s 6(a)

SIB

System Health

The underlying conditions that support SIB to achieve its vision "resilience against those who wish us harm"

Governance focus		Oversight – work is underway	
SIB's internal focus	**External to SIB**	**People**	**Enabling systems**
We are clear on our **purpose**, effectively **prioritise** national security and related investment for now and the future, are **coordinated** across the wider system, and leverage **international relationships**	Ministers, agencies, organisations, and New Zealanders recognise the **value of national security** and appreciate they may have a role in maintaining NZ's values	Our national security **workforce** is capable, trustworthy and appropriately sized to deliver the Government's priorities	Our physical and technological **infrastructure** and **policies** enable us to operate in a secure and joined up manner
s 6(a)			
1.1 We have clear **goals**, know SIB's **value add** and have clear **accountabilities.** We **measure our work**, know whether we are making a difference and seek improvements	2.1 We maintain **trust and confidence** of the government of the day, and the New Zealand public, by being transparent around threats, risks and opportunities	3.1 An **integrated, flexible and skilled workforce** enables the sector to be responsive to the changing demands placed on it	**4.1 Information assets are protected** from unauthorised use, accidental modification, loss or release
1.2 We are **coordinated**, efficient, and involve the right people	2.2 The Government and New Zealanders **value national security** and **understand their role**	3.2 Access to information and assets is only given to **suitable**	4.2 **Physical security measures** protect people, information and assets
1.3 We provide the conditions for **sound strategic decision making**	2.3 We **understand the resources** needed t meet the Government's priorities and are transparent on what cannot be delivered		4.3 Our **classified infrastructure** is fit for purpose
s 6(a), s 9(2)(g)(i)	2.4 We work collectively to develop **system level funding** bids (and are considering opportunities with the proposed **Public Service Act)**		
1.5 We effectively leverage **international relationships**			

Objective	Key areas for consideration	Work prog	Comment
Internal environment: We are clear on our purpose, effectively prioritise national security and related investment for now and the future, are coordinated across the wider system, and leverage international relationships			
1.1 We have clear **goals**, know SIB's **value add** and have clear **accountabilities.** We **measure our work,** know whether we are making a difference and seek improvements.	SIB has a clear **understanding how it will meet its vision** "resilience against those who wish us harm" and uses strategic priorities to determine the relative priority of system activity		*Risk statement*: if we do not have a **strategy**, **prioritisation mechanism**, or being explicit about what we are not resourcing, we cannot be confident we have **overarching coherence and direction**, and that our level and nature of risk management is **publically acceptable**
	We regularly **measure SIB's governance role** and can articulate how SIB is making a difference		
	We measure whether we are **affecting change** across the system		
	As part of our desire for **continuous improvement** we consider & incorporate recommendations from reviews, Royal Commissions, Inquiries and debriefs.		
1.2 We are **coordinated,** efficient, and involve the right people	We seek opportunities for better **coordination between agencies** to reduce duplication, increase **efficiencies** and clarify accountabilities		*Risk statement*: if we are not coordinated across the large number of often complex agencies we risk **inefficiencies**, **duplication** or **gaps**.
1.3 We provide the conditions for **sound strategic decision making**	We understand our environment and how this may change in the future, including the impact of next-generation trends such as emerging technology		*Risk statement*: if we do not have a comprehensive understanding of our environment including a **forward scanning function** we risk continually being **reactive**, leading to **inefficiencies, missed opportunities, sub-optimal decision making** and potentially failure
	Strategic decision makers are supported by valued assessments and advice		
	SIB's NRR risks are clearly defined, allocated and supported by work programmes that are resourced by all involved *HRB's version includes systematically identifying new and emerging risks*		
s 6(a)			
1.5 We effectively leverage **international relationships**	s 6(a), s 6(b)(i)		s 6(a)
	s 6(a), s 6(b)(i)		
	We are aware of, and leverage, other agencies' **international engagement**		

Objective	Key areas for consideration	Work prog	Comment
External environment: Ministers, agencies, organisations, and New Zealanders recognise the value of national security and appreciate they may have a role in maintaining NZ's values			
2.1 We maintain **trust and confidence** of the government of the day, and the New Zealand public, by being transparent around threats, risks and opportunities	We monitor / build our **collective social licence** which aids in maintaining an appropriate authorising environment and enables us to deliver the outcomes NZers expects		s 6(a), s 9(2)(g)(i)
2.2 The Government and New Zealanders **value national security** and **understand their role**	In a coordinated manner, we **strengthen and broaden understanding of national security** so ministers understand their role within it, how it underpins wellbeing, and its value in supporting strategic decision making		
	Agencies' significant **national security requests of ministers are coordinated** to ensure collective narrative is reinforced, and priority issues are elevated		
	In a coordinated manner, we **strengthen and broaden understanding of national security** so **entities** and the public understand their role		
	Agencies' significant messaging relating to national security is coordinated within an **overarching narrative**		*Risk statement:* If national security communications are not coordinated we risk disjointed messaging and missing opportunities to credibly and actively participate in public discussions in a coordinated manner
2.3 We **understand the resources** needed to meet the Government's priorities and are transparent on what cannot be delivered			*Risk statement*: If we cannot articulate the impact of demand outstripping resourcing, consequential poor delivery risks losing trust and confidence of ministers and the public
2.4 We work collectively to develop **system level funding** bids (and are considering opportunities with the proposed **Public Service Act)**	We develop **joint funding initiatives** that reflect system priorities so resourcing can be applied in the most appropriate place		*Risk statement*: if we do not consider system-wide funding needs, we miss opportunities for strengthened system design, holistic funding, and ensuring high priority initiatives are funded
	We seek opportunities for **improved system design** and horizontal accountabilty through engagement with SSC on the new Public Service Act		

