

Office of the Prime Minister

Prime Minister

Minister for National Security and Intelligence

Minister for Child Poverty Reduction

Minister Responsible for Ministerial Services

Associate Minister for Arts, Culture and Heritage



3 0 NOV 2022

Scott

fyi-request-20735-d62cca62@requests.fyi.org.nz

Ref: NSI OIA 2022-016

Tēnā koe Scott

Official Information Act request for copies of listed NSI briefings

I refer to your Official Information Act 1982 (the Act) request, received on 3 October 2022. You requested:

***ONE:** [1718NSP/033] "Foreign Interference - Brady Report and Canberra Visit" [December 2017]*

***TWO:** [1819NSPD/064] "Our parting thoughts and wishes for the National Security System" [December 2018]*

***THREE:** [2021NSP/014] "QAnon - Designation and Dis-information" [October 2020]*

***FOUR:** "Russia-Ukraine Situation and National Security System Preparedness" [1 February 2022]*

***FIVE:** "Potential Domestic Implications of Russia-Ukraine Conflict and Proposed Response" [8 February 2022]*

***SIX:** "2022-02-25 ODESC note to PM: Russia/Ukraine ODESC #1" [25 February 2022]*

***SEVEN:** "2022-02-28 ODESC note to PM: Russia/Ukraine ODESC #2" [28 February 2022]*

***EIGHT:** "Policy levers for Addressing Mis/Disinformation" [9 March 2022]*

***NINE:** "Update on Algorithmic Workstream" [8 April 2022]*

***TEN:** "Briefing on the Declaration on the Future of the Internet" [20 April 2022]*

***ELEVEN:** "Progress for a framework on Emerging Technology in New Zealand" [2 May 2022]*

***TWELVE:** "Work Programme on End-to-End Encryption" [11 May 2022]*

***THIRTEEN:** "Foreign interference targeting New Zealand communities: letter to Minister Radhakrishnan" [12 May 2022]*

***FOURTEEN:** "Briefing to PM on Buffalo Shooter incident" [25 May 2022]"*

I note we last wrote to you on 28 October, providing a response to parts 1 – 3, 6 – 9, and 11 – 14 of this request. In that letter, we advised that the time frame for responding to the remainder of your request needed to be extended under section 15A of the Act by 20 working days because it necessitated further consultations to be undertaken before a decision could be made. Following this, we are now in a position to provide a further response. Please find responses to the remaining parts of your request (**in bold**) below:

Private Bag 18041, Parliament Buildings, Wellington 6160, New Zealand

+64 4 817 8700 | j.ardern@ministers.govt.nz | beehive.govt.nz

**FOUR: “Russia-Ukraine Situation and National Security System Preparedness”
[1 February 2022]**

With regard to your request for the aide-memoire ‘Russia-Ukraine situation and National Security System Preparedness’, please find a copy enclosed. Some information, including Attachment A, is withheld under the following section of the Act:

- Section 6(a), to protect the security or defence of New Zealand or the international relations of the Government of New Zealand.

FIVE: “Potential Domestic Implications of Russia-Ukraine Conflict and Proposed Response” [8 February 2022]

With regard to your request for the aide-memoire ‘Potential Domestic Implications of Russia-Ukraine Conflict and Proposed Response’ please find a copy enclosed. Some information is withheld under the following section of the Act:

- Section 6(a), to protect the security or defence of New Zealand or the international relations of the Government of New Zealand, and
- Section 9(2)(b)(ii), as the release of the information would likely unreasonably prejudice the commercial position of the person who supplied or who is the subject of the information.

TEN: “Declaration for the Future of the Internet” [20 April 2022]

With regard to your request for the briefing ‘Briefing on the Declaration on the Future of the Internet’, this is withheld in part under the following sections of the Act:

- Section 6(a), to protect the security or defence of New Zealand or the international relations of the Government of New Zealand,
- Section 6(b)(i), to protect the entrusting of information to the Government of New Zealand on a basis of confidence by the Government of any other country or any agency of such a Government,
- Section 6(b)(ii), to protect the entrusting of information to the Government of New Zealand on a basis of confidence by any international organisation,
- Section 9(2)(a), to protect the privacy of individuals, and
- Section 9(2)(g)(i), to maintain the effective conduct of public affairs through the free and frank expression of opinion.

In making this decision, we have considered the public interest considerations in section 9(1) of the Act.

You have the right to ask the Ombudsman to investigate and review our decision under section 28(3) of the Act.

