Document 1

Request Doc ONE

~~RESTRICTED~~

DEPARTMENT
of the PRIME MINISTER
and CABINET

BRIEFING: Foreign Interference – Brady Report and Canberra Visit

Date:	11 December 2017	Tracking number:	1718NSP/033
Security classification:	**RESTRICTED**	Priority:	Medium
Action sought:	Noting	Required by:	12 December 2017

Contact for telephone discussion (if required)				
Name	**Position**	**Telephone**		**1st contact**
Howard Broad	Deputy Chief Executive, Security and Intelligence	s9(2)(a) [redacted]	s9(2)(a) [redacted]	✓
s6(a) [redacted]	Director, National Security Policy			
s6(a) [redacted]	Senior Policy Advisor, National Security Policy			

Minister's office to complete:

□ Approved
□ Noted
□ Seen
□ See Minister's Notes

□ Declined
□ Needs change
□ Overtaken by Events
□ Withdrawn

Comments:

DEPARTMENT
of the PRIME MINISTER
and CABINET

BRIEFING: Foreign Interference – Brady Report and Canberra Visit

Date:	11 December 2017	Tracking number:	1718NSP/033
Security classification:	**RESTRICTED**	Priority:	Medium
Action sought:	Noting	Required by:	12 December 2017

Purpose

To provide you with advice on public commentary regarding foreign interference in New Zealand, and s6(a) A classified annex is attached.

Together these notes will inform your discussion with officials on Tuesday 12 December 2017.

Recommendations

The Department of the Prime Minister and Cabinet recommends that you **note** the contents of this briefing and the attached classified annex (1718NSP/038).

Howard Broad
Deputy Chief Executive, Security and Intelligence
Department of the Prime Minister and Cabinet
11 December 2017

Rt Hon Jacinda Ardern
Minister of National Security and Intelligence

Date: 12 / 12 /17

Summary

1. In September 2017, Professor Ann Marie Brady of the University of Canterbury published a report titled *Magic Weapons: China's political influence activities under Xi Jinping* (the Brady Report) which has since been the topic of some public commentary. The Brady Report presented an overview of the coordinated acceleration and expansion of Chinese political influence activities worldwide, including a focused case study on the extent of these activities in New Zealand.

2. Independently of the Brady Report, officials are concerned about the apparently significant extent of foreign interference activity in New Zealand, s6(a) [redacted] and the cumulative threat this poses to our national interests (i.e. our sovereignty, national security, economy, and international relationships).

3. Recently, the Security & Intelligence Board of ODESC established a cross-agency foreign interference working group led by the Ministry of Business, Innovation and Employment (MBIE). That group's mandate is to identify the scale and scope of this issue and to coordinate any policy response.

s6(a) [redacted]

The Brady Report identified accelerated foreign interference activities occurring in New Zealand

6. Brady offers a number of explanations for China's interest in New Zealand, including:

- our responsibility for the defence and foreign affairs of the Cook Islands, Niue and Tokelau means we can potentially offer four votes for China at international fora;
- New Zealand has "an international reputation as a hotspot for global money laundering";
- New Zealand is a claimant state in Antarctica and one of the closest access points;
- we have cheap arable land and a sparse population, and provide a significant share of China's milk imports; and
- New Zealand is useful for near-space research.

7. The Brady Report claims that China is targeting New Zealand – along with other nations – with a concerted foreign interference campaign which aims to encourage support for the Chinese Communist Party's (CCP) political and economic agendas by co-opting political and economic elites. Brady asserts that these covert and coercive political influence activities (known in China as 'united front' work) in New Zealand are at "a critical level", reflecting China's interest in this country.

8. Specifically, the Brady report claims that:

   - The CCP seeks to establish a China-centred economic order through its Belt and Road initiative, and uses foreign interference activities to cultivate support around the world for this initiative
   - New Zealand has been a testing ground for China's foreign interference activities in recent years, including:
     - political influence and donations;
     - efforts to bring Chinese language media under the control of the CCP with the intent to suppress dissent in the Chinese community; and
     - the use of mergers, acquisitions and partnerships to acquire local influence and to gain access to technology and strategic information.

9. Brady has publicly called for the government to initiate a suite of legislative and policy reforms to protect New Zealand's interests and protect against inappropriate foreign interference more broadly. She has repeatedly pointed to the efforts now being taken by our Australian counterparts to address this issue.

New Zealand has established a cross-agency foreign interference working group to understand the threat and lead a balanced policy response

10. Independently of Brady's claims, officials are concerned about the apparently significant extent of foreign interference activity in New Zealand, s6(a) [redacted] Left unaddressed, this activity may pose a cumulative threat to our national interest (i.e. our sovereignty, national security, economy, and international relationships).

s6(a) [redacted]

12. To ensure a careful and dispassionate analysis of the issue, the Security and Intelligence Board of ODESC established a cross-agency working group led by MBIE, and including DPMC, Treasury, MFAT, MPI and others. This group has been tasked with developing an economic policy framework for responding to foreign interference, which considers both opportunities and risks.

13. The group's initial objective is to establish an understanding of the nature, scope, and scale of foreign interference risks in New Zealand, with a view to setting out a case for change as part of a balanced and proportional response to these risks (whether through legislation, regulations, operational programmes and initiatives, or a mix of the above).