Objective	Area of work	Work prog	Comment
Our national security workforce is capable, trustworthy and appropriately sized to deliver the Government's priorities			
s 6(a)	National Security Workforce (SIB component – TS workforce) • Career Pathways • Career mobility		s 6(a)
	Diversity Project s 6(a) (managing candidates with checkable background issues)		
3.2 Access to information and assets is only given to **suitable people**	Protective Security Requirements – Personnel Security [work programme underway]		
	Protective Security Requirements – Personnel Security [work programme underway]		

Objective	Area of work	Work prog	Comment
Our infrastructure and policies enable us to operate in a secure and joined up manner			
4.1 Information assets are protected from unauthorised use, accidental modification, loss or release	Protective Security Requirements – Information security [work programme underway]		
	Classification system review [project underway] *(For review by PSR)*		
4.2 **Physical security measures** protect people, information and assets	Protective Security Requirements – Physical security [work programme underway]		

s 6(a)

[redacted]

Date	13 December 2017
To	Chair and Members: Security and Intelligence Board
From	National Security Policy, DPMC
For your	Decision

National Intelligence Priorities – 2018 Refresh

Purpose

1. This paper updates SIB on the 2018 national intelligence priorities refresh, after initial consultation with key agencies and Priority Coordination Group coordinators. It seeks agreement to recommendations that will provide the basis for a fit-for-purpose set of national intelligence priorities in 2018.

National intelligence priorities help us focus our effort on understanding the most important national security issues

2. In 2016 the Chair of ODESC advised the Cabinet National Security Committee that the national intelligence priorities:

   - Guide the activities of New Zealand's **wider intelligence sector**, to ensure it provides intelligence on what matters most to our national interest;
   - Show the sector where to target its **covert** [secret/classified] **and overt** [unclassified] **intelligence capability** to achieve the highest national security impact; and
   - Inform **collection and assessment**.

3. The First Independent Review of Intelligence and Security in New Zealand reiterated the vital role that intelligence plays in informing strategic policy decisions that influence New Zealand's position in the world and more immediate decisions relating to specific situations, as well as assisting frontline enforcement agencies.

The Intelligence and Security Act 2017 sees the intelligence and security agencies working with other domestic agencies (including law enforcement agencies) towards key government priorities

4. The Intelligence and Security Act 2017 is now in effect. A primary policy objective underpinning the Act is promoting greater cooperation between the intelligence and security agencies (GCSB and NZSIS) and other domestic agencies, including law enforcement agencies, to ensure that the intelligence and security agencies' shared objectives and the New Zealand government's priorities are achieved.

5. The intelligence and security agencies' shared objectives are to contribute to the protection of New Zealand's national security; and the international relations and well-being of New Zealand; and the economic well-being of New Zealand. New Zealand government priorities are expressed through the objectives and priorities set for government agencies, and in turn, expressed to GCSB, NZSIS and the National Assessments Bureau (NAB) through the national intelligence priorities.

But the national intelligence priorities may not be doing what we need them to

6. Consultation with a range of domestic agencies who collect, prepare and use intelligence and assessments, and priority coordinators indicates that the link between the national intelligence priorities, and the use of intelligence and assessment to support government priorities that relate to national security and the protection of national interest is not as strong as it could be.

...because there is no agreed understanding of who they apply to and what they are trying to achieve

7. Despite previous advice to Cabinet, there is a lack of agreed understanding regarding what the national intelligence priorities are for, who they apply to, and how they are to be resourced across the sector. In particular, there is confusion amongst agencies and within Priority Coordination Groups as to whether they apply only to the intelligence and assessment activities of GCSB, NZSIS and NAB or whether they are intended to guide collaboration across all agencies who can contribute to understanding the issues, regardless of the source of the intelligence and information.

8. A lack of common understanding across the national security sector of the role of the national intelligence priorities:

    - *Reduces the ability of individual agencies and the system as a whole to develop a detailed understanding of important national security issues (and risks)* – by not encouraging a collaborative approach across all information/intelligence types and sources across government.
    - *Overlooks the benefit that overt intelligence and unclassified information and assessment/analysis from a range of policy and operational agencies provides* by helping to "connect the dots" when understanding many of the national intelligence priorities.
    - *Encourages a focus on tactical/operational uses of intelligence and assessment* – rather than also promoting the usefulness of intelligence and assessment in informing strategic planning and policy-making.
    - *Contributes to a lack of clarity within Priority Coordination* Groups – when agencies do not see their needs, mandates or resourcing reflected in the intelligence priorities.

