Strengthening civil society resilience to mis- and disinformation in Aotearoa New Zealand

Recommendations from the Multi-Stakeholder Group advising the Department of the Prime Minister and Cabinet

FEBRUARY 2024

Co-chairs' Foreword

New Zealanders are exposed to more information than ever before. Thanks to digital communications mediums, there is now more diversity in how the people of Aotearoa both receive information and participate in the gathering and creation of information, and there is also a greatly increased volume of information available. A dark side of this increase in media volume and participation is the relative ease in creating and disseminating information that is false. False information can cause harm – and according to information reviewed in the process of creating this report, those harms are reportedly increasing in Aotearoa (see Appendix B).

For these reasons, we have been pleased to lead this process, working with a multi-stakeholder group of experts to consider whether and how Aotearoa may increase resilience to the effects of disinformation. As our report identifies, governments cannot and should not seek to resolve these challenges alone. Instead, we believe there is strength in considering these issues in a multi-stakeholder manner – to allow a wider range of participants, perspectives, and potential solutions to be considered. While our group was not constructed to be, and does not purport to be, a representative grouping, our work was enhanced by working in a multi-stakeholder manner, and in incorporating the range of professional backgrounds and experiences our group members offered.

The challenges we have considered in forming this report included definitional issues of what disinformation and adjacent phenomena are; what evidence there is both domestically and internationally of effective frameworks and programmes to address the incidence and negative effects of disinformation; the nature and impact of harms that disinformation fosters; and the range of community-led approaches to increasing resilience to disinformation. Based on these considerations, we have then explored who should act, and what appropriate actions could be. Throughout our discussions, we have been keenly aware of issues of freedom of expression, existing frameworks for managing harms, and how our recommendations may complement our national settings in these areas.

This report seeks to be a step forward in the consideration of these issues. We have sought to frame our recommendations to provide a platform for how New Zealand's approach to disinformation may continue to evolve. This includes our recommendations on guiding principles for a national level response to disinformation, and on how multistakeholder and representative participation can lead this work from here.

We believe these recommendations, if implemented, will provide a means for Aotearoa to better consider how best to increase resilience to information issues over time.

It has been our privilege to chair this work, and our thanks to the group participants, and our secretariat, in how we have considered these issues together.

CO-CHAIRS

Robyn Kamira
Andrew Cushen

Group members and process

Process followed by group and qualifications on conclusions

This group was convened by the Department of the Prime Minister and Cabinet in July 2023, bringing together expertise in disinformation research, law, Te Ao Māori, journalism, public policy, community engagement, and other related areas to provide advice to the Department of the Prime Minister and Cabinet on how to understand and respond to disinformation in Aotearoa New Zealand.

Group members were appointed for their individual experience and expertise, not as representatives of an institution, organisation, or representative of a group or community.

Following a series of in-person and online group discussions and one-on-one interviews with the group members, the Brainbox Institute produced a draft report designed to reflect the group's emerging views and conclusions. This draft report was iterated on rapidly through extensive consultation with group members to produce the report you are now reading.

This process engaged with an incredibly complex issue, and has been inherently limited by the time available, the positionality and perspective of the group, and the limits of the knowledge present in the group. With more time or a greater budget, the group may have looked to add members, create networks, or consult with local and international experts to fill some of the gaps that undoubtedly remain despite our best efforts.

Group membership

Andrew Cushen (Co-Chair) is a consultant with experience across strategy, policy and public affairs. He has a background in telecommunications and the internet and brings to the group perspectives on building effective and sustainable community initiatives.

Robyn Kamira (Co-Chair) (Te Rarawa, Te Aupōuri, Tai Tokerau whānui) is the founder of Māori-owned technology consulting company Pāua Interface Ltd, delivering professional advice to Māori, government and NGO clients on data and digital projects, including those in security-related areas. She also has a background in research, Te Ao Māori, indigenous peoples, and information technologies, and brings perspectives on the adjacency of these combined sectors.

Brent Carey (Te Āti Awa) is the Chief Executive Officer at Netsafe. He is a lawyer with areas of interest in tech, privacy, public law and the internet. He has a background in working for integrity and self-regulatory bodies in both New Zealand and Australia, and brings perspectives on malinformation, trust and safety, compliance, and enforcement and internet governance.

Statement from Brent: *Throughout this process, I have been unable to support the creation of a singular civil society organisation tasked with distributing public funds to fight disinformation and misinformation. A number of civil society organisations are already dedicated to bolstering community defences against misinformation and disinformation. Instead, I advocate for the government to continue funding public and private sector specific projects in this area. These projects should have clearly defined scopes, objectives, and measurable, reportable outcomes.*

Dr Mona Krewel is a senior lecturer in the School of History, Philosophy, Political Science and International Relations and the Director of the Internet, Social Media, and Politics Research Lab (ISPRL) at Te Herenga Waka Victoria University of Wellington. She has a background in political communication research, and her work focuses on social media effects on voting behaviour, and online dis- and misinformation. She brings expertise on the use of fake news, half-truths, and conspiracy theories in election campaigns to the group.

Vivien Maidaborn is the CEO of Internet New Zealand Ipurangi Aotearoa, and has experience in civil society, and multi-stakeholder processes and decision making. She has a background in digital equity, social change and the uses of online resources and information in forming social movements. Vivien brings to the group perspectives on use of mis- and disinformation to undermine vulnerable communities' right to participation, and protection.

InternetNZ Ipurangi Aotearoa partnered with DPMC to distribute a one-off fund providing financial support for community-based initiatives that build resilience against the harms of disinformation.

Jeremy Rees is an editor and journalist, and is currently Executive Editor at Radio New Zealand and acted as Head of News during his time on the group. He is a former member of the Media Freedom Committee and has an interest in freedom of expression issues.

Paul Rishworth KC is a barrister at Britomart Chambers, Auckland, specialising in human rights law. His background includes research and teaching in public law at The University of Auckland Law School since 1987. He brings a legal perspective to the group's work.

Statement from Paul: *I was not able to be certain (from the research with which we were provided) that there is disinformation and misinformation causing harm in New Zealand (as opposed to there being differences of political and other forms of opinion, or other forms of communication not within our group's terms of reference such as hate speech and harassment). I accept that, in principle, the propagation of disinformation and misinformation may be harmful and, where it is, that such harm may not always be able to be averted by counter-speech. This is why I am able to support a recommendation that there be a non-governmental entity charged with collating and evaluating further quality research into its prevalence and impact, so as to assist with the evidence base for long term work.*

For this reason, but also for the others given in the report under "recommendation 4", I was not able to support the establishment of an entity that would provide government-sourced funds to particular "community-led mitigation and resilience-building efforts" and conceived as a response to the phenomenon of disinformation and misinformation. But that does not exclude support for general educative measures relating to digital literacy and how to navigate digital media as a source of reliable information.