Ngā mihi nui,



Raj Nahna
Chief of Staff



Aide-Memoire

RUSSIA-UKRAINE SITUATION AND NATIONAL SECURITY SYSTEM PREPAREDNESS

<p>To</p>	<p>Rt Hon Jacinda Ardern, Minister for National Security and Intelligence,</p> <p>Hon Grant Robertson, Minister of Finance</p> <p>Hon Andrew Little, Minister Responsible for the GCSB and NZSIS</p> <p>Hon Nanaia Mahuta, Minister of Foreign Affairs</p> <p>Hon Poto Williams, Minister of Police</p> <p>Hon Peeni Henare, Minister of Defence</p> <p>Hon Dr David Clark, Minister for Digital Economy and Communications</p>	<p>Report No</p>	<p>DPMC-2021/22-1326</p>
<p>From</p>	<p>Tony Lynch, Deputy Chief Executive, National Security Group (DPMC)</p>	<p>Date</p>	<p>1/02/2022</p>

Purpose

1. This aide-memoire sets out how the National Security System is preparing for any Russian incursion against Ukraine. This preparation includes consideration of our readiness for retaliation, or other potential consequences for New Zealand and our interests. National Security Group (DPMC) is leading system coordination of these elements.
2. Much of our understanding about the criticality and imminence of the situation at this stage is derived from classified information. **Attachment A** provides you with a classified assessment (drafted jointly by NZ Defence Intelligence and the National Assessments Bureau) outlining what we know now and potential strategic implications.

System readiness

3. The National Security System (NSS) has been activated to enable system readiness and ensure strategic coordination in preparation for threats and risks arising from Russian activity against Ukraine. A first Watch Group (Tier 2/Tier 3 officials) was held on 31 January 2022, to ensure agencies had the full intelligence picture and shared situational awareness, which provides a basis for undertaking coordinated preparatory activities for:
 - a. retaliation arising from the global response to any Russian action, directly or indirectly targeting New Zealand; and
 - b. other disruptions which may impact across a range of New Zealand's interests (e.g. supply chain disruption).
4. DPMC's National Security Group has established an overarching strategic coordination mechanism to ensure coordination across multiple agencies in the areas of intelligence, policy, communications and system-level risk.
5. This structure will help ensure decisions are escalated to, and able to be taken at, the appropriate level. It will also ensure that:
 - a. there is strategic coordination and alignment across a range of threats, risks and issues;
 - b. strategic decision-making is informed by coordinated intelligence and policy advice;
 - c. Ministers and the public are assured that risks will be appropriately managed in a coordinated way;
 - d. shared situational awareness is maintained, as agencies work through response and policy options; and
 - e. existing capacity and resources issues, in the COVID context and involving other system pressures, are considered and managed from a system level.

6. s6(a) [Redacted]

s6(a) [Redacted]

s6(a) [Redacted]

s6(a) [Redacted]

s6(a) [Redacted]

s6(a) [Redacted]

s6(a) [Redacted]

7. s6(a) [Redacted]

Recommendations

8. It is recommended that you note the contents of this aide-memoire.

	NOTED
Tony Lynch Deputy Chief Executive National Security Group	Rt Hon Jacinda Ardern, Minister for National Security and Intelligence Date: / /
NOTED	NOTED
Hon Grant Robertson, Minister of Finance Date: / /	Hon Andrew Little, Minister Responsible for the GCSB and NZSIS Date: / /
NOTED	NOTED
Hon Nanaia Mahuta, Minister of Foreign Affairs Date: / /	Hon Poto Williams, Minister of Police Date: / /
NOTED	NOTED
Hon Peeni Henare, Minister of Defence Date: / /	Hon Dr David Clark, Minister for Digital Economy and Communications Date: / /

Attachment A Russia/Ukraine: On the Precipice

ATTACHMENT A

Russia/Ukraine: On the Precipice

Released under the Official Information Act 1982



Aide-Memoire

POTENTIAL DOMESTIC IMPLICATIONS OF RUSSIA-UKRAINE CONFLICT AND PROPOSED RESPONSE

To	<p>Rt Hon Jacinda Ardern, Prime Minister and Minister for National Security and Intelligence,</p> <p>Hon Grant Robertson, Deputy Prime Minister and Minister of Finance</p> <p>Hon Dr Megan Woods, Minister of Energy and Resources</p> <p>Hon Andrew Little, Minister Responsible for the GCSB and NZSIS</p> <p>Hon Nanaia Mahuta, Minister of Foreign Affairs</p> <p>Hon Poto Williams, Minister of Police</p> <p>Hon Peeni Henare, Minister of Defence</p> <p>Hon Dr David Clark, Minister for Digital Economy and Communications</p>	Report No	DPMC-2021/22-1355
From	Tony Lynch, Deputy Chief Executive, National Security Group (DPMC)	Date	8/02/2022

Purpose

1. As requested by the Prime Minister on 3 February 2022, this aide-memoire updates Ministers on the potential domestic implications for New Zealand of continued and/or escalating Russian aggression against Ukraine. These could arise due to:
 - a. Russian retaliation to any state's response – including New Zealand's – to Russia's actions; or
 - b. other disruptions not directly targeting New Zealand, but with harmful domestic consequences.
2. It also provides detail on mitigations and work underway to enhance domestic preparedness and additional material being prepared to support Ministers' understanding of the likely implications of any escalation in the crisis.