...and there are a range of other challenges impacting effective use of outputs from the national intelligence priorities

9. Other factors are also stopping intelligence and assessment about the national intelligence priorities from informing decision-making and policy-making to the fullest extent that it could:

    - *The current priority descriptions are not clear enough,* and don't provide enough guidance around what areas are of most importance within the priority, why they are important and what outcomes are sought. This also inhibits the development of an effective performance framework.
    - *The priorities don't reflect what agencies actually need from intelligence* because they don't relate to the outcomes they are required to deliver to government. Agencies are therefore developing their own intelligence priorities independent of the national intelligence priorities. This implies an inefficient system that is not making best use of scarce resources.
    - s6(a) [redacted]
    - *Many outputs are too highly classified for use,* and/or not focused on the areas where agencies would get most value, or need to draw on the benefit of analysis or assessment

insights. s6(a) [redacted]

- *There is a lack of cleared people and a lack of (convenient) SCIFs* to read and store classified material. If the right people at the right level don't know the material exists, they can't use it effectively.

There is scope to provide more clarity in the national intelligence priorities framework to make them more effective

10. SIB members are encouraged to see the 2018 refresh as an opportunity to position the national intelligence priorities framework so that it is effective in guiding the use of intelligence and assessment to manage key national security issues. To do so, the refresh must first address the above noted questions and challenges as much as possible. Other initiatives underway will also help address those that cannot be resolved through the national intelligence priorities alone (such as the NZIC customer engagement initiative, and the TS Network, TS Workforce projects).

...by ensuring a common understanding of what the national intelligence priorities are for and who they apply to

11. As noted, the national intelligence priorities apply to ***covert and overt*** intelligence, collected and assessed by the ***wider intelligence sector*** (which should be read as the range of agencies making up the national security sector). This recognises that to best inform our understanding of national security issues, and to be used effectively across government, including operationally and in policy-making, covert intelligence is only useful when it is understood in context, using overt intelligence and unclassified information collected by a range of agencies.
12. To reaffirm, the national intelligence priorities are therefore both the mechanism used to 'point the covert and overt intelligence collectors' in the right direction; and a framework of national security issues that need information-sharing across government to understand, monitor and take action on.
13. As a result, the national intelligence priorities apply to many national security sector agencies, not just the GCSB and NZSIS. Every agency should identify the role they play in improving the sector's understanding of those issues: whether by actively tasking according to the priorities when collecting overt or covert intelligence; by providing contextual unclassified information; by contributing analysis or assessment; or by using intelligence and assessment to inform policy advice and decision-making.
14. If agencies actively share intelligence, information, analysis, assessment or advice related to a particular national intelligence priority to the best extent possible (noting statutory restrictions in some areas), we will more effectively be able to demonstrate value for money of the significant range of resources dedicated to intelligence across the national security sector.

...by taking a wider perspective when determining issues that comprise the national intelligence priorities

15. The current priorities were determined by ratings against two main considerations:

s6(a) [redacted]

16. Many agencies consulted indicated that because these evaluation criteria were based on those developed for the NZIC Strategy, Capability and Resourcing Review (SCRR, which applied only to GCSB, NZSIS and NAB), they do not fully reflect the collective interests of all agencies that contribute to, or make use of (or would like to), the national intelligence priorities.

17. Although a range of agencies from the national security sector participated in the original ratings process in 2015, the criteria used did not necessarily fully capture those agencies' interests and priorities, or the way in which intelligence adds value to their work. The criteria also do not reflect the way in which agencies making up the broader sector are resourced nor do they fully reflect the holistic and integrated approach to managing national security risk across the 4Rs that the system expects of those agencies.

18. The 2018 national intelligence priorities should reflect the progress and advancements made in respect of the intelligence and security agencies (via the Intelligence and Security Act 2017) and in the national security system as a whole (eg establishment of a National Risk Unit; more collaborative work programmes across SIB) since the last two refreshes. This means more deliberately considering the strategic national security outcomes and priorities that the full range of national security sector agencies have been mandated to deliver to government. Doing so would allow the priorities to also promote New Zealand's national advantage, by using intelligence to provide decision advantage in many areas.

19. To do this, the 2018 national intelligence priorities should comprise issues that:

    a. Impact on national security and/or **national interest;** and

    b. Benefit **from covert and overt intelligence shared across government**; and

    c. **Reflect the key priorities national security sector agencies have been set by government**.

20. Adding to the SCRR criteria in this way will not negatively impact performance reporting for the core NZIC. DPMC and the Joint Directors-General Office are currently developing a new performance framework designed to measure the impact of the additional SCRR resources and the overall success of the NZIC as a system. This performance framework will incorporate any changes to the national intelligence priorities.

21. Explicitly including key government priorities in the national intelligence priorities will bring the following benefits:

    - Allow Ministers to more easily link intelligence to government priorities/portfolio priorities and how intelligence and assessment can help them make decisions;
    - Allow more policy and operational decisions within the national security system to be supported by relevant intelligence analysis and assessment;
    - More accurately reflect the improving level of understanding of our national risks and the drivers of those risks, and threats to national security and interest;

- Provide greater recognition of the role of policy and operational agencies in understanding the issues, and also more accurately reflect the intelligence needs of those agencies;
- Ensure covert intelligence resources are being dedicated to those national security issues where the can add most value; and
- Reduce the number of internal intelligence priorities agencies need to develop and allow them to focus on non-national security related agency priorities linked to other statutory functions or government priorities.

