives

(18) So if protecting us from these risks is national security, what's Government's objectives?

a. We ensure that New Zealanders are safe at home or abroad.

b. We maintain the integrity of our democratic system, our institutions, and the systems and processes of Government.

c. We secure our sea, air and electronic lines of transport and communication into and out of New Zealand. We decide who comes here and upon what conditions; and who may make use of New Zealand's plentiful resources.

d. We support the international rules based system,

e. And a sound international financial system; we protect the integrity of our economy

f. We identify and mitigate risks to the built and natural environments

g. And how do we arrange ourselves in the face of these threats? By “being **resilient**….” Resilience means that systems, people, institutions, physical infrastructure, and communities are able to anticipate risk, limit impacts, cope with the effects, and adapt or even thrive in the face of change. “Being resilient” is therefore a key goal of the national security system, emphasising the need for mature risk management processes, and the maintenance of common and unique capabilities that mitigate risk.

The Fundamental Pillars of Capability

(19) Common capabilities start at the very strategic level. For example, we are **a confident pluralistic, tolerant, functional democracy**. Compare us to the places in which conflicts occur. Our Governments can be trusted. We understand our past, and are clear about our future. We preserve the separations of power in our constitution, founded as it is on our inherited laws, conventions and the application of the Treaty of Waitangi. Governments accept their responsibility (kawanatanga) to protect the people and respect the rule of law. That’s a good start.

(20) We support, and are supported by, **an international rules based order** that disciplines power through law, custom and convention, and according the same rights to all countries. Our long-time support of United Nations interventions is clear evidence of our multi-lateral commitment. Yet in these matters we are neither content, nor complacent. Our place in the world is supported by a cadre of professional diplomats led emphatically by Ministers in the Government of the day. We make sure our positions are made clearly and transparently, and we relentlessly tread the corridors and avenues of foreign capitals so that we understand, in good time, the positions of foreign governments. Forewarned is forearmed.

(21) New Zealand also seeks to buttress our security and advance our national interests through **security partnerships** and relationships with other states. Our closest relationship is with Australia. This relationship is derived from our closeness, shared history and experience, cultural and family ties, business links and security cooperation. It is our first and only enduring security alliance. Our Defence White Paper says about Australia “New Zealand has no better friend or closer ally”.

(22) Beyond the Tasman link, our primary security relationships are otherwise within **the 5-Eyes**, a unique security partnership. This WW1 cooperation between the US and UK in World War I began as classical code breaking, intercepting naval communications sent by Morse code and using the information militarily. By the end of World War II, the US and UK had a recognisably global signals intelligence machine in place, and they chose pragmatically to repurpose this as a wider collective security partnership to trusted partners.

(23) What about New Zealand? We’ve always seen our security as collective: indeed, New Zealand’s major foreign wars (Afghanistan in the 19th century, the Boer War, two World Wars, Korea and Vietnam) have been predicated on the sense that we participated in a wider community of interest whose values and

aspirations we shared, and where we saw that a threat to one was something that mattered to us, no matter how far away. We've had our own history and have our own story, but it has never been an isolationist one. Given how much of our prosperity depends on the international rules based system, the case for taking our share of the burden in a collective process is as relevant now as it ever was.

(24) There's a myth about the 5-Eyes, that it costs us our foreign policy independence. I think that's demonstrably not so: decisions in the 1980's about potentially nuclear armed ships, and in the early years of this century about non-participation in the second Iraq War both showed New Zealand able to take decisions at variance with its allies without permanently rupturing its underlying partnerships. The 5-Eyes arrangement provides for a lot of sharing – not just information but also technology and some of the associated skills and insights. It makes our Armed Forces and our Security Agencies much more competent than would otherwise be the case. Not freeloading, mind, nor enticed to do things outside our national interest, our defence and security professionals are well regarded amongst peers overseas.

(25) The Five Eyes is not our only **security partnership**. We have others. For example, we work within the Five Power Defence Arrangement centred on South-East Asia. We have relationships elsewhere in Asia and in Europe. We provide and receive assistance in the Pacific. We see informed and mutually cooperative linkages as beneficial to our national security.

Other Security Capabilities

(26) We have other security capabilities. The foremost is our New Zealand Defence Force. As the Prime Minister noted in his foreword to the 2016 White Paper "New Zealand's strategic environment continues to evolve, sometimes rapidly, and our defence policy needs to adapt to these changes." This adaptation is made through an independent policy process consistent with New Zealand's values and interests. The PM also noted the relationship between the Defence Force and national resilience as evidenced by deployments in response to the Christchurch earthquakes. For example, a quick check of the signalled capability policies show an alignment between the risks New Zealand face, and intended new capabilities. I've spoken of the cyber risk - look then to the recent white paper for additional capability that the Defence Force can defend itself from modern cyber capabilities. So it is to be.