Background

3. The risk of military conflict between Russia and Ukraine is growing, with Russian aggression escalating to incursion or invasion now considered likely and that this could occur with little or no warning. The deliberate use of military force in violation of Ukrainian sovereignty and territorial integrity would constitute a grave breach of international law. It would also likely have significant humanitarian consequences, and economic and security implications for New Zealand.
4. In response, government agencies are developing our international response to, and enhancing our domestic readiness for, such escalation. These workstreams are currently being led by the Ministry of Foreign Affairs and Trade (MFAT) and the Department of the Prime Minister and Cabinet (DPMC), respectively.
5. With respect to our international response, on Friday, 28 January 2022, the Minister of Foreign Affairs referred an MFAT submission to the Prime Minister that sought agreement to proactive diplomatic efforts to de-escalate the crisis, and outlined potential diplomatic options available to New Zealand in the event of further Russian aggression. Ministers jointly agreed to this diplomatic approach on Tuesday, 1 February 2022.
6. With respect to enhancing our domestic preparedness, on Tuesday, 2 February 2022, DPMC provided a briefing to Ministers that included:
 - a. s6(a) [REDACTED]
 - b. information on the activation of the National Security System (NSS), which has the goal of building common awareness of, and supporting preparation for, any conflict or the global response to it [DPMC-2021/22-1326 refers].
7. On Thursday 3 February 2022, the Prime Minister requested additional advice on the impacts of regional conflict on energy, supply chains, and digital networks, and how agencies were working to mitigate them.
8. This briefing discusses these risks, as well as the other main risks that regional conflict poses to New Zealand and our mitigations. DPMC has prepared this in consultation with MFAT, the Ministry of Business, Innovation and Employment (MBIE), the Ministry of Transport (MoT) and the Reserve Bank of New Zealand (RBNZ).

Domestic implications of a Russia-Ukraine conflict and mitigations

9. This section details the most significant risks prospective conflict poses to New Zealand's domestic security, mitigations and work to enhance domestic preparedness. These include:
 - a. increases in the price of liquid fuels (including natural gas);
 - b. (further) disruption of global supply chains;
 - c. economic and financial market instability;
 - d. malicious cyber activity that affects global institutions or domestic networks; and
 - e. as a consequence of the above, pressures on New Zealand's critical infrastructures.

10. While discussed separately at a high level, these risks are linked and could compound one another in complex ways. For example, increasing fuel prices will amplify existing supply chain and inflationary pressures, with implications for global and domestic economic growth and financial markets. These interconnections make forecasting the precise scale of any impacts on New Zealand difficult, but the need to prepare for them where possible is clear.
11. Throughout this section 'conflict' is used to describe disruptions caused by:
 - a. strategic manoeuvring and 'grey zone' activities that stop short of invasion (for example, movements of troops and malicious cyber activity);
 - b. actual invasion; and
 - c. the potential global response to conflict, were it to occur (for example, US sanctions).
12. This reflects the fact that even without armed engagement, Russia's activities will disrupt global markets, with implications for New Zealand (though the magnitude is likely smaller).

Fuel prices are likely to increase

13. Russia is the world's second largest oil producer (about 12 per cent of total global crude oil exports), and Europe's largest supplier of natural gas (around 40 per cent of the continent's piped supply). Any escalation in the conflict will have material implications for global oil and gas markets, European energy markets, the cost of European manufacturing, and trigger continued supply substitution and the potential draw down of strategic reserves.
14. These disruptions are likely to have price, rather than supply, implications for New Zealand. While almost none of New Zealand's physical supplies of oil and refined fuels are imported from that region, global price movements generally flow quickly into New Zealand fuel prices.
15. While it is difficult to forecast the precise scale of any increase, the combination of the conflict and potential sanctions (for example, on Russia's energy earnings) means that price rises could be material. Increased fuel prices will feed into already high levels of inflation directly and indirectly, with higher energy costs increasing the cost of producing almost all goods across the economy.
16. New Zealand has limited levers to affect global fossil fuel prices. However, our participation in the International Energy Agreement, under which reserve oil stocks may be released in collective response to significant market disruptions, can help mitigate short-term price increases. MBIE will keep Ministers informed of any notable developments.

Supply chain constraints will worsen

17. COVID-19 has placed global supply chains under severe pressure, with any conflict expected to compound these existing general constraints. Reasons could include higher fuel prices, rerouting of freight to avoid conflict zones, and effects on the supply of seafarer labour, for which Russia and Ukraine are two of the top five global suppliers. Any restrictions on the movement of Russian and/or Ukrainian nationals could significantly reduce global shipping capacity.
18. In addition to creating indirect pressures across the supply chain, conflict between Russia and Ukraine could also have major implications for the supply and/or price of two goods of particular importance to the global (and domestic) primary sector:
 - a. fertiliser (where Russia is a major producer); and

- b. grain (Russia is the world's largest exporter of wheat and Ukraine is a key global supplier of oilseeds and grains).¹
19. Reflecting our limited trade with Russia and Ukraine and the lack of any critical supply chain dependencies on inputs from either jurisdiction, New Zealand is most likely to experience these pressures indirectly. However, increases in the price of shipping, the price of goods manufactured via global value chains, and the price of fertiliser and grain, will add to delays in accessing some goods and to inflationary pressures.
20. The RBNZ, through monetary policy, is well placed to respond to inflation and agencies are working - as part of the COVID-19 response - to resolve supply chain congestion. This ongoing work is expected to also be able to accommodate any additional conflict-driven pressures.
21. s9(2)(b)(ii)