...and the relative emphasis and resourcing across the priorities

22. The current priorities are grouped into three categories: **High** (topics that are the priority focus for the intelligence sector's collaboration); **Medium** (topics to be delivered to the extent possible within available resources); and **Low** (topics which chief executives would consider resourcing as circumstances demand, or as resources allow). s6(a) [redacted]

23. However, within the national intelligence priorities there are issues that varyingly:
    - Need covert intelligence to be monitored and understood;
    - Have multiple dimensions, or impact across many parts of government, to which covert intelligence may contribute but that overt sources of intelligence and information may provide more effective understanding; and
    - Require more deliberate and coordinated effort across a range of agencies to understand, but that covert intelligence may only add value to in particular circumstances.

24. The very inclusion of this range of issues within the national intelligence priorities suggests that **all national intelligence priorities should receive some kind of proactive effort and resourcing** – but the type and nature should vary according to the category. A more flexible framework for determining the relative importance of a priority, and the appropriate level of resourcing and coordination, would make the national intelligence priorities more relevant to a wider range of agencies.

25. The proposed three-tier framework in **Table 1** below suggests the **relative emphasis of a priority** based on two key factors that focus on why an issue needs to be understood:
    a. How important the issue is to New Zealand's national security and national interest, and the role it plays in achieving key government priorities (which includes promoting national advantage); and
    b. The depth of understanding required, as determined by the nature of decisions that are likely to be required.

26. Focusing on why an issue needs to be understood helps us to determine how each priority should be resourced to achieve the most useful outcomes. Covert, overt and foreign intelligence, as well as intelligence, policy and operational agencies all play different roles in understanding the three categories of issues outlines above. The national intelligence priorities should be flexible enough to help agencies determine where they can add the most value – and give them the flexibility to direct resources that way.

CATEGORY ONE	CATEGORY TWO	CATEGORY THREE
Issues of the **highest importance** to New Zealand that **involve imminent or current threats** to New Zealand's national security and/or national interest, the safety of New Zealanders, and are related to significant national risks. *Generally imminent or "life and limb" harms.*	Issues of **high importance** to New Zealand that involve **risks** to New Zealand's national security and/or national interest, and/or support the achievement of key government priorities. *Generally, longer run "burning" issues.*	Issues of **substantial importance** to New Zealand and which contribute to the achievement of national security objectives and/or key government priorities, and which contribute to the management of national risks.
Government must be fully informed of these issues to make immediate policy or operational decisions, including threat mitigation and emergency response decisions.	**Government must be well informed** on these issues to make timely policy and operational decisions, and to develop fit-for-purpose risk management across the 4Rs.	**Government must be adequately informed** to make measured policy or operational decisions, including the development of fit-for-purpose risk management across the 4Rs.

Table 1. Proposed framework for determining relative emphasis of the national intelligence priorities

27. **Table 2** below is a proposed framework for **determining the relative resourcing of each category**, based on three factors:

    a. The contribution covert intelligence will play and the likely extent of resourcing from the covert intelligence agencies;

    b. The contribution overt intelligence will play and the role policy and operational agencies will make; and

s6(a)

s6(a)

Table 2. Proposed framework for determining relative resourcing of the national intelligence priorities

28. For example, the GCSB or NZSIS may determine they cannot add value to or support a Category One priority, but that they do have niche capabilities that could add value to a Category Two or Three priority instead. The GCSB or NZSIS might enhance their outreach to relevant New Zealand agencies on Category Three issues to facilitate better access to foreign intelligence.

29. We would expect Category One and Three to comprise only a small number of priorities, with the majority sitting in Category Two. The ability to move issues between categories would remain, should circumstances require it.

30. Priority Coordination Groups were established in late 2015 as a collaborative mechanism to ensure customer needs drive collection and assessment responses across the high priority national intelligence priorities. This recognises that collaboration between collectors, assessors and customers is critical to understanding the issues represented in the national intelligence priorities.

31. As well as adopting the above framework, it would be beneficial to adopt a more flexible approach to establishing Priority Coordination Groups. s6(a)

32. This could mean establishing groups only when they can add significant value and improve the level of understanding of the issue and the ability of agencies to use intelligence and assessment to inform their decision-making, strategic resource allocation and medium-to-long-term planning. It could also mean recognising when a Priority Coordination Group (as we know it now) is not the best mechanism for coordination, and not requiring one to be established just because a priority sits within a certain category. Instead, it may be more beneficial and productive to take advantage of effective alternative mechanisms for coordination already in place, albeit with those mechanisms remaining accountable to the National Intelligence Coordination Committee, as standard Priority Coordination Groups are.

33. It is too early to indicate how many Priority Coordination Groups this would translate into for the 2018 national intelligence priorities, or how this might be determined. This will form part of the next phase of the refresh (developing the full set of priorities), and be one of the matters brought back to SIB for discussion.