(27) There are reforms underway in respect of the intelligence agencies. The NZ SIS and GCSB are both responding to changes in New Zealand's threat environment. These changes create pressures that challenge pre-existing notions of separation between foreign and domestic threats, and between types of intelligence collection such as HUMINT, SIGINT and nowadays OSINT. Any change to the agencies – legislative, policy or practice, edges into a very contested political environment. But the repair of the fracture in public confidence in the agencies, and of the political consensus around such key components of national security capability, are key objectives of the current government. This is being pursued down three lines of effort:

a. Firstly, in the area of mandate – the resetting of Parliamentary direction and control over the agencies – effected through a new enactment covering the two primary intelligence agencies and touching the third (National Assessments Bureau). The Bill, as it currently stands, was introduced into the House two weeks ago and is now being subjected to a lengthy process of debate in a select committee. The legislation is directed at governance, structure, powers, and process.

b. Secondly, lies in the area of purpose – and how within the broader set of legislated permissions the government of the day refines direction through the setting of intelligence priorities and then checks performance back against those priorities

c. And thirdly, in the area of capability. After a considered and in depth review process which included an analysis of then current and necessary capabilities to impact on the national security objectives was made, Ministers agreed with a proposal that a progressive development of capabilities was necessary if the agencies were to fulfil their role. In part this was to ensure they could service heightened expectations around accountability, but mostly this was recognition that as an essential part of New Zealand's understanding and mitigation of risk, they were operationally fit for purpose. Increases in baseline funding for the agencies were notified in the 16/17 Budget.

Other Capabilities

(28) A number of our other domestic institutions either are, or contribute, a common capability. The Police, like NZDF are a large disciplined service capable of scaling to support an emergency or tackle a long run risk such as transnational crime. Our border agencies patrol our perimeter for illegal entrants, contraband, biosecurity threats and other threats. Increasingly, our security partners see merit in harmonising law enforcement policies on issues that have an international character. This includes the mutual assistance authorities that Police have to extend their investigative powers into other jurisdictions or the arrangements in place to share information on people or things (like passports) that are of security interest and executed by Customs and NZ Immigration Service..

(29) Other capabilities that are of general utility and a critical success factor in sound governance of risk include basic features of our government system. Examples are our health system – so important that it functions well when under threat from a pandemic virus.

(30) Local government is intrinsically linked to national security through the system we have in place to manage civil contingencies – our regional civil defence and emergency management network that connects communities through territorial local authorities and central government at the Ministry of Civil Defence and Emergency Management (now placed within the Department of Prime Minister and

Cabinet to bring it closer to the central system of national security coordination.) Local government are beefing up their risk focus

(31) The private sector contributes to national security through routine business continuity planning. Defending utilities such as power, communications and water is core capability. Distribution systems – including the logistics of food – enables communities to bounce back rapidly if designed with risk in mind, as they are.

(32) The security of the nation, therefore, is not just about our core security apparatus – its about how resilient we are in the face of risk.

The National Security System

(33) Which brings me to the system of national security coordination. How do we turn our latent resilience into expert action? One major capability we have is our ability to work together in the national interest using a common system.

(34) The system is headed by the Cabinet Committee for National Security (chaired by the PM) which provides a forum for Ministers to discuss and decide matters relating to cross cutting issues of security concern.

(35) There exists an Officials' Committee on Domestic and External Security Coordination – "ODESC". This framework is where officials collectively support Ministers in their responsibilities for cross cutting risk – a system about which has been spoken little. Once I was on radio talking about organised crime in New Zealand and said that my worry was such that "I intended to raise organised crime as a national security concern at ODESC". I had hardly finished on the point and the phone rang – a senior colleague chiding me that "Howard - ODESC has never been publicly avowed in New Zealand". This was less than ten years ago! Recently Fairfax ran a whole page article on DPMC's Andrew Kibblewhite and ODESC. Such is change.

(36) ODESC was 'restructured' in 2014, with a new framework of interconnecting committees, and made subject to Cabinet direction on roles and responsibilities. A position was created in DPMC to sit at the centre of the system to assure its proper functioning. ODESC coordinates national capabilities around risk management. That is, to identify and describe our risks, reduce the likelihood of a security event, build preparedness for national resilience, respond expertly to events when required and recover rapidly and expertly from adversity. The typology here is the "Four R's", hopefully known to you all. Somewhat flippantly, I would say that unless you are capable across those four R's you expose yourself to three more – "recrimination and retribution and resignation!"