Dr Chris Wilson is a Senior Lecturer in Politics and International Relations at the University of Auckland. He researches and teaches courses on political violence of various forms, how and why individuals and groups radicalise, including to violent action, and on how societies polarise and descend into violent conflict. He brings his insights on these topics to the group, including how and why disinformation can proliferate and facilitate distrust, hate, intergroup tension, and violence.

Chris is the co-founder and director of Hate and Extremism Insights Aotearoa, which has been commissioned by the Department of the Prime Minister and Cabinet to research and analyse themes and trends in disinformation in New Zealand.

Executive Summary

Mis- and disinformation are complex and delicate challenges and must be addressed carefully. This report examines core definitional questions and both domestic and international landscapes before making the group's recommendations.

Recommendation 1 – be guided by these five principles:

We recommend that any future work on mis- and disinformation response and/or mitigation by either government or civil society draws on five principles which provide guardrails and address responsibilities, trust, evidence-based action, a coordinated approach, and recognition of the sustained and long view of resilience necessary to generate positive outcomes:

PRINCIPLE 1: **Government must act, but carefully and responsibly**

PRINCIPLE 2: **Build trust**

PRINCIPLE 3: **Be evidence-based and iterative**

PRINCIPLE 4: **Supplement and support the existing landscape**

PRINCIPLE 5: **Take a broad and long view**

Recommendation 2 – civil society should lead and coordinate responses to mis- and disinformation in Aotearoa:

This group recommends that civil society should play a leading role in activities to respond to mis- and disinformation. These activities should be coordinated and incorporate a broad range of key stakeholders, with a central point of exchange and accountability.

Recommendation 3 – undertake additional empirical work and evidence-gathering specific to Aotearoa:

Additional empirical work and evidence-gathering is critical to building an evidentiary base to guide and explore the benefits and drawbacks of potential interventions. Support for these functions will almost certainly require ongoing resourcing, including from government.

Recommendation 4 – determine whether and how to fund community-led mitigation and resilience building efforts:

This group has not been able to reach consensus on whether and how government should provide funding for community responses, mitigation and resilience building efforts. Whether and how government should fund these efforts is a question with political, policy, and leadership components that will need to be addressed by future work in this space.

Recommendation 5 – continue to consider and develop New Zealand's approach to increasing resilience to mis- and disinformation:

The above recommendations constitute a first step towards a New Zealand that is resilient at both an institutional and social level to the harms of mis- and disinformation. However, in future, there will be a need to address additional questions, respond to further challenges, and make necessary adjustments. The challenge posed by mis- and disinformation is sprawling and multi-faceted and will need to be addressed on an ongoing basis as New Zealand moves forward.

Table of Contents

Introduction

PURPOSE OF THIS REPORT

This group has been convened to provide advice to the Department of the Prime Minister and Cabinet on how Aotearoa New Zealand can address the dissemination, harms, and causes of disinformation without undermining trust in institutions, engaging in overreach, harming vulnerable groups, unjustifiably limiting free expression under the New Zealand Bill of Rights, and while taking into account the obligations of the Crown to give effect to Te Tiriti o Waitangi.

Problem statement

It is widely acknowledged that people can be convinced of factually false information – sometimes maliciously (often referred to as “disinformation”) – by those seeking to manipulate them, and sometimes benignly (often referred to as “misinformation”) by those acting in good faith. While these phenomena have always been a feature of human communication, ubiquitous internet connectivity and social media have enabled the spread of information – and therefore of these phenomena – on a massively increased scale. The development and deployment of generative AI is considered likely to exacerbate this spread still further by making it easy to create misleading content at scale.

In a number of countries, the spread of mis- and disinformation online is associated with, and believed to have contributed to, state propaganda operations surrounding diplomatic and military conflicts, reducing the effectiveness of public health responses to Covid, and the degradation of social cohesion and democratic resilience.

This can cause harm to individuals (such as convincing them to make dangerous health decisions or encouraging harassment), institutions (such as undermining trust in government or media on the basis of falsehoods), and society as a whole (such as making it harder to reach consensus on important issues that must be addressed). Concrete examples of harm caused by mis- and disinformation include: playing a major role in triggering the January 6 2021 assault on the US Capitol via false claims that the 2020 United States presidential election was stolen, and more recently, the wave of anti-immigrant violence triggered by unfounded speculation following a stabbing in Dublin in November 2023.

Repeated public surveys indicate considerable concern about the impact and prevalence of mis- and disinformation in New Zealand. New Zealand’s 2022 Parliament occupation intensified concerns domestically that we, like many other countries, were at risk of slipping into a “post-truth” society where individuals and communities cannot agree on a common reality or hold any trust in political, media, or social institutions. However, there is also a risk that actions taken to respond to mis- and disinformation (or the perceived harms of mis/disinformation) may risk undermining fundamental human rights, such as freedom of expression. It is widely acknowledged that steps taken by some governments overseas ostensibly to respond to mis/disinformation have unjustifiably undermined human rights, or otherwise further undermined public trust in government.

Definitions and scope

The first challenge for any project that deals with terms like mis- and disinformation is defining them. These terms have accrued a number of finely balanced definitions for different contexts. Importantly, the choice of which definitions to adopt will have a significant impact on the scope of any work undertaken. If the definitions are overly broad, it can create unacceptable impacts for human rights, including freedom of expression. It can also produce misleading or contradicting assessments of the extent of the problem. If the definitions are too narrow, responses and recommendations risk being ineffective and significant harms may be overlooked. Any definitions must account for context, as well as uncertainty and disagreement in the way they are applied.

We have chosen to adopt a relatively broad definition of concepts of mis- and disinformation and of the kinds of harms they can produce. This definition enables us to consider the issue holistically, while preserving space for subsequent efforts in this area to adopt a flexible approach to defining mis- and disinformation depending on their specific work programmes and contexts. These definitions are not suitable for all purposes. When considering any future work or specific interventions, especially those which may be targeted at directly countering or limiting the reach of mis- and disinformation, it will be important to consider whether or not this broad definition is suitable for the given context.