14. The group's overall goal is to support Ministers in ensuring New Zealand's regulatory regime provides individuals, businesses and government institutions with the tools and confidence to conduct their affairs without inappropriate foreign interference.

15. We are separately working with the Ministry of Justice to consider more specific legal and justice-related issues relating to foreign interference. This work is in its infancy, but will likely include considering whether the setting in the Electoral Act 1993 around foreign-sourced donations are still appropriate, and whether the risk of foreign interference might require additional treatment.

s6(a)

[redacted]

18. The Australian government has recently announced a number of broad national security measures that will, among other things, strengthen its ability to counter foreign interference. While related to foreign interference, these measures were not specifically in response to this issue.

19. In July 2017, Prime Minister Turnbull announced a package of organisational reforms that seeks to establish more enduring and better integrated intelligence and security arrangements. It includes:

- the establishment of an Office of National Intelligence as the principal intelligence advisory agency to the Prime Minister, responsible for the strategic development and management of the Australian Intelligence Community;

- the creation of a Home Affairs portfolio (similar to the Home Office of the UK) including immigration, border protection, and domestic security and law enforcement, which will be responsible for providing strategic planning and coordination for a network of independent security and law enforcement agencies; and

- strengthened oversight powers for the Attorney-General, and incorporation of an Inspector-General of Intelligence and Security and the Independent National Security Legislation Monitor within the Attorney-General's portfolio.

20. Further, in January 2017 the Australian government established the Critical Infrastructure Centre (CIC), dedicated to managing the national security risks associated with critical infrastructure and foreign investment (i.e. sabotage, coercion and espionage). CIC is responsible for building and maintaining a critical assets register, which will provide a consolidated view of critical infrastructure ownership in high risk sectors across the economy. It will also undertake national security risk assessments and advice to support decision-making on foreign investment transactions.

21. s6(a) [redacted] Prime Minister Turnbull announced the biggest overhaul of espionage and intelligence laws in decades, which will:

- ban foreign political donations;

- force lobbyists working on behalf of other nations to declare their who they are working for; and

- introduce stronger and new criminal penalties for offences including espionage and unlawful interference that would harm the national interest.

s6(a) [redacted]

s6(a)

[redacted]

s6(a)

[redacted]

Ongoing work and next steps

s6(a)

[redacted]

36. The foreign interference working group continues to scope the risks associated with foreign interference, and will report to the Security and Intelligence Board in April 2018.

37. In the interim, officials continue to engage with ongoing work across government with implications for foreign interference, most specifically on reforms to the Overseas Investment Act 2015 being led by Minister Parker. This work provides an opportunity to consider how we identify and manage national security risks arising from foreign investment.

38. There are essentially four streams of work in play. Those are:

- the MBIE work described above;

- work with the Ministry of Justice, to consider whether the settings in the Electoral Act 1993 around foreign-sourced donations are still appropriate, and whether foreign interference necessitates any amendment or addition to existing criminal offences. This work is in its infancy;

- ensuring that foreign interference has an appropriate profile in our National Intelligence Priorities, s6(a)
- ensuring that we are using our complete information holdings to get the best understanding of what is taking place, s6(a)

Document 3

Request Doc THREE

DEPARTMENT OF THE
PRIME MINISTER AND **CABINET**
TE TARI O TE PIRIMIA ME TE KOMITI MATUA

Memo

OUR PARTING THOUGHTS AND WISHES FOR THE NATIONAL SECURITY SYSTEM

To	The Prime Minister / Minister for National Security and Intelligence	**Report No**	1819NSPD/064
From	Andrew Kibblewhite and Howard Broad	**Date**	18/12/2018

Purpose

1. In January, we will both be finishing our roles in DPMC and, failing some unscheduled security event, 19 December is our last official face-to-face national security meeting with you. We would like to use some of that time to share our thoughts on some of the key risks and issues that relate to the national security system.

Comment

2. Of the range of risks and issues facing the national security system, we feel that the following are the most pressing and will require attention in 2019:

   a. Getting the National Risk Register work over the line

   b. Enabling Ministers to work strategically and collaboratively to manage risks

   c. Protecting our relationships with our partners

   d. Increasing New Zealand's s6(a) [redacted] in the Pacific

   e. Establishing the National Emergency Management Agency (NEMA)

   f. Continuing to strengthen the role and presence of DPMC's National Security Group

Getting the National Risk Register work over the line

3. A primary objective inspiring both of us in our DPMC roles has been to complement the well-practiced ODESC response approach with a more strategic, longer-term focus. Our thinking, reinforced by some strong advice from the Auditor-General, was that adopting a proactive risk management approach would best enable that objective. With much better knowledge about the kinds of risks that affect New Zealand's national security, we can better manage them to ensure our continued success and overall resilience as a nation.

4. DPMC developed a register based on a comprehensive assessment of our national security environment. The register enables better identification, understanding, comparison, and management of national risks. It is also a useful tool to help us think about emerging risks

facing New Zealand (specifically those that may manifest in the decades to come) so we can develop appropriate policy interventions for them *before* an unforeseen event or crisis strikes.

5. We are proud of the progress that DPMC has made on the national risk register front. Part of that progress has been building regular risk conversations into the architecture of the strategic coordinating committees of ODESC, (the Security and Intelligence Board (SIB) and the Hazard Risk Board (HRB)) to ensure Chief Executives jointly take responsibility for profiling and comparing risks and offering advice to Ministers on where action might be necessary.