Economic and financial market instability will likely intensify

22. New Zealand does not have significant direct trade or financial links with Russia or Ukraine. This means that escalation of the Russia-Ukraine conflict is more likely to indirectly affect the domestic economy through impacts on global financial and commodities markets. This includes the potential for:
- a. a spike in risk aversion, which would weigh on assets like stocks and lead to a tightening in global financial conditions (for example, reducing business' access to finance). However, it is difficult to forecast the effect of this, given it would likely be offset by increased investment flows into bonds, pushing interest rates lower;
 - b. a decline in investor confidence, which could:
 - i. hamper liquidity as investors seek safe-haven assets (for example, gold and government bonds); and
 - ii. lead to depreciation of the New Zealand dollar, increasing the impact of global commodity price rises; and
 - c. downstream impacts of lower growth in some of our key trading partners (particularly countries in Europe) that have larger and more direct exposure to Russian trade and financial flows. This could include a reduction in asset prices and liquidity, compounding and accelerating the effects describe above.
23. If an invasion did occur and additional sanctions were imposed on Russia by the United States and European countries, the New Zealand economy would be more directly affected with two-way trade significantly reduced (though from a low base).
24. The potential removal of Russian institutions from SWIFT, a global interbank payment system, would also further hinder trade and financial markets activity, but not prevent it given the existence of less-widely used but functional alternatives.

¹ Together, Russia and Ukraine export 28.6% of the world's wheat and 19.6% of the world's corn.

Malicious cyber activity disrupts global and/or domestic activity

25. Russia is a highly capable cyber actor. In previous hostilities with its neighbours, Russia has used a broad spectrum of offensive cyber activities in support of its objectives, s6(a) s6(a) and sophisticated attacks on critical infrastructure. We expect that any incursion will most likely be accompanied by increased malicious cyber activity focussed on Ukrainian interests, tailored to support Russia's offline actions s6(a)

26. Unlike the other risks where New Zealand is only indirectly exposed due to our connections to global markets and systems, malicious cyber activity poses potential indirect and direct risks to New Zealand's security in three ways, detailed below. These are:

- a. the downstream implications of Russian targeting globally significant infrastructures or institutions, potentially in response to foreign states' response to the conflict;
- b. unintended consequences of malware or other tools directed at Ukraine and Ukrainian interests; and
- c. s6(a)

27. New Zealand is indirectly exposed to the potential consequences of Russian activity targeted at globally important infrastructures or institutions (for example, those relating to the global financial system). Such actions could occur in retaliation to the imposition of sanctions or other responses to the conflict. While Russia may ultimately avoid activity that provides a legitimate pretext for a Western response during any conflict, it could nevertheless seek to cause significant disruption with material consequences for New Zealand, even though our own networks are unaffected. s6(a)

28. New Zealand is also indirectly exposed to potential unintended consequences of Russian activity against Ukraine. Any significant malicious cyber activity includes a possibility of collateral damage to other internet users, particularly those who are connected to the target entity. If Russian actors employ malware, for example, the consequences could extend beyond Russia and Ukraine and have significant global and domestic implications. This occurred in 2017, when Russia released the NotPetya malware, which was initially targeted at Ukrainian systems, but ultimately disrupted businesses and governments across the globe.

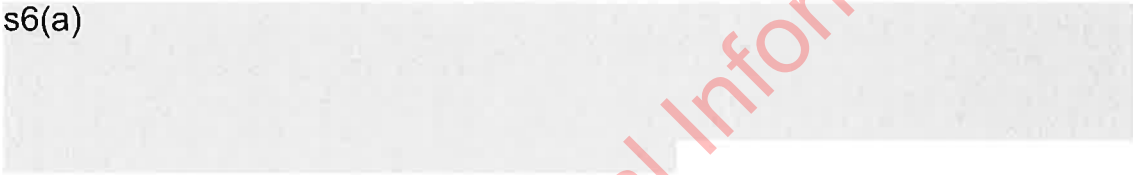
29. While the release of such malware would increase the risk of cyber security incidents affecting New Zealand, the type of risk is not fundamentally different from those faced on a business-as-usual basis and businesses are expected to have processes in place to manage them. The National Cyber Security Centre has also provided advice to nationally significant organisations on the potential cyber security risks and mitigations.

30. s6(a)

Pressures on critical infrastructures may grow

31. Critical infrastructures include assets, systems, networks and services that underpin and include significant businesses in the finance, energy, three waters, telecommunications, transport, and health sectors.
32. While unlikely to be directly affected by any potential conflict, New Zealand's critical infrastructures are highly dependent on the global market for inputs, which the conflict would disrupt. Infrastructures are also increasingly connected to the internet – and to each other – making the entire system more susceptible to malicious cyber activity, whether directly targeting New Zealand or not.
33. While it is difficult to forecast how events will affect these infrastructures, conflict-driven risks to supply chains, fuel prices, and digital systems are likely to exacerbate existing challenges rather than create new ones. Infrastructures are already managing supply chain and other cost pressures and are expected to have systems to ensure service continuity. For 'lifeline utilities', a subset of New Zealand's most critical infrastructures including the major airports, telecommunications, three waters, and electricity providers, preparing for these challenges is a Civil Defence Emergency Management Act requirement.