...and finally, by improving the clarity of the national intelligence priorities themselves

34. The current descriptions of the individual national intelligence priorities do not clearly address the high-level "what, why, and who?" questions required to determine detailed intelligence requirements in support of each priority. They have more emphasis on process, rather than the outcomes sought.

35. To improve implementation of the priorities and support the effectiveness of Priority Coordination Groups, the 2018 priority descriptions should provide more relevant information that helps translate them into detailed intelligence requirements, and ensure the right mix of collectors, assessors and customers are engaged. This means clearly stating:

    a. What the key focus areas of interest are within the broad issue;
    b. Why the issue is of interest to New Zealand and the national security sector;
    c. What strategic outcomes are expected from understanding the issue; and
    d. Who the key customers are which need intelligence and assessment of the issue.

36. Focusing on the nature of New Zealand's interest in the issue, and the link to government priorities and outcomes sought, will provide a clearer baseline from which to work when determining detailed intelligence requirements. These descriptions are not intended to be so prescriptive that there is little room to move: emphasising the outcomes sought will retain the existing flexibility to

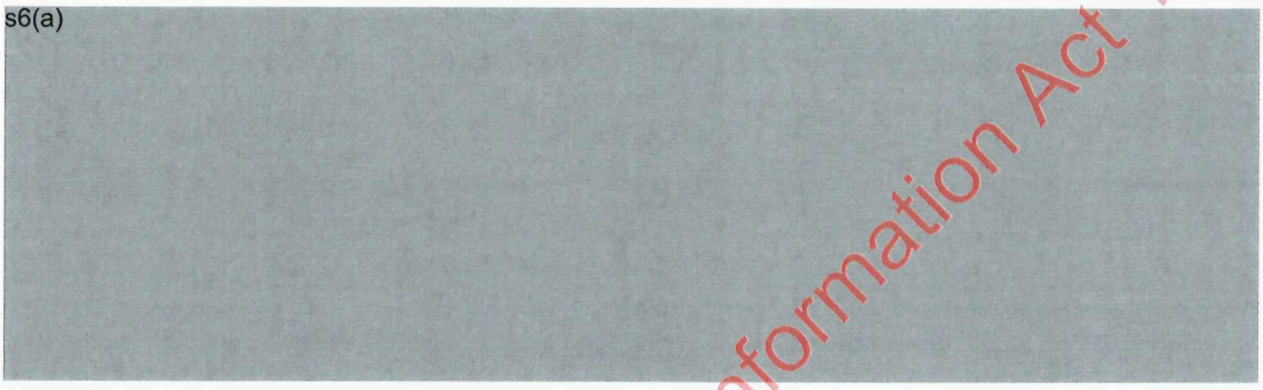
adapt areas of focus within a priority as circumstances demand. The responsibility for determining detailed intelligence priorities will remain at the Priority Coordination Group level.

Agencies have a range of intelligence and assessment needs that can be met through a more collaborative approach to the national intelligence priorities

...which indicate some changes to the current priorities should be considered

37. A range of key issues and areas of priority are emerging for consideration in the 2018 national intelligence priorities. At this stage, the most obvious of these which reflect potential changes from the current priorities include:

s6(a)



38. Further detail on these issues, as raised during initial agency consultation, is at Annex A. There is a broad degree of convergence between these emerging themes and the factors identified in the draft NAB Strategic Assessment. This is not a complete list of all issues likely to be covered in the 2018 NIPs, as several of the current priorities will carry over.

39. DPMC will continue to work with agencies over the coming months to develop the key issue areas for the 2018 national intelligence priorities, and develop proposed content of each priority, as the new government develops its priorities for national security sector agencies and a direction of travel for national security issues. Tentatively, the new priorities are expected to go to Cabinet in April 2018.

Annex A – Feedback from initial agency consultation

s6(a) [Summary of Annex A. Agencies provided feedback on the following topics: Regional security (Pacific, Asia, Middle East and North Africa), transnational organised crime, border security, foreign interference, corruption and fraud, emerging technology, space security and economic security.]

X

Stocktake of New Zealand agency activity to counter extremism online

Contents

Framework 2
Summary 3
Context 3
Key findings & questions 3
Overarching work 5
Policy 5
Community & civil society 6
International engagement 6
Online exploration 7
Online interaction & communication 7
Action & sentencing 9
Post-sentencing management 9

Framework

	Cross system work	Policy	International engagement
Activity	Legislation	Policy advice	International fora
Agency	Ministry of Justice	DPMC Ministry of Defence New Zealand Police	Ministry of Foreign Affairs and Trade New Zealand Police

	Online exploration	Online interaction & communication	Action & Sentencing	Post-sentencing management
Activity	Facilitate removal of content	Intelligence gathering	Intelligence gathering Investigation of potential criminality	Management of internet access Disengagement
Agency	Department of Internal Affairs	New Zealand Police NZDF NZIC	Department of Internal Affairs NZIC New Zealand Police	Department of Corrections

Summary

Context

When looking at activity to counter violent extremism online (online CVE), it is important to note that the online sphere does not exist in a vacuum and that there is significant crossover between the offline and online environments. The online environment is a key vector for violent extremist activity. Activities such as incitement, preparation, coordination, financing and the carrying out of terrorist activity can happen both online and offline. Counter extremism efforts therefore deal with the whole person, and not just online activity. (R)