6. We would like to see the risk work used more broadly within agencies, not just at the system governance level. Our concern is that if the register is not given the appropriate Government mandate in 2019, we will lose the gains we have made in this area. This would be unfortunate, because the strength of the register lies in the standardised approach it uses to assess national risks, which allows 'all hazards – all risks' to be measured in comparable ways. A Government mandate will provide the push needed to truly embed this approach at all levels across the national security system.

7. We developed the National Risk Report (the report) as a public-facing summary of the register. The report encourages key decision makers to have open conversations about managing national risk. We think that a wider dialogue with New Zealanders will support a risk and resilience-based approach to national security by normalising issues that can often seem quite scary or removed from most people's daily lives. In our view, the New Zealand public is ready for this conversation, and having the conversation with the public will enhance New Zealand's overall resilience.

8. s9(2)(g)(i) [redacted] We believe that this Government in fact has a positive story to tell in this regard. The two reports we recently sent you from SIB and HRB show the many actions Ministers and national security agencies have taken in response to identified risks. This is a good news story and one that supports the transparency aspirations of your Government.

9. s9(2)(g)(i) [redacted] There are also high expectations around the release of the report, from academics, journalists, local government, and others and not proactively publishing the report will likely force its release through Official Information Act channels. If this happens, we could also lose control of the narrative around the report's purpose and benefit to New Zealand.

10. As such, we would recommend that you pursue the report's release at a suitable time in the first half of 2019 to:

    a. Facilitate a discussion that is open to the public about the spectrum of national risks, how they are broadly assessed, and outline the steps government is taking to better manage them; and

    b. Signal the continued move towards a proactive national security system.

Enabling Ministers to work strategically and collaboratively to manage risks

11. s6(a), s9(2)(g)(i) [redacted]

s6(a), s9(2)(g)(i)

12. [redacted]

Protecting our relationships with our partners

13. s6(a) [redacted]

14.

15.

16.

Increasing New Zealand's s6(a) [redacted] *in the Pacific*

17. s6(a) [redacted]

18. National security agencies are already working hard in the Pacific to strengthen our relationships and support Pacific countries undertake these building processes. Some examples include:

- s6(a) [redacted] The New Zealand Defence Force's Pacific-wide involvement in readiness and responses exercises for severe weather events or regional insecurity. s6(a) [redacted]

- The work underway to promote Pacific security capacity and leadership by rolling out leadership capacity training across the Pacific public security sector; building Pacific security capacity and capability within Pacific Island countries in cybersecurity, biosecurity, law enforcement, maritime domain awareness, border management and security enforcement, and developing Pacific Island countries' national security system response strategies.

- Plans are in place for New Zealand agencies to support Pacific countries build up their own Protective Security Requirement settings to ensure they can better collect, retain, and receive (from New Zealand) classified security information.

- s6(a) [redacted]

19. s6(a) [redacted]

20.

21.

Establishment of the National Emergency Management Agency (NEMA)

22. An important function in achieving national security is responding effectively to emergencies when they occur. The system must be ready and able to respond, and support recovery when required, to emergencies across all hazards and risks.

23. We support the establishment of a National Emergency Management Agency (NEMA) to replace the Ministry of Civil Defence and Emergency Management. We think NEMA should be a Departmental Agency to give it the Ministerial control and oversight it needs during emergencies, while also providing the required mana and greater autonomy to deliver on its set of functions, particularly in non-emergency times. We support NEMA being hosted within DPMC to support the 'all hazards/all risks' approach and the ODESC system but we note that a case can be made to shift NEMA to the Department of Internal Affairs.

24. s9(2)(g)(i) [redacted]

25. The flow-on implications of the NEMA decision (including uncertainty for MCDEM and DPMC staff and keeping the wider emergency management system reform process on track) are such that an early decision about its location will be beneficial.

Continuing to strengthen the role and presence of DPMC's National Security Group (NSG)

26. The security and intelligence activities are spread across many aspects of government, and it is NSG's role to ensure that there is a whole of system view of risks, priorities and actions, and where system performance can be improved.

27. The year ahead will provide opportunities to further extend the NSG's role and influence, including through playing a stronger convening and leadership role on key issues like Foreign Interference, s6(a) [redacted], and cyber security.

28. NSG will oversee and coordinate the implementation of the National Security and Intelligence Priorities, and will lead the continuous improvement of ODESC's strategic boards (SIB and HRB), focusing on building system health and system stewardship.

29. We would like to see the NSG become a powerhouse for coordinated, high-quality advice on intelligence and national security matters. Often this will cut across other agencies' and Ministers' portfolio areas. We stress that this is not asserting tight control over all national security issues but rather about providing an independent 'system' view on issues and providing more effective support to ease the collective burden on agencies.

Recommendations

30. We recommend that you note the contents of this memo.

Andrew Kibblewhite
Chief Executive

Department of the Prime Minister and Cabinet

Howard Broad
Deputy Chief Executive, Security & Intelligence

Department of the Prime Minister and Cabinet

NOTED

To Rt Hon Jacinda Ardern

Prime Minister / Minister for National Security and Intelligence

Date: / / 2018

Document 3

Request Doc THREE

DEPARTMENT OF THE
PRIME MINISTER AND **CABINET**
TE TARI O TE PIRIMIA ME TE KOMITI MATUA

Briefing

QANON – DESIGNATION AND DIS-INFORMATION

To Prime Minister (Rt Hon Jacinda Ardern)			
Date	1/10/2020	**Priority**	Routine
Deadline	N/A	**Briefing Number**	2021NSP/014

Purpose

This briefing provides advice on whether QAnon meets the criteria for designation as a terrorist entity under the Terrorism Suppression Act 2002, and details upcoming work on combatting dis-information.