34. s6(a)



Next Steps

35. This topic is on the agenda for the national security and intelligence meeting hosted by the Prime Minister on Wednesday 9 February 2022, which most Ministers receiving this briefing are expected to attend. Officials from DPMC, NAB and Defence Intelligence will be available to answer any additional questions.
36. Ahead of any additional tasking from this meeting:
 - a. DPMC has tasked lead agencies with assessing the risks within their portfolios and their readiness to respond by 10 February. This will inform further national security system activity in relation to New Zealand's response to any potential conflict;
 - b. MFAT is developing additional advice on the potential measures that New Zealand might take to respond to further Russian aggression in the absence of an autonomous sanction's regime; and
 - c. MFAT is working in consultation with the Treasury and the Ministry of Primary Industries to enhance our understanding of the broader economic implications of any potential conflict for New Zealand.

Recommendations

37. It is recommended that you note the contents of this aide-memoire.

<p>Tony Lynch Deputy Chief Executive National Security Group</p>	<p>NOTED</p> <p>Rt Hon Jacinda Ardern, Prime Minister and Minister for National Security and Intelligence</p> <p>Date: / /</p>
<p>NOTED</p> <p>Hon Grant Robertson, Deputy Prime Minister and Minister of Finance</p> <p>Date: / /</p>	<p>NOTED</p> <p>Hon Dr Megan Woods, Minister of Energy and Resources</p> <p>Date: / /</p>
<p>NOTED</p> <p>Hon Andrew Little, Minister Responsible for the GCSB and NZSIS</p> <p>Date: / /</p>	<p>NOTED</p> <p>Hon Nanaia Mahuta, Minister of Foreign Affairs</p> <p>Date: / /</p>
<p>NOTED</p> <p>Hon Poto Williams, Minister of Police</p> <p>Date: / /</p>	<p>NOTED</p> <p>Hon Peeni Henare, Minister of Defence</p> <p>Date: / /</p>
<p>NOTED</p> <p>Hon Dr David Clark, Minister for Digital Economy and Communications</p> <p>Date: / /</p>	



Briefing

DECLARATION FOR THE FUTURE OF THE INTERNET


To: Rt Hon Jacinda Ardern, Prime Minister

Date	11/04/2022	Priority	High
Deadline	15/04/2022	Briefing Number	DPMC-2021/22-1988

Purpose


To seek your consideration of New Zealand becoming a supporter of the US-led "Declaration for the Future of the Internet" and, should time allow, to consider pre-recording a video message for the Declaration's launch event at the White House on 28 April 2022.

Recommendations

- Note** the Declaration text aligns with New Zealand's interests and signals our desire for a strong tech partnership with the USA.
- s6(a) 
- Agree** that New Zealand support the Declaration, subject to other key partners confirming their support. **YES / NO**
- Agree**, should time allow, to pre-record a video Statement (draft script provided in annex) **YES / NO**
- Refer** this briefing to the Ministers for Digital Economy and Communications and Foreign Affairs and Trade for information **YES / NO**

BRIEFING TITLE

Report No.



Paul Ash
Special Representative for Cyber & Digital, DPMC

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

Rt Hon Jacinda Ardern
Prime Minister

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

Contact for telephone discussion if required:

Name	Position	Telephone	1st contact
Paul Ash	Special Representative for Cyber and Digital	Mobile: s9(2)(a)	✓
Halia Haddad	Manager, National Cyber Policy Office	Mobile: s9(2)(a)	

Minister's office comments:

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

.....

BRIEFING TITLE

Report No.

DECLARATION FOR THE FUTURE OF THE INTERNET

Purpose

To seek your consideration of New Zealand becoming a supporter of the US-led "Declaration for the Future of the Internet" and, should time allow, to consider pre-recording a video message for the Declaration's launch event at the White House on 28 April 2022.

Background

s6(a)

1. At President Biden's invitation, you attended his Summit for Democracy on 9 December 2021, leading a session on strengthening democratic resilience. You spoke about the importance of a free, open, secure internet and of harnessing multi-stakeholder approaches to address the challenges to democracy that arise in the digital space.

2. s6(a)

3. s6(b)(ii)

4. s6(a), s6(b)(i)

s6(a)

5. The US Embassy in Wellington démarched DPMC with the declaration text on 29 March 2022. In their pitch they noted that the Declaration is political in nature and is *'the start of a conversation'* that will be wide-ranging and inclusive. s6(a)

At that démarche we welcomed the prospect of coordinated multistakeholder work on the range of challenges posed to liberal democracies by online developments. s6(a)

s6(a)

6. The Declaration contains a series of principles that are intended to be considered by policymakers as they develop legislation and policy tools. These include: protecting human rights & fundamental freedoms; a global internet; inclusive and affordable access; trust in the digital ecosystem; and multistakeholder governance.