But much extremist activity now takes place online. For the purposes of this project, therefore, this stocktake has focussed on activity that takes place in the online environment – defined as *all layers and functions of the internet across all devices and platforms.* (R)

When examining New Zealand agency activity to counter extremism online, the scale and profile of violent extremism within this country must also be taken into account. We are vulnerable to violent extremism, and there are a number of individuals, off-shore and in New Zealand, who are potentially of national security concern. We do not, however, face the scale of problem seen by our partners. This has implications for our system's response to countering extremism online. (R)

Key findings & questions

Both online extremism and online countering violent extremism are very complex areas with implications in both the domestic and international environments. The issue is borderless, and the line between extremism and freedom of speech can be difficult to identify. In addition, the pace of technology change means that governments can struggle to keep up with extremist activity and innovation. (R)

The spectrum of CVE activity within New Zealand ranges from international advocacy to operations. Domestically, there are many agencies involved and a number of relevant pieces of legislation. At this stage, work seems to be appropriate to our context and the number of cases we are dealing with, as well as the fact that much of the associated work is being done by international and private sector partners. (R)

- Domestically, there are other work-streams underway relevant to the approach to extremism online. This includes a CT Strategic Framework, a project focused on New Zealand's approach to the prevention of violent extremism as well as consideration of CT legislation. However, none of these projects draw together our approach to extremism online. (R)
    - *Building off the online stocktake, is there value in drawing together our approach to online extremism through a dedicated work stream (as we have done for the prevention of violent extremism more broadly)?* (R)

- Internationally, the issue features regularly in global fora, and there is an opportunity to be more organised, make a more active contribution, and have a clearer agenda. Our relationships with security partners and the private sector help us manage the threat from extremism online, and contribute to global efforts. Much of the extremist content and interactions we come into contact with is hosted overseas, and on platforms not based in New Zealand. Therefore we are reliant on these partners to take down content and pass on information. In addition, the development of global best practice is important in giving governments the tools needed to tackle online extremism. (R)

  - *Given that international fora are a key space for engaging with private sector and government partners, is this an area we could do more in?* (R)

- A number of agencies are currently building capability or considering building capability in the area of online CVE. These agencies include DIA and New Zealand Police. There is overlap with work to tackle other crime and we are effectively using learnings from this work in other areas, and developed capabilities in CVE could be fed back into other areas. (R)

  - *We acknowledge that the size of the problem in New Zealand is limited, but is this an area that could benefit from additional capability build?* (R)

- In both the operational, strategic and policy areas, there are a lot of players involved in the New Zealand system. It isn't clear how coordinated we currently are, although there might be good reasons for this. There seems to be work taking place at each stage of the radicalisation cycle, as well as overarching work. But this project appears to be the first time that information about online CVE work has been collated. (R)

  - *Could we be more co-ordinated, for example by having a dedicated cross-agency group for online CVE? (noting the relationship to the first question regarding a dedicated work stream).* (R)

Overarching work

Legislation

The following laws make up the legislative framework that governs online CVE:

- The Terrorism Suppression Act, particularly offences of recruiting for or participating in a terrorist group.
- Films, Videos and Publications Classification Act, in particular offences around objectionable publications.
- Parties to offences under the s 66 of the Crimes Act, specifically inciting, counselling or procuring offences.
- Harmful Digital Communications. This act is not intended to be relevant to terrorism, but may have some limited application.
- The Search and Surveillance Act, which may be relevant to investigating offences.
- Mutual Assistance in Criminal Matters Act, which may be relevant to investigations that have an international dimension. (R)

The Films, Videos and Publications Classification Act is the main piece of legislation that has been used in New Zealand to prosecute offences connected to online extremism, such as the sharing of extremist material. (R)

Review of legislation

DPMC and the Ministry of Justice are currently leading a review of counter terrorism legislation. (R)

There are a number of areas of focus, but two have particular significance. The first considers whether there is a case for new offences that typically occur earlier in the course of radicalisation – such as expressing support or calling for terrorist acts, or manufacturing and distributing terrorist publications. Many of these activities will predominantly occur online. (R)

The second considers whether there is a case for new or expanded control orders to manage the behaviour of people of concern. Such control orders could include managing access to the internet, or forbid associations with other people of concern. Officials have gained ministerial agreement to undertake more detailed work in these areas as a priority. (R)

Policy

Policy work in this area is mostly aimed at developing and implementing general cyber policy and initiatives which are not usually necessarily focused on online extremism. This includes formation of international norms of responsible state behaviour and considering the challenges posed by encryption. (R)

Agencies also contribute to the development of government policy mainly through providing second opinion policy advice, and through participating in interagency groups and discussions. Representation may be a mix of policy, operational and technical. For example, Police are a member of the Cyber Policy Group. (R)

The National Cyber Policy Office (NCPO) within DPMC leads the development of cyber security policy advice for government. It oversees the development and implementation of New Zealand's Cyber Security Strategy. (R)

Counter terrorism and cyber security can intersect, for example, in the area of illegal online terrorist content, which is a cybercrime. (R)