Recommendations

1. **Note** that it is considered that QAnon does not meet the criteria for designation as a terrorist entity
2. **Note** that DPMC and the Department of Internal Affairs are currently scoping a strategic framework to strengthen New Zealand's resilience to disinformation

Tony Lynch **Deputy Chief Executive,** **National Security Group**	Rt Hon Jacinda Ardern **Prime Minister**
1./10/2020	4./10/2020

Contact for telephone discussion if required:

Name	Position	Telephone	1st contact
Tony Lynch	Deputy Chief Executive, National Security Group	s9(2)(a) [redacted]	✓
Dan Eaton	Director, National Security Policy Directorate	[redacted]	

Minister's office comments:

- ☐ Noted
- ☐ Seen
- ☐ Approved
- ☐ Needs change
- ☐ Withdrawn
- ☐ Not seen by Minister
- ☐ Overtaken by events
- ☐ Referred to

QANON – DESIGNATION AND DIS-INFORMATION

Purpose

1. This briefing provides advice on whether QAnon meets the criteria for designation as a terrorist entity under the Terrorism Suppression Act 2002, and details upcoming work on combatting dis-information.

QAnon

2. QAnon is an extremist ideology, based on a conspiracy theory which alleges that Western governments are corrupt and enable (or perpetuate) widespread child abuse. Followers believe that clues to the extent of the conspiracy are detailed online by a person within the US Government, with a Q-level security clearance. A wide and inconsistent range of beliefs flow from this central tenet, including opposition to 5G, anti-Semitism, and white nationalist views.

3. QAnon-linked conspiracy theories have found support within some communities in New Zealand, largely linked to the proliferation of COVID-related disinformation coming out of the US during our periods of lockdown.

4. Anti-mask and anti-lockdown narratives couched in broad human rights and basic freedoms terms (and often grounded in narratives linked to the US Constitution), have proven to be one such vector for broader conspiracy theories with links to QAnon narratives. Some of these theories have included that the New Zealand government was intentionally withholding information from the public, that the government was utilising the pandemic to impose martial law or otherwise erode human rights, and that the outbreak was intentionally planned to manipulate the election.

5. s9(2)(g)(i) [redacted]

Criteria for designation

6. You have asked whether QAnon should be designated as a terrorist entity. Section 22 of the Terrorism Suppression Act (TSA) provides for entities to be designated as a terrorist entity, if the Prime Minister believes on reasonable grounds that the entity has knowingly carried out, or has knowingly participated in the carrying out of, one or more terrorist acts. Designation therefore requires the existence of an entity and the carrying out of one or more terrorist acts which can be attributed to that entity.

7. s6(a) [redacted]

8. These criteria are addressed in turn below. The advice provided is preliminary, and has not undergone a full legal analysis or consideration by the Security and Intelligence Board.

Is QAnon an entity?

9. Section 4 of the TSA defines an entity as 'a person, group, trust, partnership, or fund, or an unincorporated association or organisation'. There is no further detail within that legislation as to what constitutes an entity, but we consider that of these options, QAnon is most likely to be considered a group.

s9(2)(g)(i) [redacted]

Has QAnon carried out a terrorist act?

13. In order for this criteria to be met, one or more terrorist acts must be carried out and be directly attributable to the entity itself. Section 5 of the TSA defines a terrorist act as an act intending to cause:

- the death of, or other serious bodily injury to, 1 or more persons (other than a person carrying out the act):

[1] A v Secretary of State for the Home Department 2004

- a serious risk to the health or safety of a population:

- destruction of, or serious damage to, property of great value or importance, or major economic loss, or major environmental damage:

- serious interference with, or serious disruption to, an infrastructure facility, if likely to endanger human life:

- introduction or release of a disease-bearing organism, if likely to devastate the national economy of a country.

14. The terrorist act must also be carried out for the purpose of advancing an ideological, political, or religious cause, and with the intention to induce terror in a civilian population or unduly compel or to force a government or an international organisation to do or abstain from doing any act. 'Carried out' includes planning or preparation, or a credible threat to carry out an act.

s9(2)(g)(i) [redacted]

s6(a), s9(2)(g)(i) [redacted]

s9(2)(g)(i) [redacted]

What can be done about QAnon?

19. Countering an ideology, particularly one whose mode of transmission is through disinformation, is extremely difficult. Firstly, most disinformation is legal (unless it calls for violence or promotes hate speech) and is protected by freedom of expression laws. Secondly, direct counter-narratives can serve to highlight and reinforce the disinformation or conspiracy theory and give credence to its proponents. And strong government-led opposition (including Ministerial statements) can bolster people's belief that they're "challenging the mainstream narrative" and "speaking truth to power".

20. Available research and international experience suggests that efforts to mitigate the effect of disinformation must be based on open principles of transparency, integrity, accountability and stakeholder participation. They must also uphold the principles of a

free, secure and open internet, privacy and New Zealand's human rights commitments, including freedom of expression.