The text aligns with Aotearoa New Zealand's values and interests

7. The text draws from the same elements as the Christchurch Call, although it addresses a much wider range of issues. It signals a strong commitment to promoting human rights online, a free, open, and secure (and globally connected) internet as a vehicle for inclusive growth and innovation, and a commitment to multistakeholder partnerships and engagement.
8. The principles are also well aligned with the framework being developed for the Digital Strategy for Aotearoa: mahi tika - trust, mahi tahi - inclusion, and mahi ake – growth.
9. Joining this Declaration would be a helpful way of aligning Aotearoa New Zealand with a public statement on the importance of a more effective and coherent approach to internet governance, working with others. This in turn could assist with improving engagement in these processes, by government agencies and through more frequent and effective coordination with stakeholders outside of government, working from a shared values-base for decision making.
10. Consideration of Te Tiriti o Waitangi and Maori rights and interests will be important in implementing the principles of this Declaration, particularly around inclusive and affordable access, and engagement of stakeholders in governance. Improved consultation with Maori on internet governance issues would be beneficial, whether we join the Declaration or not.

s6(a)

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

Aotearoa New Zealand's legislation provides for a 'vendor-neutral' and risk-based approach, s6(a). Our legislation does not characterise vendors or supplying countries as being trustworthy or otherwise. s6(a)

s6(a)

12. s6(a)

s6(a)

- Ahead of your forthcoming visit, Aotearoa New Zealand has proposed the US engage with us on a bilateral technology partnership to take forward the economic opportunities and the responsible deployment of digital technologies. As part of that work, we are scoping to training and developing a diverse cohort of young policy and technical professionals to support medium- to long-term digital development. The Declaration's principles would provide a helpful common basis upon which to build such a bilateral partnership.

We need to balance our reputation and bilateral interests

- New Zealand's 'value add' in any processes that emerge from this declaration would be based on our role as a vibrant liberal democracy, with a strong focus on digital economic development, and with a strong track record on engaging effectively with civil society, industry and governments on responsible technology. This is, in large part, based on our role as the co-founder of the Christchurch Call, and the credibility we have built as a trusted and engaged digital partner. s6(a)

- s6(b)(i)

- Your forthcoming visit offers a rare opportunity to position Aotearoa New Zealand in the thinking of policymakers in the USA and elsewhere as an engaged, reliable partner on a priority issue. Support for the Declaration would underpin that engagement ahead of the visit itself. s9(2)(g)(i)

Launching the Declaration

- The US is planning to launch the Declaration at the White House at an event hosted by National Security Advisor Jake Sullivan. s6(a), s6(b)(i)

The event is intended to begin with pre-recorded messages from selected world leaders, and a selection of Ministers who are physically present will 'sign' the declaration. IT has been suggested that, should New Zealand support the Declaration, you may wish to offer a pre-recorded video message for the event.

- We have accordingly drafted a proposed video message text (attachment B) for use, should you wish to endorse the Declaration and should your schedule allow. The draft points to our experience with the Christchurch Call and picks up some important messages

raised by civil society stakeholders about how the Declaration should be implemented in an inclusive and participatory way.

19. In addition to signalling our good intentions through supporting the Declaration and, potentially, providing a pre-recorded message, domestic agencies may also choose to also build on nascent efforts to better coordinate and engage on internet governance, working with Internet New Zealand and other stakeholders.

Next Steps

20. We outline four possible approaches:

Option 1:

s6(a)

Option 2:

Join subject to confirmation that likeminded Governments are doing so. Don't send a video

s6(a)

Option 3:

(recommended option) Join Subject to confirmation that likeminded Governments are doing so. Use video to put down markers on process

This would allow New Zealand to clearly signal our intentions and value-add including through the Christchurch Call experience.

Making good on any markers put down e.g. on inclusive approaches to internet governance would be good for New Zealand but would require resources and effort.

Option 4:

Join and express wholehearted support via video message

s9(2)(g)(i)

21. This briefing recommends you pursue option 3. If you confirm that approach, officials will:

a) s6(a)

b) Engage with international and domestic civil society and industry stakeholders about the initiative, including how we can best reflect the human rights and other principles through Aotearoa New Zealand's participation in internet governance bodies.

c) Work with your office to record a short video message to be played at the launch event.

BRIEFING TITLE

Report No.

Consultation

22. The following agencies and entities have been consulted:

a) s9(2)(g)(i)

[Redacted]

b) s9(2)(g)(i)

[Redacted]

c) MFAT, NCPO, and the Christchurch Call Unit are supportive of the Declaration as a vehicle to help advance a bilateral digital partnership, and to assist agencies to coordinate more effectively on internet governance issues.

d) s9(2)(g)(i)

[Redacted]

Attachments:	
Attachment A:	Declaration text
Attachment B:	Proposed Script for a video message
Attachment C:	Civil Society letter on the original 'alliance' concept

Attachment B to be withheld in full under s9(2)(g)(i)

Attachment C to be withheld in full under s6(a)

ATTACHMENT A

Text of the Declaration for the Future of the Internet

We are united by a belief in the potential of digital technologies to promote connectivity, democracy, peace, the rule of law, sustainable development, and the enjoyment of human rights and fundamental freedoms. As we increasingly work, communicate, connect, engage, learn, and enjoy leisure time using digital technologies, our reliance on an open, free, global, interoperable, reliable, and secure Internet will continue to grow. Yet we are also aware of the risks inherent in that reliance and the challenges we face.