In this report, we use “disinformation” to refer to information that is provably false or misleading, and that is created or disseminated with the intent to cause harm and/or which could reasonably be expected to be harmful to an individual, group or community. We have focused on this definition, so as to explicitly exclude matters of opinion or simple political difference.

Intent to cause harm or to deceive is an important component of legal and academic definitions of disinformation, which sets it apart from misinformation.

We use ‘misinformation’ as a label for information that is false but has not been disseminated with intent to deceive or to do harm. Further caveats and considerations surrounding intent and harm can be found in Appendix A.

Mis- and disinformation often co-occur with other phenomena such as ‘malinformation’ (generally defined as true information shared with intent to cause harm, such as malicious leaks and doxxing), hate speech and harassment. Each is a distinct phenomenon and raises different issues. However, there may be some common factors across mis- and disinformation, hate speech and harassment, and these common factors can be relevant to responding to them effectively. The group has elected to focus on mis- and disinformation specifically, given the range of interventions already underway to address related content and harms, and given the scope of the group’s Terms of Reference.

We also acknowledge that matters of truth are not always clear. There may be fair disagreement about whether something is true or not, or there may be no way of telling whether something is true or false. Some communications may also be harmful, but their truth or falsehood may be irrelevant or inapplicable, for example, because the communication is a matter of opinion or political expression. Under our definition, these cases would not be considered mis- or disinformation.

We acknowledge that even these definitions of mis- and disinformation are open to a certain degree of contextual interpretation, and that different people or groups can often have fair disagreements about whether an individual piece of information constitutes mis- or disinformation. This is unavoidable and we have carefully tuned our recommendations accordingly.

Current context

Domestic

Individuals or groups of people are capable of using communications technologies for illegitimate objectives, or to do harm. In Aotearoa New Zealand, there are claims, research and evidence that the spread of falsehoods presently results in harm to targeted groups, such as trans people and Māori. We include references to the material we have considered in Appendix B. However, based on the available reporting, Aotearoa New Zealand appears to be in a stronger position relative to much of the rest of the world. New Zealanders consistently report comparatively high levels of trust in government, media, and social institutions. While this may be an area of comparative strength, the group acknowledges that this does not forgive or minimise the harm targeted groups report.

Conclusions on the prevalence of mis- and disinformation in New Zealand vary, depending largely on the definitions of mis/disinformation adopted, data collection practices, data sources, and the methods used to infer intent, and accordingly whether or not a given communication should be categorised as mis- or disinformation. The material this group has evaluated indicates however that some of the issues and impacts on community resilience from mis- and disinformation observed in other jurisdictions are also present in New Zealand. There are varying opinions on the degree to which the presence of this mis- and disinformation can be attributed to influence campaigns by nation states. We provide a summary of some of these in Appendix B.

Any analysis of the prevalence and impact of mis- and disinformation in New Zealand (as well as critical assessment of those analyses) will provoke complicated discussions on topics noted in our section on definitions and scope. However, New Zealand is not shielded from broader international trends and influences that contribute to the prevalence, distribution, and impact of mis- and disinformation. In addition, some nation states and state-backed actors have the capability and willingness to conduct influence operations utilising disinformation if they perceive that the circumstances require it. A significant increase in mis- and disinformation runs the risk of undermining attempts to promote digital citizenship and participation, reducing trust and institutional legitimacy and therefore the strength of our democracy.

Based on the experience of group members, the available evidence, broader international trends, and commentary and investigation by experts, the group concludes that some action is necessary to mitigate current harms, and to prevent actual and potential harms from developing further. Also, we cannot discount the experiences of members of the community who report experiencing harm due to mis- and disinformation. This is especially true in situations where mis/disinformation and coordinated online behaviour is accompanied by other kinds of unacceptable behaviour, such as illegal conduct, incitement to hatred or discrimination (hate speech), or incitements to violence.

DOMESTIC RESPONSES

In order to assess where domestic activities should be augmented or supplemented, we have recorded our assessment of the landscape across governmental and non-governmental initiatives.

Several non-governmental initiatives exist in New Zealand for responding to mis- and disinformation. Research into the prevalence of mis/disinformation is performed by the entities surveyed in Appendix B, among others. Civil society organisations offer educational services, support, and (when funding is available) financial support for community-led initiatives to address mis/disinformation and its harms. Grassroots volunteer groups play a range of roles from fact-checking to counter-messaging, to community support. This community-led activity risks being hampered by the absence or inadequacy of resourcing, i.e., the longer-term funding arrangements, time, skills, and focus available to all in this space is limited. The ongoing viability of community-led efforts is dependent on their ability to secure funding.

There are also a range of initiatives underway across government to respond to mis- and disinformation. The Department of the Prime Minister and Cabinet has a role in coordinating some of these efforts across government and has engaged with non-governmental entities to help build resilience towards the harms of mis- and disinformation – for instance, by convening this very group, by partnering with Internet New Zealand to give a grant to enable community-driven responses to mis- and disinformation, and by contracting researchers to conduct empirical research into New Zealand's information landscape. The Electoral Commission has protocols for dealing with inaccurate information and publishes information on how to identify it, and the Ministry of Education has considered the need to navigate false information online when refreshing the curriculum surrounding digital citizenship skills. Independently, the Office of the Prime Minister's Chief Science Advisor has recently undertaken a research project exploring how young people's resilience to false and misleading online information can be built through critical thinking, mana motuhake, and digital citizenship skills.

However, overall domestic efforts remain largely dispersed – within government, outside government, and between government and non-government bodies. This may be desirable where separation of functions and powers is necessary, or legal mandates differ, and to preserve safeguards against dangerous centralisation of response where that may threaten freedom of expression. However, there are benefits to otherwise legitimate and transparent coordination for the following reasons:

- To identify and fill knowledge and funding gaps, surface community projects, and to ensure funding is distributed more effectively.
- To maintain and preserve diversity of response, counter-messaging, and education, as well as minimising unnecessary duplication.
- To allow concerned citizens to properly access and make use of mis- and disinformation response mechanisms, as well as to enable concerned or sceptical citizens to scrutinise overall response and build public trust and confidence.

International

Large-scale trends are deepening many aspects of the challenge posed by mis- and disinformation. Geopolitical tensions and the accompanying use of disinformation techniques are intensifying, and internet platforms dealing with lower revenues, increased user-bases, and pressure to grow are unlikely to be equal to the challenge of effectively and sensitively moderating across the world. Increasingly harsh responses from authoritarian nations continue to lessen social licence for even well-intentioned government interventions elsewhere.