21. While some work has been done within the New Zealand government, academia and in the media to understand COVID-related disinformation and to build public resilience to it, at present there is no lead agency to coordinate this work and to address the broader impacts of disinformation.

22. DPMC and the Department of Internal Affairs are currently scoping work for a strategic framework to strengthen New Zealand's resilience to disinformation. Agencies intend to seek Cabinet approval by the end of the year to develop this. The framework may include recommendations for:

    a. a coordination body, to ensure that government communications effectively get ahead of disinformation curves (e.g. ensuring the public has the right information on COVID vaccines well before they become available and disinformation campaigns take hold);

    b. referral mechanisms, for disinformation that crosses thresholds into criminal or extremist behaviour and requires a censorship or enforcement response; and

    c. a broader civil society and academia led multi-stakeholder approach to monitoring disinformation, engaging with tech platforms, and to building public awareness, critical thinking skills and online media literacy.

Next Steps

23. DPMC, working with the Department of Internal Affairs and other relevant agencies, will provide a briefing on dis-information to Ministers following the formation of a government after the 2020 General Election. Subject to Ministers' views, Cabinet approval would be sought to develop a comprehensive, multi-stakeholder strategy on disinformation and misinformation. Seeking Cabinet approval would ensure visibility across the full range of Cabinet portfolios potentially impacted, and would provide the mandate for a coordinated whole-of-system approach to responding to this problem.

s9(2)(g)(i)

[redacted]

Document 4

Request Doc EIGHT

DEPARTMENT OF THE PRIME MINISTER AND CABINET
TE TARI O TE PIRIMIA ME TE KOMITI MATUA

Briefing

POLICY LEVERS FOR ADDRESSING MIS/DISINFORMATION

To: Rt Hon Jacinda Ardern, Prime Minister and Minister for National Security and Intelligence

Date	9/03/2022	**Priority**	High
Deadline	16/03/2022	**Briefing Number**	DPMC-2021/22-1604

Purpose

To provide you with some further information about potential policy levers, including through international coordination, to address online mis/disinformation networks and their impacts on Aotearoa New Zealand. This responds to your request during the National Security and Intelligence meeting with DPMC officials on 2 March.

Recommendations

1. **Note** the contents of this brief;
2. **Provide** feedback on the range of options provided; and
3. **Discuss** with DPMC officials options for managing and progressing this work. **YES / NO**

Tony Lynch
Deputy Chief Executive,
National Security Group

..../..../....

Rt Hon Jacinda Ardern
Prime Minister
Minister for National Security and Intelligence

..../..../....

Anneliese Parkin
Deputy Chief Executive, Policy

09/03/2022

Contact for telephone discussion if required:

Name	Position	Telephone	1st contact
s9(2)(g)(ii) [redacted]	Manager, Security & Intelligence Policy National Security Group	s9(2)(a) [redacted]	✓
s9(2)(g)(ii) [redacted]	Christchurch Call Coordinator PM's Special Representative on Cyber and Digital		

Minister's office comments:

- ☐ Noted
- ☐ Seen
- ☐ Approved
- ☐ Needs change
- ☐ Withdrawn
- ☐ Not seen by Minister
- ☐ Overtaken by events
- ☐ Referred to

POLICY LEVERS FOR ADDRESSING MIS/DISINFORMATION

Executive Summary

1. Mis/disinformation is not a new problem.[1] It has been around in various forms throughout history. But the arrival of mass social media has enabled mis/disinformation to be scaled at a global level for the first time, delivering an asymmetric tool for manipulation of large groups of people across borders and geographical distances, with limited traceability and at very low cost.

2. New Zealand, like many of our likeminded partners, has been impacted by networks that disseminate harmful mis/disinformation. This has affected for example the public health response to COVID-19. It has also manifested in more sinister ways, leading to radicalisation of at-risk individuals, threats and intimidation of people in our communities, and as a vehicle to undermine trust in democracy, media, and the institutions of government.

s9(2)(g)(i)

4. There are no easy solutions. Our approach will need to be comprehensive and long-term to build resilience within society to manage future mis/disinformation topics. New Zealand is not alone in recognising the nature of the problem and grappling with appropriate ways to address it. s9(2)(g)(i)

5. Mis/disinformation networks employ a range of strategies to get their message across. An effective response will also need to play out across multiple channels and elements. Broadly, an effective response requires effort across four areas:

   a) Coordinated identification of networks and narratives;
   b) Strategic communications and engagement;
   c) Exposure and disruption of mis/disinformation networks; and
   d) Building resilience to mitigate vulnerabilities.

6. This paper looks at an initial set of possible approaches within these four areas. While regulatory systems can be helpful, they have limitations in this context and cannot be the whole answer.

7. The Department of the Prime Minister and Cabinet (DPMC) recommends an approach that is: clearly mandated, coordinated and led from the centre, engaging a range of government agencies with expertise in the digital environment, law enforcement, national security and

[1] For the purposes of this briefing we use the term mis/disinformation to refer to the spectrum of false and misleading information. Misinformation is information that is false, but not created with the intention of causing harm. Disinformation is information that is false and deliberately created to harm a person, social group, organisation or country.

intelligence, and the social sector, alongside the private sector, the internet community, tangata whenua, civil society, and other community representatives. This "whole of society" approach would need dedicated resources and the ability to steer a combined cross-government and multi-stakeholder effort. It would need to be staffed by people with a deep understanding of internet governance and the technology sector, the security aspects, how different communities respond to mis/disinformation, and the international context. s9(2)(g)(i) [redacted]

s6(a), s9(2)(j) [redacted]

9. In terms of DPMC resourcing, we would need to be careful if you wish to take this forward that mis/disinformation work is adequately resourced and that it mutually reinforces, rather than impinges on, the work of related programmes. s6(a), s9(2)(j) [redacted] As with the Christchurch Call, our view is that this work should not be led solely by the security sector (i.e. we wish to avoid securitising this issue). The work will require strategic coordination across a range of sectoral work streams.