NCPO chairs the Cyber Policy Group, a cross-agency group addressing cyber security policy including MBIE, MoD, CERT NZ, SSC, NZDF, IC, Police, Justice, MFAT and DIA. (R)

In addition, NCPO leads the inter-agency work to consider the policy, legal and capability issues related to the possible broader use of cyber operations in support of our national security and law enforcement objectives. (R)

Cyber operations can include activities such as deterring, denying, interfering, manipulating, degrading, disrupting or destroying the computers, information, or communications systems, networks and information infrastructures of a malicious actor or adversary. The effects of a cyber operation can range from subtle to destructive. (R)

There are a wide range of potential applications for cyber operations including law enforcement, counter-terrorism, and military uses of across a range of NZDF operations. (R)

In the face of widespread use of technology, these tools are increasingly necessary because of the limitation of established lawful means of response and the difficulties of taking cross-border action. (R)

In a counter-terrorism context, cyber operations could be used to interfere with the internet communications or website of a terrorist group. (R)

A particular area of focus for NCPO is whether the legal framework is keeping up with technological change, an area of interest under New Zealand's 2018 Cyber Security Strategy. (R)

Defence (externally focussed)

New Zealand also has Defence related policy that relates to countering online extremism. The Ministry of Defence supports the Government to develop and give effect to New Zealand's Defence policy, including in relation to Government's policies and expectations for Ministry of Defence and NZDF activities that relate to countering online extremism. (R)

Currently, this is not an active area of policy work for the Ministry, either in the broader policy sense or in relation to particular Defence activities. (R)

The MoD does, however, have a range of work-streams on countering extremism and terrorism more generally (notably in relation to South East Asia and the Middle East). They also have an active policy programme examining Defence's role in relation to cyber issues. Issues relating to countering online extremism come up – including when engaging with international partners – during the course of these activities. (R)

The NZDF is working on strategic level policy framework to bring agencies working on particular issues together, and help look at issues holistically. Work is currently in progress with a projected time frame of 2-3 years. (R)

s6(a)

Community & civil society

Community and civil society engagement is aimed at maintaining trust and confidence, and demonstrating openness and accountability. It is part of broader engagement and CVE activity. (R)

Police also undertake some interactions with community groups and human rights groups around any concerns about the use of counter terrorism legislation to address concerns that it may be anti-Muslim as opposed to offence specific. (R)

DIA is working across a number of government and non-government agencies in a project that uses search terms to encourage a social intervention. Inputted search terms are used to nudge individuals to a help page offering non-judgemental, free counselling. Jigsaw, a Google subsidiary, is enabling this work by allowing the project to use Google to advertise the help page. This project is primarily concerned with child sexual offenders but learnings from it are relevant to online CVE. (R)

International engagement

Our international relationships are important when dealing with extremist content online, as partners internationally are reliant on each other to remove content that is hosted in partner countries. (R)

A key challenge of international engagement work is reconciling the spectrum of views on enforcement/removal of content, freedom of speech and respect for human rights, and ability of governments to respond and operate effectively in a fast-moving environment s6(a) . (R)

International engagement by New Zealand agencies is predominantly aimed at sharing best practice in countering violent extremism online and supporting the development of international norms which reflect New Zealand values. (R)

MFAT, in coordination with security sector agencies, engages on issues related to countering violent extremism online in a variety of fora, including multilateral bodies such as the UN and in our bilateral and regional engagement with other states. MFAT has also welcomed the establishment of the Global Internet Forum to Counter Terrorism, which is a private sector response to the challenges of online extremism and extremist content. A New Zealand delegation attended the Global Internet Forum to Counter Terrorism and Tech against Terrorism launch event in June 2018. (R)

Police is a major player in New Zealand's international CVE contributions, particularly through long standing law enforcement and capacity-building relationships in South East Asia. NZP also participates in and contributes to international discussions addressing the threat of terrorist use of the internet, whether through/alongside MFAT or dedicated streams of international engagement such as the Five Eyes Law Enforcement Group (FELEG). (R)

Outcomes include pressure on content providers, although it is not clear if outcomes are specifically through New Zealand engagement or we are part of the overall pressure. Occasionally, New Zealand agencies also receive technical and other support and assistance from partners, such as training opportunities. (R)

Online exploration

Extremist content viewed on the internet is dealt with in one of two ways, depending on where that content is hosted. (R)

If the content is hosted abroad (for example, on YouTube or Facebook), New Zealand agencies can approach private sector companies or partner agencies to facilitate the removal of the content. The Police, for example, flags content to providers when they are alerted to it. (R)

If the content is hosted in New Zealand, the Censorship Compliance Unit at DIA facilitates the removal of extremist content online. Around 500 CT/CVE cases a year are dealt with by the Unit. (R)

New Zealand hosted extremist content is identified by the team or by overseas organisations such as the Internet Referrals Unit in Europol, who contact the Unit to facilitate removal of content. If the situation is urgent, they can ensure that content is removed within 15 minutes. (R)

The Unit has a mandate to use Section 3 of the Films, Videos and Publications Classification Act to take down criminal or terrorist activity and publications that are hosted in New Zealand, or where the hosting location is not clear. Content that the Unit deals with is mainly hosted on Mega or Zapi Hosting and they have a good working relationship with Mega. (R)