ODESC – Strategic Mode

(37) The ODESC system divides into a strategic and operational mode. In strategic mode a senior officials committee known as ODESC G is chaired by said Andrew Kibblewhite. It meets infrequently, but with a

remit to ensure the system maintains focus on priority risks, and otherwise is a well performing enterprise.

(38) The "Strategic Risk and Resilience Panel" is ODESC G's "critical friend". It comprises a group of public and private sector individuals skilled in risk management; some because of a science background, others because of professional roles in large private sector companies. It is an independent advisor to ODESC G and thus has free licence to comment to them on the matters it deals with. It does so vigorously.

(39) Reporting to ODESC(G) are the Security and Intelligence Board (SIB) and the Hazard Risk Board (HRB). These groups, split the "two sides" of national security risk between them, and are attended by public sector Chief Executives of agencies with primary responsibility for risks on each side. MFAT, NZDF, Police and DPMC are commonly represented on both boards.

a. SIB, in addition to the common agencies, includes the intelligence agencies, Customs and the Ministry of Defence – and shortly will add MBIE to the group in recognition of the growing connection to national security of that agency. In addition to a collective focus on core security and intelligence risks this board acts as a clearing house for sector issues. What are these – well they are mainly a case of the blinding obvious and about the clear and present dangers which I have already spoken. The Board also considers some common problems such as intelligence coordination, attracting and retaining staff, and interdepartmental security issues.

b. The HRB, in addition to common agencies, includes Transport, Health, MCDEM, Primary Industries and the Fire Service. This Board focuses on hazard risks such as derive from geologic instability, shoreline threats from tsunami, transport system security, pandemics and biosecurity. System issues also feature, such as the national security exercise programme, common tools such as the critical incident management system (a set of common command and control rules for handling major incidents) and the security sector professional development programme.

(40) Outputs of this strategic mode of operation include strategic assessment and more detailed assessments of risk, shared policy development, and interagency sponsored projects.

ODESC - Operational

(41) But we know, for example, that often adversity strikes in an unforeseen way (i.e. the Black Swan even or cascading system risk). ODESC is configured also to respond to crises. We know from hard experience that it is best that a **known and practiced** system engages to **support and facilitate** the actions of a resilient community.

(42) Therefore we have built a standard operating methodology to guide participants. The system's objectives, roles and responsibilities, and key processes are documented at a high level. As an issue emerges, either for treatment as a risk, or as an event or incident to manage, and cross government coordination is required, DPMC - either on request or on its own volition - activates the system by calling a "**Watch Group**". By this time a lead agency will already have engaged on the issue, most

probably implementing a prepared contingency plan and involving other agencies and specialists. The Watch Group begins a different process, connecting the operational level to the cross government policy and political domains. The Watch Group convenes senior officials to consider the issue, frame and make sense of it, measure it ("do we have a problem here") and figure out what to do (in reality – what advice to give). These occur with remarkable frequency. Less frequently, is the escalation to Chief Executives of departments and ministries when the advice is that there is a problem – the lead agency might have pitched in "too low and slow" or the problem is more complex than envisaged. The political context can be tested when the Prime Minister calls senior and relevant Ministers together to provide guidance or decisions relative to the national interest – and introducing the necessary political calculus to the response.

(43) You should note that many of the ODESC principals have a form of statutory independence (for example the Commissioner of Police, or the Director of Security) or have responsibilities that escalate with authorisation by a Minister (for example the Director of Civil Defence). The ODESC system stands neither in the way of the peculiar manner in which they are obliged to act, nor as a bureaucratic impediment compromising speed of action. It facilitates the free flow of information to where it is needed most and thus aids decision making.

(44) Certain objectives are within clear view:

a. Roles and responsibilities are clarified. This has a number of dimensions:

   i. The determination of which agency has lead operational status. The lead agency typically coordinates the operational response, provides the communications lead and briefs into the political process through their Minister.

   ii. Clarity over who is doing what; and where the centres of gravity are in terms of addressing the issue, and what the operational imperatives are. Who is the individual responsible for sending out the situation reports, who is governing the work programme or action list?

   iii. Those with specific roles to perform have a forum in which to discuss factors relating to the national interest – even if ultimately that is a matter for the exercise of their independent judgment.

b. Secondly, a common operating picture emerges. Agencies work from a common and consistent set of facts. This needs to be done at speed, and is never fast enough for the political communicators who are engaged from the get-go. What is at stake is the correct framing of an issue so that it is properly addressed (again "what is the nature and seriousness of this issue – where is it heading?". Whereas when I started in this area of public service, a major sin was to over-react and trouble busy leaders with the burden of the cross-government overlay; but because of the speed and reach of communications today there is almost no risk of over-reaction – now the system errs toward activation - better to dial the system up and then let it retire, than to allow complacency to rule and forever be damned for tardiness.

c. The full use of government and other resources are brought to bear as quickly as possible. The constant trade-off is between effective consultation across perspectives and skillsets, and the time it takes to engage a problem. This brings into play other necessities in the approach. The need to exercise frequently, and the need to build relationships so that the processes for decision making are as economical as possible – less time finding the right people and less time working out operating protocols.