Inequality and economic precarity are on the rise in many countries, and public opinion polls across much of the world show a loss of trust in governments and other key institutions. Other liberal democracies such as the EU, US, the UK, Australia, and other countries across the Asia-Pacific are also struggling with mis- and disinformation. The European Union has implemented sweeping platform transparency laws based in human rights frameworks, which may have a global ripple effect that is yet to be seen. The US is unlikely to see any legislation and has also faced litigation and investigations contesting the legitimacy of mis- and disinformation monitoring and response. Prospective legislation in Australia and new legislation in the UK have drawn significant criticism from both independent human rights observers and mis- and disinformation researchers.

Artificial intelligence (AI) is likely to exacerbate the problem of mis- and disinformation in a number of ways. AI is making it easier to generate convincing but false video, audio, and text at scale. And increasing public awareness of such materials risks undermining confidence in genuine information (the so-called 'liar's dividend' – the idea that if anything can be faked, anything can be a fake). AI also is creating ethical dilemmas for news media (still struggling with adjusting business models for the web) around its use – and whether it would be a boon or a harm, for instance by undermining confidence in news. While there is potential for AI to be used to combat mis- and disinformation (for instance, by improving the moderation capabilities of major platforms), these applications are still speculative and will require significant work to realise.

There are some positive trends, however. Academic and civil society research on the scale and nature of the problem is ongoing and bearing fruit, and there is greater wariness than ever on the part of the public about information that they encounter from unfamiliar sources online (though this can be a double-edged sword – see the 'liar's dividend', in paragraph 22 above). In addition, the Digital Services Act now in effect in the EU – while not universally praised – obliges large internet platforms to disclose more information than ever before and conduct systemic risk assessments that may open new avenues for tackling the problem of widespread mis- and disinformation.

INTERNATIONAL RESPONSES

Both state and non-state actors (including companies and civil society) around the world have attempted to respond to mis- and disinformation in a range of ways. A comprehensive overview of these approaches (framed around disinformation but also largely applicable to misinformation) was compiled in 2020 by the Broadband Commission for Sustainable Development, a group established by the International Telecommunications Union and UNESCO in 2010. Through viewing disinformation holistically as a lifecycle – from instigation and creation to the means of propagation and dissemination, to impact – the report usefully highlights four key categories of disinformation responses, which each fall at different parts of this lifecycle. While there is not space in this report to thoroughly explore each response category, we think it is worthwhile to give a brief summary of these categories to illustrate the breadth of ways in which the issue of disinformation is being addressed internationally.

INSTIGATORS. Actors who initiate the creation and distribution of particular content. Often the real source and beneficiary of much disinformation and may pay for operationalisation.

AGENTS. Distributors of disinformation who operationalise the creation and spread of disinformation. In some cases, may be the same as instigators, but in many large-scale cases, agents may be paid or voluntary supporters or contractors of instigators. Could also be unwitting participants.

The first category of responses is aimed at the producers and distributors of disinformation (the 'instigators' and 'agents' stages on the lifecycle). These are mainly law and policy responses that aim to alter the environment governing and shaping the behaviour of instigators and agents of disinformation. Examples of responses in this category include regulatory action from governments, ranging from inquiries and proposed laws through to legislation and law enforcement, but they can also include softer approaches as well, such as counter-disinformation campaigns.

MESSAGES. The false and/or manipulated content that is being spread and the way it is expressed.

The next broad category consists of identification responses (aimed at the 'messages' stage of the lifecycle), which are focused on identifying, debunking, and exposing mis- and disinformation messages. The objective of these responses is to pinpoint the existence and extent of mis- and disinformation, and can include mis- and disinformation monitoring functions, fact-checking, and investigative responses. These responses are carried out by a range of actors, including news organisations, academia, civil society organisations, and independent fact-checking organisations.

INTERMEDIARIES. Vehicles for the message (e.g. social media sites and apps). These systems may enable or disable content, actors and behaviours.

The third category of responses is aimed at the production and distribution mechanisms of mis- and disinformation (the 'intermediaries' stage of the lifecycle). This involves the policies and practices of the platforms that are mediating content, such as social media, search engines and other platforms. These responses include content moderation and editorial policies, appeal mechanisms for users, automated systems that limit the spread of particular posts, and demonetisation measures to stop people profiting from sharing disinformation.

TARGETS / INTERPRETERS. Those targeted by disinformation and the effects on their beliefs and actions.

The final response category is aimed at the target audiences or interpreters of mis- and disinformation campaigns, which the report describes as the potential 'victims' of mis- and disinformation (the 'targets/interpreters' stage of the lifecycle). This category includes educational responses (such as media literacy, critical thinking or civics education), as well as ethical and normative responses (which involve public condemnation of acts of disinformation). It also includes empowerment and credibility labelling efforts, which are external tools and websites that help assist users to understand the nature of the information they are engaging with.

The report notes that evaluating the efficacy of many of these types of responses is difficult. Many of the responses are relatively new and have not yet seen broad adoption, therefore a systematic approach to evidence gathering has not yet been widely established. Nevertheless, the report recommends that a key guiding principle for all disinformation responses must be a commitment to freedom of expression and human rights. It therefore puts forward a 23-step assessment tool for evaluating the human rights impacts of future disinformation responses, particularly in relation to freedom of expression (see Appendix C).

Adapted from 'Disinformation lifecycle' from the Broadband Commission for Sustainable Development report

Defining an appropriate role for Government

Mis- and disinformation are complex topics to tackle and the appropriate role for government requires extensive discussion reflecting different perspectives. It is important to consider the risk – and reality – that the production, distribution, and adoption of mis- and disinformation may also be a symptom of broader social problems and inequities. A major driver and accelerant of mis- and disinformation is distrust in institutions such as government, and many communities in Aotearoa New Zealand are justifiably wary of government interventions – especially when they run the risk of infringing on fundamental rights such as freedom of expression. This wariness is intensified by authoritarian countries taking overt steps to control public discourse relying upon 'fake news' or 'disinformation' as justification. In the group's discussions, institutions responsible for monitoring the integrity of government departments were also identified as playing a role in responding to mis- and disinformation, both through correcting false information, as well as building public trust and confidence in government activities. Without strong social licence, interventions risk exacerbating the very problems they seek to address – and even with the best of intentions, it is always possible for coercive interventions to overstep their bounds and themselves cause harm, including to the communities they seek to protect.