We call for a new Declaration for the Future of the Internet that includes all partners who actively support a future for the Internet that is open, free, global, interoperable, reliable, and secure. We further affirm our commitment to protecting and respecting human rights online and across the digital ecosystem. Partners in this Declaration intend to work toward an environment that reinforces our democratic systems and promotes active participation of every citizen in democratic processes, secures and protects individuals' privacy, maintains secure and reliable connectivity, resists efforts to splinter the global Internet, and promotes a free and competitive global economy. Partners in this Declaration invite other partners who share this vision to join us in working together, with civil society and other stakeholders, to affirm guiding principles for our role in the future of the global Internet.

Reclaiming the Promise of the Internet

The immense promise that accompanied the development of the Internet stemmed from its design: it is an open "network of networks", a single interconnected communications system for all of humanity. The stable and secure operation of the Internet's unique identifier systems have, from the beginning, been governed by a multistakeholder approach to avoid Internet fragmentation, which continues to be an essential part of our vision. For business, entrepreneurs, and the innovation ecosystem as a whole, interconnection promises better access to customers and fairer competition; for artists and creators, new audiences; for everyone, unfettered access to knowledge. With the creation of the Internet came a swell in innovation, vibrant communication, increased cross-border data flows, and market growth—as well as the invention of new digital products and services that now permeate every aspect of our daily lives.

Over the last two decades, however, we have witnessed serious challenges to this vision emerge. Access to the open Internet is limited by some authoritarian governments and online platforms and digital tools are increasingly used to repress freedom of expression and deny other human rights and fundamental freedoms. State-sponsored or condoned malicious behavior is on the rise, including the spread of disinformation and cybercrimes such as ransomware, affecting the security and the resilience of critical infrastructure while holding at risk vital public and private assets. At the same time, countries have erected firewalls and taken other technical measures, such as Internet shutdowns, to restrict access to journalism, information, and services, in ways that are contrary to international human rights commitments and obligations. Concerted or independent actions of some governments and private actors have sought to abuse the openness of Internet governance and related processes to advance a closed vision. Moreover, the once decentralized Internet economy has become highly concentrated, and many people have legitimate concerns about their privacy and the quantity and security of personal data collected and stored online. Online platforms have enabled an increase in the spread of illegal or harmful content that can threaten the safety of individuals and contribute to radicalization and violence. Disinformation and foreign malign activity is used to sow division and conflict between individuals or groups in society, undermining respect for and protection of human rights and democratic institutions.

Our Vision

We believe we should meet these challenges by working towards a shared vision for the future of the Internet that recommits governments and relevant authorities to defending human rights and fostering equitable economic prosperity. We intend to ensure that the use of digital technologies reinforces, not weakens, democracy and respect for human rights; offers opportunities for innovation in the digital ecosystem, including businesses large and small; and, maintains connections between our societies. We intend to work together to protect and fortify the multistakeholder system of Internet governance and to maintain a high level of security, privacy protection, stability and resilience of the technical infrastructure of the Internet.

We affirm our commitment to promote and sustain an Internet that: is open, free, global, interoperable, secure, and reliable and to ensure that the Internet reinforces democratic principles and human rights and fundamental freedoms; offers opportunities for collaborative research and commerce; is developed, governed, and deployed in an inclusive way so that unserved and underserved communities, particularly those coming online for the first time, can navigate it safely and with personal data privacy and protections in place; and is governed by multistakeholder processes. In short, an Internet that can deliver on the promise of connecting humankind and helping societies and democracies to thrive.

The Internet should operate as a single, decentralized network of networks – with global reach and governed through the multi-stakeholder approach, whereby governments and relevant authorities partner with academics, civil society, the private sector, technical community and others. Digital technologies reliant on the Internet, will yield the greatest dividends when they operate as open, free, global, interoperable, secure, and reliable systems. Digital technologies should be produced, used, and governed in ways that enable trustworthy, free, and fair commerce; avoid unfair discrimination between, and ensure effective choice for, individual users; foster fair competition and encourage innovation; promote and protect human rights; and, foster societies where:

- *Human rights and fundamental freedoms, and the well-being of all individuals are protected and promoted;*
- *All can connect to the Internet, no matter where they are located, including through increased access, affordability, and digital skills;*
- *Individuals and businesses can trust the safety and the confidentiality of the digital technologies they use and that their privacy is protected;*
- *Businesses of all sizes can innovate, compete, and thrive on their merits in a fair and competitive ecosystem;*
- *Infrastructure is designed to be secure, interoperable, reliable, and sustainable;*
- *Technology is used to promote pluralism and freedom of expression, sustainability, inclusive economic growth, and the fight against global climate change.*

Principles to promote this Vision

The partners in this Declaration intend to uphold a range of key principles, set out below, regarding the Internet and digital technologies; to promote these principles within existing multilateral and multistakeholder fora; to translate these principles into concrete policies and actions; and, work together to promote this vision globally, while respecting each other's regulatory autonomy within our own jurisdictions and in accordance with our respective domestic laws and international legal obligations. These principles are not legally binding but should rather be used as a reference for public policy makers, as well as citizens, businesses, and civil society organizations.