Purpose

10. To provide you with some further information about the potential policy levers, including through international coordination to address online mis/disinformation networks and their impacts on Aotearoa New Zealand. This responds to your request during the National Security and Intelligence meeting with DPMC officials on 2 March.

Mis/disinformation leads to a range of harms...

11. Mis/disinformation has emerged as a complex security issue around the world. The development of online tools and social media environments that enable mass participation has enabled the spread and promulgation of mis/disinformation, with implications that governments and democratic societies have been relatively slow to recognise.

12. There are potentially harmful effects from the spread of mis/disinformation. At the most acute end of the spectrum these harms include threats to public safety, incitement of criminal or violent extremist activity, breakdown of social cohesion, and efforts to undermine democratic institutions. Mis/disinformation can play a role in recruitment and radicalisation strategies of violent extremist groups. It can also be a tool of corporate or State influence or driven by ideologically motivated groups. Unwitting accomplices are often involved in the dissemination of misinformation online. Distinguishing innocent participants from the nodes of deliberate and coordinated inauthentic behaviour can be difficult.

13. The impacts in New Zealand have become significant, exacerbated by the effects of the COVID-19 pandemic. While a full analysis is yet to be carried out, mis/disinformation appears to have played a significant role in the February 2022 occupation of Parliament grounds and

associated violence and intimidation towards lawmakers, the media, academics, authorities, officials, and the general public. Researchers, civil society groups, tangata whenua, and the internet community have for some time expressed concern about the impacts. s9(2)(ba)(i) [redacted]

14. Mis/disinformation networks are driven by a range of actors. State-sponsored disinformation is a particular problem, with Russia s6(a) [redacted] among the prominent actors involved. RAND Corporation (a United States-based think tank) describes Russian disinformation as a 'firehose of falsehood' because it is distributed at immensely high volume across multiple channels and has no commitment to internal consistency. 'Striking first' and using multiple networks to relay a message gives an informational advantage that is difficult to counteract. Intimidation and harassment are often used to suppress counter speech.

15. Money also plays an important role, because of the potential to monetise mis/disinformation content as a revenue source (for extremist groups and grifters alike) and as a means of financing the production, dissemination, and promotion of mis/disinformation. The economics of mis/disinformation are largely obscure, although it appears those who profit from and finance mis/disinformation frequently operate at a safe distance from those most impacted by it.

16. Mis/disinformation networks can also be driven by a range of other factors, including charismatic online personalities, development of a sense of community or shared knowledge, relatively complex psychological phenomena (including e.g. "rabbit-holing" – the descent into belief in bizarre, improbable or conspiratorial theories; or "brigading" – where groups engage in coordinated attacks on others), and genuinely held ideological beliefs (some moderate, others less so).

17. Addressing these problems is particularly challenging, whether for governments or communities. This problem set, like the online networks that drive it, is new enough that tried and tested solutions are yet to emerge. Mis/disinformation typically fits within definitions of protected or political speech. Most mis/disinformation is legal – making it difficult to address using traditional law enforcement and intelligence tools before the harms become apparent. Regulatory tools have proved particularly difficult to develop. It can be challenging to trace the financial flows, or to keep up with the shifting patterns of mis/disinformation and their impact.

18. Successfully navigating these issues requires "whole of society" solutions. Governments can't always and shouldn't usually act alone, not least because this may well underpin or reinforce those mis/disinformation narratives that focus on the role and place of government. Working with media, academia, civil society and the private sector – particularly with tangata whenua and a diverse range of communities – will be an essential ingredient in getting ahead of mis/disinformation campaigns and networks and countering them effectively. In theory, working with a broad set of stakeholders should also enable solutions to be developed that draw on a range of tools, while protecting human rights and a free, open and secure internet.

In the lead up to the 'convoy' occupation there were clear signs of mis/disinformation networks looking to incite harm and disorder, hidden in plain sight among what seemed like more typical forms of political protest. Whilst that ambiguity made it more difficult for agencies to focus in on the threat, many community groups and academics were actively calling them out. It's likely that security agencies will continue to struggle as such situations arise in the future.

Countering coordinated mis/disinformation networks requires work across at least four areas…

Coordinated identification of networks and narratives

19. It is essential to have a sophisticated and contemporary understanding and prior knowledge of relevant networks and their likely narratives, tactics, and financial flows, including through compiling open-source information, insights from communities, and overseas partners. Where justified and appropriate, with oversight, insights learned through law enforcement and security and intelligence tools of the State are also important.