Although our remit was to consider and report on a "civil society" response to the problem of disinformation – as opposed to governmental or legislative responses – we recommend strongly against expanding the existing categories of objectionable material that are already established as legitimate targets for government censorship. Expanding the use of censorship can increase distrust in government, which creates the conditions for both greater production of mis- and disinformation and its more rapid spread. In addition, it is often ineffective unless it is deployed on a scale that would be unacceptable in Aotearoa. Caution must also be exercised in the case of procedures that may result in even indirect removal or chilling of expression, such as government or non-government entities flagging problematic content directly with internet platforms (including through "trusted flagger" mechanisms).

We are highly reluctant to recommend any actions which have the potential to stifle freedom of expression. Our deliberations have not treated freedom of expression as an absolute right, given that the New Zealand Bill of Rights Act 1990 affirms all rights in terms that permit "reasonable limits" that are "prescribed by law" and "demonstrably justified in a free and democratic society". Instead, in the context of Aotearoa New Zealand's constitutional system, society and values, freedom of expression must be weighed alongside other rights, obligations, responsibilities, and accountabilities including Te Tiriti o Waitangi, as well as other considerations such as New Zealand's unique cultural contexts, obligations to protect people and groups from certain kinds of harm, and the wider challenge posed by mis/disinformation itself. In any event, we are clear that any such actions must be legal, necessary, proportionate, transparent, and for a legitimate objective. Therefore our focus has necessarily been on considering a civil society response to disinformation rather than legislative responses that prescribe any new law.

Further, we note that there are already laws, rules, and systems in place for mis- and disinformation's most damaging co-occurrences, such as hate speech, terrorist and violent extremist content, and harassment. The group acknowledges that for many people, these current solutions are underutilised, imperfect and ineffective. However, making additional recommendations for more effective prevention measures in these areas is beyond the scope of this group's assignment. In our recommendations, we have tried to avoid unnecessary duplication or overlap, but we conclude that New Zealand's resilience to mis- and disinformation would be strengthened if the systems for responding to these co-occurring phenomena were used when intended, enforced where appropriate, and reformed if ineffective.

Due to the importance of maintaining trust and public concerns about government censorship and overreach, any large-scale and enduring response to mis- and disinformation must have a substantial non-governmental component. Non-governmental responses can also be more effective, especially where they are more closely connected to communities and their real experiences. The group acknowledges the inherent limitations in Government action in this area: the core principles of a Parliamentary liberal democracy require extreme care when engaging in any government activity that could enable a government to dictate what is 'true' or 'false'.

However, the Government is also an important stakeholder – it has unique resources and capabilities alongside non-governmental actors and has obligations to address and promote the integrity of the information environment, not just to refrain from interfering. In New Zealand, the Crown has obligations of protection and promotion of a range of rights and interests under Te Tiriti o Waitangi and human rights instruments, and there is increasing discussion in multilateral institutions about States' obligations in response to mis- and disinformation. Obligations can include activities to promote and provide reliable information, including through counter-messaging campaigns, and intervening to protect the freedom of expression of marginalised or targeted individuals and groups. There are also some areas such as foreign interference that are best handled with Government powers and resources. Government is a necessary partner in activities to combat mis- and disinformation, but it should be part of the discussion rather than leading it.

Our recommendations

This group has developed its recommendations as far as possible in light of its working parameters (see Group members and process) and has deliberately opted for an approach that enables future role-players to develop its recommendations in ways that make sense in the circumstances and contexts that arise.

It is not necessary, desirable, or possible to stop people being wrong on the internet. Mis- and disinformation have been with us since the dawn of social relations, and trying to banish them completely would be a futile endeavour. Likewise, the group has been conscious throughout our work and discussions of the overlaps between mis- and disinformation and freedom of expression; the perspective that "counter" expression is an adequate response to instances of mis- and disinformation to "balance out" narratives; the extent and relativity of harm that may occur from mis/disinformation; and the risk of overreach in attempts to respond to it.

For these reasons, the group believes that its goal should instead be to mitigate the harm mis- and disinformation cause and to move towards ensuring that within New Zealand, people can agree and disagree in good faith working off a mostly shared set of facts, and that when disputes occur – especially consequential disputes – they are possible to resolve with reference to trustworthy evidence.

RECOMMENDATION 1

Consider these guiding principles in working on disinformation in Aotearoa

1. Government must act, but carefully and responsibly.
2. Build trust.
3. Be evidence based and iterative.
4. Supplement and support the existing landscape.
5. Take a broad and long view.

RECOMMENDATION 2

Civil society should lead responses to mis- and disinformation in Aotearoa

RECOMMENDATION 3

Undertake additional empirical work and evidence gathering specific to Aotearoa

RECOMMENDATION 4

Determine whether and how to fund community led mitigation and resilience building efforts

RECOMMENDATION 5

Continue to consider and develop New Zealand's approach to increasing resilience to mis- and disinformation

RECOMMENDATION 1

Consider these guiding principles in future work

We recommend that any response to mis- and disinformation should be designed with the following principles or values in front of mind and should be considered when engaging in any future work. These principles have informed the group's subsequent recommendations.

PRINCIPLE 1. GOVERNMENT MUST ACT, BUT CAREFULLY AND RESPONSIBLY

Misinformation and disinformation can create harm to institutions, social structures, and the lives of individual New Zealanders. Government has a responsibility to act to mitigate these harms, but must do so very cautiously to prevent overreach, loss of trust, or other unintended consequences. Any actions taken by the government must be legal and proportionate, and crisis responses should be time-limited and wound down as soon as possible. In broader responses, government is an important stakeholder, but should not dictate terms.

PRINCIPLE 2. BUILD TRUST

Mis- and disinformation thrive on mistrust, and any attempt to address or mitigate them should seek to build trust and consensus wherever possible. As such, while no effort can perfectly appeal to all parties, responses should take all actions possible to be non-partisan, transparent, consistent, and publicly accountable.

PRINCIPLE 3. BE EVIDENCE-BASED AND ITERATIVE

A strong empirical evidence base is necessary to ensure both a clear picture of the problem being addressed by any given response and that the response is effective. This should include studying past and present responses in order to inform future responses. Continued evidence-gathering – including both academic research and community research and consultation – will be a crucial component of any successful efforts to mitigate and build resilience to mis- and disinformation. Given the complexity of the issues in question, this evidence-gathering should be multidisciplinary and inclusive.