(45) The core system is called on to provide (amongst many things):

a. Political actors who have enough knowledge to challenge and question the system and provide visible leadership

b. Decision makers from across the security landscape

c. Professionals skilled in framing complex problems, and subject matter experts including scientists who understand the problem and can innovate solutions – and offer sound advice – and including the "red teaming" approach in which core assumptions on any matter can be tested

d. Policies and systems including those to rapidly develop and then maintain situational awareness

e. Connected communications capabilities that are practiced in escalating to emergency scale

f. A fantastic virtual rolodex where "who knows who" can be leveraged in the crisis – particularly in the non-standard segment of the national security community

g. Emergency services with business continuities that enable them to function in all circumstances

h. An international and trusted voice engaged through a respected and expert diplomatic service

i. A capable defence force with planning, logistical, engineering and field staff skilled in working as much in civil circumstances as military

j. And I could go on………

(46) The people dimension in security is critical and we have been working on building people capability.

a. Our recruitment, development and talent managements systems are starting to stream available capability through agencies (increasing secondments etc)

b. We've created an "ODESC Forum" which refers to the group of practitioners who work in the national security system. They are invited together in learning groups, or to workshop common problems.

c. They are the target of the Security Sector Professional Development programme, and agencies are sharing training opportunities for common skills (e.g. intelligence analysts).

d. We have produced a handbook to help understanding and practice.

e. We get together often to practice on thorny problems.

These are the people to whom we turn to for leadership and expertise when circumstances demand.

(47) Taking such a broad approach to risk identification and risk response requires a flexible and adaptable national security architecture. New Zealand's capacity to deal with the full range of national security challenges requires the system to be integrated, able to leverage partnerships between government agencies, local government, private companies, and individuals. There is enough bureaucracy to provide form to function but not to stifle adaptation or flexibility.

What are the current challenges in national security?

(48) I often get asked – "what keeps me awake at night?" Well, plenty, …. And then I hear you say, "well, that's what you pay me for". But I am allowed to reflect on what I think the challenges are for the national security system as we build it towards the vision of a truly "world class" system.

(49) The first is a problem somewhat peculiar to New Zealand, maybe…. It lies generally in the area of the difference in appreciation of risk between national security professionals and the general public. You know, we are often accused of drinking the national security kool-aid and thus become too amenable to over-reaction to an issue – that is to "over frame it".. On the other hand, the public has been entitled to think we are inured against risk by what someone described to me as the "moat and barrier" strategy. The moat refers to the oceans around us and that it takes a determined and skilled traveller to mount an expedition to invade us. And to do so they have to overcome the "barrier" – Australia…… As I have pointed out, national security is much more complex than that. It's a challenge to lift resilience because it disturbs the view we have of ourselves as a safe and secure haven in the South Pacific and the insurance costs – a lot….. But insurance is just that – it might reduce the risk, or ameliorate the effect – it is unlikely to eliminate the risk completely. The public never sees the "what might have been but for…." How well then are we, the New Zealand public, prepared for the fallout from a security, rather than a natural hazard event? What would the post event fallout look like? Perhaps "we spent all this money and still something happens?" Or, "what do you mean you were not sifting everything on line". So I worry about advising on the right policy balance to strikeon risk based capabilities.

(50) Secondly, it is the policy of the government to be more transparent about security risks and the capabilities we deploy. This is a good thing. *Up to a point* - and this is what concerns me. There a high tide mark at which we can declare our intentions and capabilities. To go further is to render parts of our system valueless. It is at this point that our democratic system is both challenged and yet has an answer. We elect people to govern these capabilities and they appoint others to exert controls and oversight. And then, ultimately, we have to trust them. My concern? I get a feeling as I look around the world that there are overall declining levels of trust, *in anything*…… Such a distrustful world is a dangerous one.

(51) Thirdly, and finally, I worry about relevance and competence. If we cannot strike the right policy for prudent risk management I sense we will err too much on the side of caution. Attention and

investment will wane, capabilities will erode, performance will decline, the existential questions will dominate and the risks, well they will increase. So, then, I worry that we will miss something that will end with catastrophic effect. Here, our national security depends on remaining vigilant: vigilant about our environment, and vigilant about our capability - without losing touch with those things that make us distinctively New Zealanders and basically good people.. Forewarned, is forearmed. [Ends]