Strategic communications and engagement

20. It is important to ensure, working alongside civil society, that effective, clear messaging is available to populate elements of what some state-sponsored actors call the "information space", including through inoculating against or 'pre-bunking' conspiracies; calling out tactics; and providing credible information in a format that is adapted to the target audience.

s6(a)

[redacted]

Exposure and disruption of mis/disinformation networks

21. This includes identifying, exposing, and, where appropriate, disrupting the sources of mis/disinformation. This may involve addressing inauthentic behaviour online through ensuring social media platforms enforce terms of service, content moderation, or developing policy options to pursue the funding sources that drive networks. Slowing the speed or scope of transmission can help provide more space for strategic communications. Addressing mis/disinformation once identified is most difficult in situations where the tools for action are unclear and the content does not meet policy or regulatory thresholds.

Building resilience to mitigate vulnerabilities

22. Building resilience in groups that may be more vulnerable to mis/disinformation campaigns, for example because of economic or social dislocation, can help to reduce the vulnerability to those campaigns. This includes building digital literacy, resilience, and critical thinking into education; supporting public interest media that engages multiple cultures and languages; focusing on open government; and the availability of independent fact-checking or similar tools. Effective service delivery for vulnerable groups is also particularly important, especially where these groups are subjected to threats or intimidation online. Resilience will also come through building expertise and capability within government.

As we witnessed at the convoy occupations, even with longstanding efforts to get ahead of COVID-19 disinformation, existing inequality, social disengagement and mental health issues can create vulnerabilities that are easily exploited by malign actors.

23. While they aren't more susceptible, certain New Zealanders are the targets of significantly higher levels of mis/disinformation, for instance political or religious propaganda aimed at diaspora communities, or efforts to discredit academics, public figures, or experts.

There is a range of policy approaches we could consider

24. A wide range of agencies is involved in efforts to mitigate the consequences of mis/disinformation. As with many digital issues, this diffusion is part of the challenge in responding effectively.

25. Current efforts in Aotearoa New Zealand are largely focused on mis/disinformation related to the COVID-19 response. These efforts are led by DPMC's COVID-19 Group, with support primarily from the Classification Office, CERT NZ (the central coordination point for any COVID-19 cyber security incidents and a public reporting point for mis/disinformation), Netsafe and Te Pūnaha Matatini. s9(2)(g)(i) [redacted]

s9(2)(g)(i) [redacted]

27. There is currently no strategic function to support operations, policy, and overall strategy for either addressing COVID-19 or wider mis/disinformation, or for locating this challenge appropriately in its context as an emergent issue of digital resilience. We recommend a function of this sort to ensure a coordinated government response, including tactical structures, that is adequately directed, resourced, and supported.

28. DPMC considers that **a strategic coordination function supported by a dedicated cross-agency structure** could help to integrate thinking across government, marshal our limited resources, and engage with companies and community groups on combatting harmful mis/disinformation. This function need not necessarily sit in DPMC's National Security Group and should not sit in its COVID-19 Group but should be empowered to work closely with them. Government departments are likely to need specific ministerial direction to contribute effectively to this effort as well as a structure that governs the work across agencies. Multi-stakeholder engagement outside of government will be a vital success factor.

29. New Zealand is not alone in facing up to this challenge. There is much we can learn from partners and the opportunity to contribute to shared efforts. The Nordic and Baltic States have longstanding counter-information warfare capabilities (as part of a "modern deterrence" approach to resilience), while others such as France and Canada are actively assessing how to address the risks around domestic extremism arising from disinformation. Many of New Zealand's likeminded international partners have formed cross-agency taskforces on disinformation, while others have developed specific communications cells and academic/civil society coordination platforms.

30. DPMC recommends looking at **options to partner internationally**, including pursuing aligned regulatory and operational approaches, and to look for consensus and shared action on how social media addresses mis/disinformation. s6(a), s9(2)(j) [redacted]

s6(a), s9(2)(j) [redacted]

31. **Work with online content hosting platforms** can also play an important role in countering mis/disinformation networks, including by:

    a) enhanced efforts to enforce terms of service and community standards as these relate to mis/disinformation, with a particular focus on health information;

    b) prioritising 'high quality' content such as information from qualified experts;

    c) seeking to identify, label, and de-monetise coordinated mis/disinformation;

    d) removing particularly egregious or harmful disinformation and user accounts that promote it;

    e) restrictions on paid advertising to reduce disinformation and give users visibility; and

    f) use of policies that increase the 'friction' and slow the potential rate of propagation of content from new or dubious sources, for example, limiting the scale of re-posting.

32. Some of these practices are already being actively pursued, although there is not yet a clear consensus among industry players on the best tools available to address this problem, their efficacy, or ways to manage the issues the tools create (e.g. concerns around freedom of expression or political responses that seek to force platforms to carry specific content). [redacted]

s6(a), s9(2)(j) [redacted]

33. Transparency by online platforms can also help identify who is behind campaigns, how much money is flowing into and out of those campaigns, and how effective moderation is in countering it. **More granular and localised data on mis/disinformation** identified on online platforms could be especially helpful in addressing it in New Zealand. Similarly, greater transparency from government on takedown requests and engagement with platforms on online harms may assist researchers in this space to better understand the issues and build confidence in the nature of the solutions adopted.

s9(2)(ba)(i), s9(2)(f)(iv), s9(2)(g)(i) [redacted]

35. Alongside improving identification and referral mechanisms, **whether our regulatory systems** provide relevant agencies with appropriate legal powers and tools to respond (such as around the use of open source information) should be considered – but will not be an answer alone. Efforts to **build public sector capability** to understand and respond to the complex range of issues that underpin the mis/disinformation problem will be required to support any enhanced government response to mis/disinformation.