PRINCIPLE 4. SUPPLEMENT AND SUPPORT THE EXISTING LANDSCAPE

There are already a wide variety of entities and projects engaged in efforts in this space, from volunteer groups and NGOs to government agencies. New efforts should strive to supplement and support existing work rather than duplicating it and ensure that there is greater coordination and alignment in this space. This also entails recognising the value of the unique perspectives held by different groups, bringing together diverse selections of participants for multistakeholder discussions when relevant, and knowing when to defer to those with community-specific or local expertise.

PRINCIPLE 5. TAKE A BROAD AND LONG VIEW

It takes time to build resilience, so many forms of response will need to be sustained for multiple years in order to achieve the desired results. This means planning ahead and securing durable support for such long-term projects. In addition, the creation and consumption of mis- and disinformation by both individuals and groups is increasingly considered a symptom of lack of trust in institutions and economic, political, and social anxiety. As such, an effective holistic response to mis- and disinformation must address these underlying issues.

RECOMMENDATION 2

Civil society should lead responses to mis- and disinformation in Aotearoa

This group recommends that civil society should play a leading role in activities to respond to mis- and disinformation. These activities should be coordinated and incorporate a broad range of key stakeholders, with a central point of exchange and accountability.

This will achieve a number of important outcomes including:

- greater transparency and accountability for mis- and disinformation response activities;
- more effective responses across Aotearoa New Zealand due to increased alignment and decreased duplication of effort;

- improved information-sharing between mis- and disinformation response efforts; and
- more effective and efficient allocation of resources.

Whether an existing organisation assumes these functions, or a new body or network is formed in order to fulfil them, these activities should comply with the five principles outlined above.

RECOMMENDATION 3

Undertake additional empirical work and evidence-gathering specific to Aotearoa

In addition to the coordination of civil society responses to mis- and disinformation, this group concludes that additional empirical work and evidence-gathering is critical to building an evidentiary base to guide and explore the benefits and drawbacks of potential interventions. Support for these functions will almost certainly require ongoing resourcing, including from government.

Throughout this process, our group has seen and reviewed a sample of the available information that aims to describe and analyse the nature and impacts of mis- and disinformation domestically and internationally. This includes early outputs of research groups funded by DPMC as part of its 'Public Research and Insights into Disinformation' workstream. Domestically, there is a growing body of research looking at impacts in Aotearoa, however more information is needed to determine what impacts there are with more confidence.

The availability of more empirical data and evidence will assist with appropriate scoping and design of some interventions, and thus allow them to be more impactful. A formal central point for research collation and sharing is also recommended to improve the quality and availability of research. Whether this role is best played by the coordinating entity or network referred to in recommendation 2 or by another entity or network cannot be determined at this point and is a question that future efforts in this space will need to address.

RECOMMENDATION 4

Determine whether and how to fund community-led mitigation and resilience building efforts

This group has not been able to reach consensus on whether and how government should provide funding for community responses, mitigation and resilience building efforts.

On one hand, some group members are concerned about the risks of providing such funding to community-led interventions. At the least, these group members believe that the provision of funding in this manner creates several risks, and that the design and execution of any new funding mechanisms would need to avoid or substantially mitigate:

- Appearing to create or substantially creating undue influence on behalf of the funders, whether they are government or other actors.
- Bias in funding mechanisms favouring providing funds to some groups over others.
- Funding going to projects that fail, or embrace partisanship, undermining trust in the overall response.
- Enabling projects that may give the appearance of trying to label legitimate discourse and good-faith disagreement as mis- and disinformation.

Further, those members that are concerned about the provision of funding for community-led initiatives believe that these issues are so fundamental and so acute in the case of government funding for responses to mis- and disinformation in Aotearoa that they may not be resolvable without creating further issues and harm, and/or feeding further distrust of interventions. For that reason, those members do not seek to make a recommendation in this regard.

Another group of members take the opposite view, believing that the provision of funding for community-led activities is both essential and urgent. These members believe that the risks of providing such funding either do not arise, are outweighed by the benefits of having interventions supported in the communities they serve or can be adequately managed through a careful and considered approach to providing such funding. These members believe that a provision for funding for community initiatives would have the following benefits:

- Communities currently targeted for misinformation continue to be harmed and report experiencing unsafe experiences online to a greater degree than those not targeted. This has potential detrimental impacts on participation from those groups in education, community discourse and recreation activities.
- Funding would prevent the loss of important knowledge and skills in a rapidly developing social and business context, which may otherwise occur if the current set of non-governmental skills and programme providers were unable to continue their activities.
- Community investment will complement the early education and literacy programmes to increase resilience to mis- and disinformation that government have invested in to date.
- Avoid the risk of the perception that government is protecting freedom of expression over harms to targeted communities.

Further, these members argue that community projects are more effective than other efforts in mitigating harms caused by mis- and disinformation due to their closeness to targeted communities, and that providing government funding to currently extant community projects should be an immediate priority as many report they will be unable to continue without immediate support.

Whether the risks listed are serious enough to outweigh the reasons for acting is a political question based on matters of judgement and personal values. How to design mechanisms to manage those risks is a policy question. Whether those mechanisms are adequate given the risks they are intended to manage is a political leadership question. These questions could not be answered in the abstract by this group, and will likely need to be addressed on a case-by-case basis by any future efforts in this space.

RECOMMENDATION 5

Continue to consider and develop New Zealand's approach to increasing resilience to mis- and disinformation

The recommendations this group has made constitute a first step towards a New Zealand that is resilient at both an institutional and social level to the harms of mis- and disinformation. However, as these recommendations are implemented, additional questions will need to be answered. We have outlined the most important of these below:

- Should a new entity be created to fulfil the coordination function, or should an existing entity or entities be nominated? The group recognises that there are a range of options in terms of existing entities, and that all of these options should be considered. Such consideration should include an assessment of the suitability of existing entities, the availability of funding and expertise for a new entity, and the expected effects of introducing a new entity to the already complex ecosystem of mis- and disinformation response in New Zealand.
- How should this entity or network be designed (or modified) in order to fulfil its role effectively? The principles outlined earlier in this section provide a strong basis, but as the work becomes more concrete other considerations will emerge.
- Should the other key functions – evidence-gathering and support for resilience-building efforts – also be administered by the coordinating entity or network, or by other entities?

- What processes and constraints around funding should be in place? These should be considered both for funding provided to the coordination entity or network – and any other entities fulfilling the key functions – and funding provided by these entities.
- Which aspects of our empirical evidence base around New Zealand's information environment most need to be supplemented?
- Which forms of resilience-building and/or community response are the highest priority for support?