Protection of Human Rights and Fundamental Freedoms

- Dedicate ourselves, in conducting and executing our respective domestic authorities, to respect human rights, including as reflected in the Universal Declaration of Human Rights, as well as the principles of the rule of law, legitimate purpose, non-arbitrariness, effective oversight, and transparency, both online and offline, and call upon others to do the same.
- Promote online safety and continue to strengthen our work to combat violence online, including sexual and gender-based violence as well as child sexual exploitation, to make the Internet a safe and secure place for everyone, particularly women, children, and young people.
- Promote safe and equitable use of the Internet for everyone, without discrimination based on sex, gender and gender identity, race, color, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority or indigenous population, property, birth, disability, age or sexual orientation.
- Reaffirm our commitment that actions taken by governments, authorities, and digital services including online platforms to reduce illegal and harmful content and activities online be consistent with international human rights law, including the right to freedom of expression while encouraging diversity of opinion, and pluralism without fear of censorship, harassment, or intimidation.
- Protect and respect human rights and fundamental freedoms across the digital ecosystem, while providing access to meaningful remedies for human rights violations and abuses, consistent with international human rights law.
- Refrain from misusing or abusing the Internet or algorithmic tools or techniques for unlawful surveillance, oppression, and repression that do not align with international human rights principles, including developing social score cards or other mechanisms of domestic social control or pre-crime detention and arrest.

A Global Internet

- Refrain from government-imposed internet shutdowns or degrading domestic Internet access, either entirely or partially.
- Refrain from blocking or degrading access to lawful content, services, and applications on the Internet, consistent with principles of Net Neutrality subject to applicable law, including international human rights law.
- Promote our work to realize the benefits of data free flows with trust based on our shared values as like-minded, democratic, open and outward looking partners.
- Promote cooperation in research and innovation and standard setting, encourage information sharing regarding security threats through relevant international fora, and reaffirm our commitment to the framework of responsible state behavior in cyberspace.

Inclusive and Affordable Access to the Internet

BRIEFING TITLE	Report No.
----------------	------------

- Promote affordable, inclusive, and reliable access to the Internet for individuals and businesses where they need it and support efforts to close digital divides around the world to ensure all people of the world are able to benefit from the digital transformation.
- Support digital literacy, skills acquisition, and development so that individuals can overcome the digital divide, participate in the Internet safely, and realize the economic and social potential of the digital economy.
- Foster greater exposure to diverse cultural and multilingual content, information, and news online. Exposure to diverse content online should contribute to pluralistic public discourse, foster greater social and digital inclusion within society, bolster resilience to disinformation and misinformation, and increase participation in democratic processes.

Trust in the Digital Ecosystem

- Work together to combat cybercrime, including cyber-enabled crime, and deter malicious cyber activity.
- Ensure that government and relevant authorities' access to personal data is based in law and conducted in accordance with international human rights law.
- Protect individuals' privacy, their personal data, the confidentiality of electronic communications and information on end-users' electronic devices, consistent with the protection of public safety and applicable domestic and international law.
- Promote the protection of consumers, in particular vulnerable consumers, from online scams and other unfair practices online and from dangerous and unsafe products sold online.
- Promote and use trustworthy network infrastructure and services suppliers, relying on risk-based assessments that include technical and non-technical factors for network security.
- Refrain from using the Internet to undermine the electoral infrastructure, elections and political processes, including through covert information manipulation campaigns.
- Support a rules-based global digital economy which fosters trade and contestable and fair online markets so that firms and entrepreneurs can compete on their merits.
- Cooperate to maximize the enabling effects of technology for combatting climate change and protecting the environment whilst reducing as much as possible the environmental footprint of the Internet and digital technologies.

Multistakeholder Internet Governance

- Protect and strengthen the multistakeholder system of Internet governance, including the development, deployment, and management of its main technical protocols and other related standards and protocols.
- Refrain from undermining the technical infrastructure essential to the general availability and integrity of the Internet.

We believe that the principles for the future of the Internet are universal in nature and as such we invite those who share this vision to affirm these principles and join us in the implementation of this vision. This Declaration takes into account, and expects to contribute to, existing processes in the UN system, G7, G20, the Organisation for Economic Cooperation and Development, the

World Trade Organization, and other relevant multilateral and multistakeholder fora, the Internet Corporation for Assigned Names and Numbers, Internet Governance Forum, and Freedom Online Coalition. We also welcome partnership with the many civil society organizations and non-profit organizations that are essential to promoting an open, free, global, interoperable, secure, and reliable Internet, and defending fundamental freedoms and human rights online. Partners in this Declaration intend to consult and work closely with stakeholders in carrying forward this vision.

Released under the Official Information Act 1982

BRIEFING TITLE	Report No.
----------------	------------

Released under the Official Information Act 1982

Released under the Official Information Act 1982

Released under the Official Information Act 1982

Released under the Official Information Act 1982

Released under the Official Information Act 1982