Online interaction & communication

When individuals begin to interact and communicate with others online about their extremist beliefs, ideologies and aims, it is possible their online activities will come to the attention of government agencies with the legislated mandate to investigate. Several agencies are involved with this process. (R)

New Zealand Intelligence Community

The trend of using the internet to support activities of security concern has been reflected in New Zealand, with individuals of counter terrorism concern in New Zealand s6(a)

s6(a)

s6(a)

s6(a)

GCSB works closely with NZSIS in support of their CT investigations. s6(a) s6(a) Beyond that, GCSB works closely with FVEY CT partners to understand the threat picture as they see it, and to stay across the latest FVEY CT tradecraft, which in turn helps the GCSB to better support NZSIS. (S)

s6(a)

Police and DIA

As well as engaging with individuals of concern, there is also significant open source intelligence gathering related to the online activities of persons of interest and potential persons of interest, much of which is undertaken by the Police. (R)

When handling content removal, the Censorship Compliance Unit at the Department of Internal Affairs s6(c)

Police will be developing operational policies and tradecraft in regard to many of these areas, but this is not scheduled and is envisaged as part of ongoing operational capacity development. (R)

New Zealand Defence Force

NZDF supports New Zealand Police s6(a) s6(a) through Op SOLAR. (S)

OP SOLAR is the New Zealand Government inter-agency contribution to Operation Gallant Phoenix (OGP), a s6(a) intelligence fusion centre s6(a)

OGP is an intelligence mission; s6(a), s6(b)(i)

The immediate focus for the OGP mission is s6(a), s6(b)(i) This is achieved through partner nation collaboration s6(a), s6(b)(i) s6(a)

s6(a)

s6(a)

Action & sentencing

The investigation of terrorist acts using the online realm can take several forms. Crime can have online aspects, such as where recruitment (for example) involves online activity and therefore evidence. Activity can also be purely related to online activity, such as the collection, creation, or dissemination of information. (R)

Police undertake investigation of potential criminality in terms of extremism and supporting intelligence gathering. (R)

s6(c)

The online environment is hard to navigate from a policing perspective, with people making statements and other activity online that they do not necessarily intend to enact in the physical world, also with the potential of broadcasting to a wide audience live, and the need to manage any potential threat. It can also be hard to identify who the actor is. (R)

Post-sentencing management

A tailored, case-by-case approach is used to manage individuals post-sentencing. (R)

The main tools used in relation to use of the internet are special conditions regarding internet access for sentenced prisoners who are community-based. This activity is aimed at preventing re-offending and further victimisation, and to hold offenders to account and ensure compliance with sentence. (R)

This work is not solely focused on CVE online activity as it is a standard practice for offenders who utilise computers and the internet in their offending e.g. fraud, child sex offenders. The Department of Corrections use existing tools in a CVE content, and have extended the use of these conditions for individuals of National Security interest where computers/the internet etc. use contributed to their offending. (R)

These conditions include prohibiting possession or distribution of extremist material, limiting access to internet enabled devices unless approved and supervised, and allowing the monitoring of online activity. (R)

s6(c)

In 2011, DIA undertook a trial of software that monitored offenders' access to websites. Again this was in relation to child sexual offenders but offered learnings relevant to CVE. For a number of reasons, however, the trial was not taken further. (R)

Document 4

Coversheet for SIB Item 3

Meeting Date: 13 July 2016

Responsible Agency: DPMC (NSP)

Title: The violent extremism landscape and New Zealand's response, at home and abroad

Purpose

1. This item is intended to support a strategic discussion by the SIB on both New Zealand's overarching governance arrangements for counter terrorism; and, the nature and scale of the New Zealand government's response to violent extremism, both at home and abroad.

Action Required

2. For discussion and direction setting

Comment

3. At the May meeting of SIB, members requested that the SIB forward agenda of strategic discussion topics include a conversation on:

   i. the future of the Counter-terrorism Coordination Committee (CTCC) and, therefore, a recommended approach to governance of the counter-terrorism space; and

   ii. the domestic and international dimensions of the Islamist-inspired violent extremism phenomena, and what New Zealand's strategy should be to prevent/counter violent extremism (P/CVE), both at home and as part of the global response.

SIB Senior Officials Meeting

4. At their regular monthly meeting held on Thurs 30 June, SIB senior officials recognised the urgent need for agencies to grip up New Zealand's counter terrorism (CT) arrangements in line with ministerial expectations. Several members noted the continuing absence of an overarching CT strategy for New Zealand, despite at least two attempts to deliver one in recent times. As such, while the CT governance structure proposed by DPMC (NSP) looked good, the need for an overall narrative tying all of the nine elements together and articulating what New Zealand is seeking to achieve remains.

5. The Chair, Howard Broad, signalled his intention to propose to SIB CEs that overarching leadership of counter terrorism in New Zealand would sit better with an operational agency such as Police. This is contrary to the current situation where DPMC plays this role. In the ensuing discussion, the group recognised that transferring CT leadership to Police did make sense, but acknowledged the significant additional burden on Police resources that would result. All agreed that a key, and perhaps determinative, element, yet to be resolved is who the lead Minister is for CT.