Once these recommendations have been implemented, it will be necessary to re-evaluate their results to ensure that they are creating the desired outcomes. For this reason, we also recommend a review and possible readjustment of response activities in a 3–5-year timeframe following implementation. The lessons and experience gained through operating the coordinating entity or network will also in of itself provide a basis for answering and updating this list of questions, and a basis through which a coordinating body may adapt to desired outcomes.

The challenge posed by mis- and disinformation is sprawling and multi-faceted. While no single group or report can solve these issues entirely, we believe that the principles and recommendations given here will stand New Zealand in good stead as it moves forward into an increasingly information-dense, complicated, and precarious world.

Appendix A.
Additional definitional concerns and considerations

The group found it necessary to treat the topic of intent with great care for the following reasons:

- In practical contexts, it is rarely possible to conclusively determine the intent that sits behind a communication, or even a pattern of communication among multiple people or groups.
- Some signals used to determine intent – such as indicators of coordinated behaviour, or shared messaging – can be signs of authenticity, or reflect sincere belief. It may be possible for different people to disagree about whether coordination, or shared beliefs or sentiments indicate intent to do harm.
- If disinformation campaigns are effective, they will frequently be re-shared by people or groups who do not have any malicious intent and have been deceived. People also re-share false information for a range of complex reasons.
- In some situations, knowing whether a person or group is intending to do harm or intending to deceive can be very important for considering how to respond, and whether certain kinds of responses will be effective. For instance, in some situations, if there are strong reliable indicators of intent to deceive or do harm, then more rigorous interventions may be justified.
- False information can be harmful, even if it is not shared with intent to do harm or to deceive anyone.

Harm is another concept that we opted not to comprehensively define in this report, as we think that assessments of harm will depend heavily on contextual factors, including the following:

- Not all false information is equally harmful to everyone. The severity and type of harm caused by the same false information can vary widely for different people or groups.
- Different communities may have different perceptions of what constitutes harm or serious harm.
- The harmfulness of otherwise false information may depend heavily on context, for example, current events may make an otherwise innocuous false statement harmful.
- In some situations, there might be fair disagreement about whether or not something is actually harmful, potentially harmful, or can be shown to have caused harm.
- In some situations, there might be fair disagreement about whether the potential harms should otherwise be tolerated because they are justifiable for other reasons, such as freedom of expression, or other human rights.
- Harms which might be seen as low level or less serious may still be able to be mitigated without restricting freedom of expression or introducing other negative consequences, so focusing on serious harm alone is unnecessary.

It may also be useful to refer to the Harmful Digital Communications Act 2015 as an indication of parameters for unacceptable kinds of communications that have been accepted in Parliamentary debate. This is not to say that the Harmful Digital Communications Act has no flaws – only to say that a starting point for discussion may be useful.

Appendix B.
Summary of assessments on New Zealand's information environment

Misinformation and disinformation narratives in the 2023 New Zealand General Election
(commissioned by DPMC)

Logically Limited analysed posts from platforms including X/Twitter, Facebook, Instagram, Telegram, TikTok, YouTube, Reddit, and 4chan in a four-week period around Aotearoa's 2023 general election. This work was primarily focused on locating and classifying election-related mis- and disinformation. While they found numerous examples of false claims and misleading narratives intended to undermine the perceived legitimacy of New Zealand's democratic process, they concluded that there was no evidence of either coordinated inauthentic behaviour or foreign information manipulation/ interference, and that narratives that may have posed a risk to public safety and undermined confidence in the democratic process were 'highly limited in reach to only a small minority of the population'.

Disinformation Trends in New Zealand: A HEIA Snapshot Report, October 2023
(commissioned by DPMC)

HEIA analysed posts from 'publicly available platforms where disinformation is prevalent (4chan, 8kun, Gab, Telegram, Reddit)' over the first 10 months of 2023. They found key interconnected narrative threads in New Zealand-based disinformation: Distrust of the response to Covid-19 and health authorities more generally, conspiracy theories that New Zealand is being manipulated by 'globalists' creating a 'new world order', claims that New Zealand is anti-democratic and unlawful, and belief that social justice causes such as trans rights and co-governance are nefarious attempts to weaken society. They emphasise that the platforms and posters they analysed represent a small fraction of New Zealand's population but feel that 'many of these ideas have a wider constituency in the country'.

Understanding the New Zealand Online Extremist Ecosystem
(commissioned by DIA, 2021)

This report from the Institute for Strategic Dialogue was focused on extremist content, though the authors noted that this has a sizable overlap with disinformation. They examined users and content across Twitter/X, YouTube, Facebook, Gab, Parler, Reddit, Telegram, and some smaller platforms. Multiple researchers collaborated to ensure that data captured was explicitly extremist and originating from users that identified themselves as New Zealanders. Their research found that 'extremist accounts make up a tiny proportion of New Zealand users of social media' but 'are noisier, more visible and angrier online than the average New Zealand user'. They also noted that 'the far-right are by far the most numerous and active group online.'

New Zealand Social Media Study (NSMS): Election 2023

The Internet, Social Media, and Politics Research Lab at Victoria University analysed Facebook posts by New Zealand political parties and their leaders over the election period. They found only a minimal increase in the percentage of posts they identified as either 'fake news' or 'half-truths' compared to their 2020 election survey. Of these posts, almost 80% attacked health institutions (53%) and experts (25%). Other targets of attack in disinformation posts included transgender people (15.8% of posts), the government (15.8%), the 'mainstream' media (8.4%), and Māori (7.7 %). While some posts by

parliamentary parties or their leaders were classified as ‘half-truths’, only a few relatively small outside-parliament parties’ posts were considered to qualify as ‘fake news’.

Public polling
by Netsafe, the Classification Office, and DPMC

Polling by a variety of organisations has consistently found high levels of concern about mis- and/or disinformation on the part of the New Zealand public. A 2020 survey by Netsafe found that eight in ten respondents recalled seeing ‘fake news’ on social media, with 52% admitting they had fallen for at least one piece of fake content. 48% were concerned that they may mistakenly spread false information.

A 2021 survey by the New Zealand Classification Office found that 82% of respondents were ‘somewhat’ or ‘very’ concerned about the spread of misinformation in New Zealand, with only 2% ‘not concerned at all’. 75% and 74% respectively expressed that false information about Covid-19 and climate change was either ‘definitely’ or ‘probably’ an ‘urgent and serious threat’. 81% expressed that they thought misinformation was becoming more common over time.