36. **Increasing the resilience of the public is crucial.** Educational efforts, digital literacy, resilience, and online critical thinking capacity, and public interest media need to reach and engage all communities. Social cohesion and policies that address social justice, acute inequality and mental health also reduce the vulnerability of populations to coordinated disinformation campaigns.

There are a range of options available to address current gaps and limitations

37. Given the need to move quickly, DPMC has identified some options that could be pursued, consistent with the areas and themes identified above. While these options have been informed by existing interagency work, they are initial thoughts and have not been consulted widely. They are intended as early advice to inform your thinking.

38. We propose further discussion across DPMC, including on aspects you indicate an interest in pursuing, to be followed by more detailed development and engagement with relevant agencies as work shapes up. This would include consideration of any risks associated with these approaches.

Overall Structure, Resourcing, and Coordination

Current gaps & limitations	Options to address
s9(2)(g)(i) [redacted]	A strategic coordination function with a clear mandate, and resources to work across government and to engage with communities, NGOs, the internet community and the private sector to address mis/disinformation. DPMC's experience to date is that a wide range of agencies will need to be engaged and that a strong steer will be needed to their respective ministers to allocate priority and resources to this work.
s9(2)(ba)(i) [redacted]	Improving support to affected communities, including accelerating the development of options for public reporting and referral of harmful behaviour online.
There is not a clear consensus approach to this issue internationally.	Engagement with likeminded partners to understand what they are doing and how we might work together. s6(a), s9(2)(j) [redacted]

Coordinated identification of networks and narratives

Current gaps & limitations	Options to address
Insights from academia, operational agencies, and communities are not effectively integrated into a unified picture of risks from disinformation. Risks are assessed from a national security perspective, but not necessarily with reference to social cohesion, or the longer-term issues of maintaining trust in democratic institutions.	A multi-stakeholder coordination structure to identify harmful disinformation networks operating in New Zealand. A cross-government and multi-stakeholder network that helps develop and implements strategies to counter these risks.
Absence of consistent high-quality data on the prevalence of disinformation targeting New Zealand-based users. Activity often does not meet the legal, regulatory or national security thresholds for law enforcement and intelligence and security agencies to collect and report on. s9(2)(g)(i) [redacted]	Encourage more regular standardised reporting of country-level, or sub-country-level data on disinformation. This could make use of structures developed under a proposed industry Voluntary Code of Practice, or the Department of Internal Affairs-led Content Regulatory Systems review. Engage and work with non-governmental entities and researchers to provide regular scanning and assessment of the open source mis/disinformation environment landscape, across as many platforms as possible, to provide a system analysis of harmful mis/disinformation in Aotearoa New Zealand. (The COVID-19 Group currently has an open RFP for this, specific to the COVID-19 response; this option would expand that to cover a broader range of types of mis/disinformation.)

Strategic communications and engagement

Current gaps & limitations	Options to address
Current strategic communications approaches are specific to COVID-19 and are not set up or resourced to be enduring or effective outside the COVID-19 response.	Consider establishing an enduring government team to lead and coordinate consistent approaches for building awareness to mis/disinformation and communications responses across government.
Work on public interest media, communications on COVID-19, and DPMC work to engage community groups on preventing violent extremism, capacity	Establish a multi-stakeholder group to integrate thinking on countering mis/disinformation in different communities.

building and counter-narratives, remains siloed and not integrated.	Capacity building for resilience, digital literacy and positive narratives focussed on groups that may be particularly at risk. Identification of 'gaps' including educational content, counter-narrative, or public interest media programming in different languages and formats.

Exposure and disruption of mis/disinformation networks

Current gaps & limitations	Options to address
Legal constraints on the scope of what state agencies can act on makes this a difficult task, particularly where it falls outside the scope of a traditional national security threat. Online platforms and civil society can play an important role here.	Seek advice from relevant agencies on what they can currently do in this space and what a more integrated response might look like. Investigate additional legal powers, if they are considered appropriate. Discuss further with international partners in government, civil society and the private sector to identify possible approaches that are consistent with human rights law and a free, open and secure internet. Look for aligned approaches with likeminded partners, including EU member states.
The economics of mis/disinformation flows are poorly understood, but the profitability of certain types of mis/disinformation appear to play a role in developing and amplifying harmful content, often across multiple jurisdictions.	Task agencies with identifying options to address funding of harmful disinformation. Work with international partners to develop a better understanding of the issue and contribute to the development of an appropriate range of legal, regulatory or voluntary remedies.

Building resilience to mitigate vulnerabilities

Current gaps & limitations	Options to address
Work programmes on social cohesion, digital curriculum, and better public media will be helpful in this space. But they are longer-term in nature, and require exploration of how best they can contribute to resilience against mis/disinformation.	Task agencies to identify the most acute short-term vulnerabilities and develop approaches to accelerate and target work in those areas. Work with public sector agencies and civil society to develop capability in key areas (these could include internet governance, community engagement, technical capabilities, etc…).

Next Steps

39. We would welcome the opportunity to discuss this paper with you and seek your feedback. Following your feedback, officials will work to fully develop a more coordinated response to this issue. Further advice will be provided on resourcing requirements, and engagement with relevant ministers.

s6(a), s9(2)(j)

[redacted]

s6(a), s9(2)(j)

[redacted]