The 2022 National Security Public Survey commissioned by DPMC found that 84% of respondents considered the threat posed by misinformation ‘somewhat real’ or ‘very real’. This was the second highest level of concern recorded, compared to 87% for natural disasters, 47% for other countries interfering in New Zealand’s interests in the Pacific, and 43% for the personal safety of themselves or their family being violated.

New Zealand’s media landscape and mis/disinformation (presented to group)

A presentation to the Multistakeholder Group by an experienced news media veteran noted that levels of hostility towards journalists in the country had grown as mis- and dis-information levels had risen, and that reporters were increasingly having to take precautions to protect themselves including de-escalation training and reporting in pairs during periods of tension. Media play a key role against mis- and disinformation through verifying facts, reporting issues and different points of view. But it can be hard for the industry as a whole to react to significant mis-information because media companies are independent and there are fewer industry bodies which bind the ecosystem together, save the Media Freedom Committee. The workforce is also increasingly stretched.

The Disinformation Project
– ongoing monitoring work

Since 2020, The Disinformation Project has conducted ongoing disinformation monitoring work on social media. Earlier work examined the prevalence and nature of unreliable and untrustworthy narratives around the Covid-19 pandemic, finding that Aotearoa New Zealand’s experience was linked to international mis- and disinformation trends, with some local differences. Later work has examined the prevalence of ‘dangerous speech’ online in Aotearoa New Zealand, including transphobic, misogynistic and racist rhetoric. Overall, the Disinformation Project contends that there is a direct link between this online speech and offline violence, and that foreign actors are intentionally manipulating New Zealand’s information environment.

Appendix C.
Tool to assess disinformation responses

Taken from *Balancing Act: Countering Digital Disinformation while respecting Freedom of Expression* by the ITU/UNESCO Broadband Commission for Sustainable Development. We note that these questions are generally intended to apply to legislative responses rather than the civil society response we discuss in the report.

Have responses been the subject of multi-stakeholder engagement and input (especially with civil society organisations, specialist researchers, and press freedom experts) prior to formulation and implementation? In the case of legislative responses, has there been appropriate opportunity for deliberation prior to adoption, and can there be independent review?

Do the responses clearly and transparently identify the specific problems to be addressed (such as individual recklessness or fraudulent activity; the functioning of internet communications companies and media organisations; practices by officials or foreign actors that impact negatively on e.g., public health and safety, electoral integrity and climate change mitigation, etc.)?

Do responses include an impact assessment as regards consequences for international human rights frameworks that support freedom of expression, press freedom, access to information or privacy?

Do the responses impinge on or limit freedom of expression, privacy and access to information rights? If so, and the circumstances triggering the response are considered appropriate for such intervention (e.g., the Covid-19 pandemic), is the interference with such rights narrowly-defined, necessary, proportionate and time limited?

Does a given response restrict or risk acts of journalism such as reporting, publishing, and confidentiality of source communications, and does it limit the right of access to public interest information? Responses in this category could include: 'fake news' laws; restrictions on freedom of movement and access to information in general, and as applied to a given topic (e.g., health statistics, public expenditures); communications interception and targeted or mass surveillance; data retention and handover. If these measures do impinge on these journalistic functions or on accountability of duty-bearers to rights-holders in general, refer to point 4.

If a given response does limit any of the rights outlined in 4, does it provide exemptions for acts of journalism?

Are responses (e.g., educational, normative, legal, etc.) considered together and holistically in terms of their different roles, complementarities, and possible contradictions?

Are responses primarily restrictive (e.g., legal limits on electoral disinformation), or there is an appropriate balance with enabling and empowering measures (e.g., increased voter education and media and information literacy)?

While the impact of disinformation and misinformation can be equally serious, do the responses recognise the difference in motivation between those actors involved in deliberate falsehood (disinformation) and those implicated in unwitting falsehood (misinformation), and are actions tailored accordingly?

Do the responses conflate or equate disinformation content with hate speech content (even though international standards justify strong interventions to limit the latter, while falsehoods are not per se excluded from freedom of expression)?

Are journalists, political actors and human rights defenders able to receive effective judicial protection from disinformation and/or hateful content which incites hostility, violence and discrimination, and is aimed at intimidating them?

Do legal responses come with guidance and training for implementation by law enforcement, prosecutors and judges, concerning the need to protect the core right of freedom of expression and the implications of restricting this right?

Is the response able to be transparently assessed, and is there a process to systematically monitor and evaluate the freedom of expression impacts?

Are the responses the subject of oversight and accountability measures, including review and accountability systems (such as reports to the public, parliamentarians, specific stakeholders)?

Is a given response able to be appealed or rolled-back if it is found that any benefits are outweighed by negative impacts on freedom of expression, access to information and privacy rights (which are themselves antidotes to disinformation)?

Are measures relating to internet communications companies developed with due regard to multi-stakeholder engagement and in the interests of promoting transparency and accountability, while avoiding privatisation of censorship?

Is there assessment (informed by expert advice) of both the potential and the limits of technological responses which deal with disinformation (while keeping freedom of expression and privacy intact)? Are there unrealistic expectations concerning the role of technology?

Are civil society actors (including NGOs, researchers, and the news media) engaged as autonomous partners in regard to combatting disinformation?

Do responses support the production, supply and circulation of information – including local and multilingual information – as a credible alternative to disinformation? Examples could be subsidies for investigative journalism into disinformation, support for community radio and minority-language media.

Do the responses include support for institutions (e.g., public service messaging and announcements; schools) to enable counter-disinformation work? This could include interventions such as investment in projects and programmes specifically designed to help ‘inoculate’ broad communities against disinformation through media and information literacy programmes.

Do the responses maximise the openness and availability of data held by state authorities, with due regard to personal privacy protections, as part of the right to information and official action aimed at pre-empting rumour and enabling research and reportage that is rooted in facts?

Are the responses gender-sensitive and mindful of particular vulnerabilities (e.g., youth, the elderly) relevant to disinformation exposure, distribution and impacts?

If the response measures are introduced to respond to an urgent problem or designed for short term impact (e.g., time sensitive interventions connected to elections) are they accompanied by initiatives, programmes or campaigns designed to effect and embed change in the medium to long term?

Strengthening civil society resilience to disinformation in Aotearoa New Zealand • Recommendations from the Multi-Stakeholder Group advising the Department of the Prime Minister and Cabinet

FEBRUARY 2024 • ISBN 978-0-947520-41-0

This work is licensed under the Creative Commons Attribution 4.0 International licence. You can copy, distribute and adapt it, as long as you attribute the work and abide by the other licence terms. For more information, go to creativecommons.org/licenses/by/4.0/