DIGITAL THREATS TO DEMOCRACY DIALOGUE

Dialogue Summary Report

LOWY
INSTITUTE

Executive summary

The Lowy Institute convened the Digital Threats to Democracy (DTD) Dialogue on 12 October 2022. This Dialogue was funded by the New South Wales Department of Premier in Cabinet and was a day-long, closed-door session that brought together a distinguished group of diverse subject matter experts, government officials and civil society stakeholders to examine intersecting digital challenges to democracy. The aim of the Dialogue was to foster connections across subject matter and policy areas in order to spark new ideas and more coordinated approaches to meet these challenges. To foster frank discussion, the session was conducted under Chatham House rules. Therefore the comments and recommendations made during the Dialogue and reflected in this report are not attributed. Additionally, the summary of the Dialogue and recommendations for future consideration should not be taken as endorsed or agreed upon by all Dialogue participants but rather are a reflection of the ideas and topics discussed.

The Dialogue was the cornerstone of a broader 12-month project that seeks to identify and examine the intersecting digital threats to democracy across four key areas: online disinformation, online hate and extremism, tech-enabled foreign interference and regulation of the digital sphere.

The Dialogue was structured according to these key themes and organised and hosted by Research Fellow and Project Director Lydia Khalil from the Transnational Challenges Program at the Lowy Institute. The Dialogue was divided into five concurrent panels that featured presentations by subject matter experts, followed by a moderated discussion between Dialogue participants. The Dialogue also included two keynote speeches delivered by international experts Nina Jankowicz, Vice President at the UK-based Centre for Information Resilience, and Dr Joan Donovan, Research Director of the Shorenstein Center on Media, Politics and Public Policy at Harvard University.

The following Summary Report consolidates and summarises the key points of the presentations, discussions and recommendations for consideration that arose from the DTD Dialogue.

Dialogue program and information

On 12 October 2022, the Lowy Institute convened the Digital Threats to Democracy (DTD) Dialogue. The Dialogue brought together subject matter experts, government officials and civil society stakeholders to examine intersecting digital threats to democracy. The Dialogue was organised and hosted by Research Fellow and Project Director Lydia Khalil from the Transnational Challenges Program at the Lowy Institute. The aim of the Dialogue was to foster connections across subject matter and policy areas to spark new ideas and coordinated approaches to digital challenges to democracy.

The DTD Dialogue was structured around five panels that each featured presentations by subject matter experts, followed by a moderated discussion between Dialogue participants. The following are descriptions of the panel topics and issues considered.

Participants in the Dialogue examined and debated the challenges posed by and within the digital realm to the functioning of democratic procedures, levels of trust in democratic governance and the information environment that impacts the way citizens participate and interact in democratic societies. Two keynote speeches were delivered by international experts Nina Jankowicz, Vice President at the UK-based Centre for Information Resilience, and Dr Joan Donovan, Research Director of the Shorenstein Center on Media, Politics and Public Policy at Harvard University.

Panels and discussions

Panel 1: Tackling online disinformation

Panel presenters and Dialogue participants were asked to engage with how disinformation impacts citizens' ability to access accurate information, which is essential for deliberation and decision-making in democracies. They also considered how disinformation is reducing trust in democratic governance, increasing polarisation, corrupting information ecosystems and even undermining consensus reality. A key question that Dialogue participants debated was what could be done to mitigate the spread of disinformation online or whether government should enact policies to counter disinformation online and its effects. The panel also assessed the criteria for what would make a successful countering disinformation program or policy.

Panel 2: Understanding and addressing online extremism

A growing body of evidence demonstrates that the internet can be an important factor in facilitating radicalisation to violent extremism. At the same time, there is acknowledgement that such a broad conclusion requires more detailed analysis. The panel engaged with how the internet and other computer-mediated communications can have multiple and various roles in facilitating radicalisation and mobilisation to violent extremism. Discussion centred on whether content moderation was an effective or sufficient mechanism to counter the expression of violent extremism online and what else should be considered to counter online extremism and its real-world harms.

Panel 3: Foreign interference in the digital realm

The digital environment has provided more opportunities for malign foreign influence and foreign interference. Through digitally enabled information warfare operations, election interference, deep fakes and various other means of undermining democratic political processes and institutions, foreign actors are violating national sovereignty via digital technologies. Participants discussed how democracies, in responding to this challenge, should react proportionately and according to democratic principles. The panel also addressed the ways in which digitally enabled disinformation, extremism and foreign interference are linked. They considered a wide range of comprehensive policy responses to address these interrelated digital challenges to democracy.

Panel 4: Regulation and transparency

After many years of a laissez-faire approach to the tech sector, there are increasingly louder calls for tighter regulation — and government has responded. But despite the new regulations that are being enacted and considered, there are few that address the tech sector's underlying business model of data acquisition and exploitation. Dialogue participants discussed the tensions between safety regulations and concerns about privacy and freedom of expression and how to best balance these competing priorities. Participants also considered regulations that would proffer greater transparency, particularly algorithmic transparency, from digital platforms and how gaining a greater understanding of how digital platforms function would help to address digital challenges to democracy.

Panel 5: Digital citizenship and impacted communities

In multicultural democracies and pluralistic societies, certain communities can be targeted as a means to undermine democratic institutions and social cohesion. At the same time, individual citizens and civil society groups have found ways to harness the digital environment to better engage in deliberation, dialogue and to address polarisation and other digital challenges. Dialogue participants examined ways in which particular communities have been impacted by online harms and how civil society and government can best mobilise to support solutions to these challenges.

Key takeaways

- Digital communications technologies have undoubtedly brought benefits and advantages to the way people work, live and communicate. But along with these benefits have come a myriad of challenges that acutely impact democratic societies. Australia is well placed to meet these challenges and has a number of protective factors embedded in its democratic structures and approaches. However, we must be proactive in meeting these challenges as they are ever evolving.

- Individuals can make a difference in countering digital threats to democracy, but societies cannot rely solely on interventions that target individuals or put the onus of responsibility to address these challenges on individual citizens. Rather, a whole-of-society approach is needed, with more leadership and regulation by the state.

- Many digital threats to democracy are created by a combination of human and technological vulnerabilities. Therefore, we cannot solely "engineer" ourselves out of these problems. We need more people- centred solutions that address human needs, frailties and vulnerabilities and approaches that can harness human emotions, ingenuity and resilience. Currently, technology and engineering are leading tech policy and development but these need to be accompanied by social and human centric approaches.

- Digital technologies have enabled the decentralisation and rapid increase of information and content production. The massive quantities of information, content and data that are produced also make the battle for attention more contested, creating a negative feedback loop of attention-grabbing content that is often highly polarising, arousing or distracting in ways that do not serve democratic societies.

- Human attention is the prized commodity in the digital economy. The 'attention economy,' driven by the clicks, views and likes of online content, drives revenue to the for-profit platforms that dominate the online ecosystem and monetises attention in ways that challenge democracy.

- Alongside the attention economy is the extraction of massive amounts of user data that is used to deliver more attention-grabbing content and targeted advertising. This poorly regulated business model has been utilised and weaponised for the spread of online disinformation and provided a mechanism for malign foreign influence and foreign interference in addition to distracting us away from more fulsome engagement in our democracy.

- More agile responses are needed from democratic governments and civil society. Democracies have been slow to recognise and address digital threats to democracy, while authoritarian adversaries are increasingly adept at weaponising the digital environment. Government policies and societal understanding and appreciation of the challenges have not generally evolved and responded at the speed of technological change. Where government responses have accepted certain risks and demonstrated agility — such as the successful online counter-disinformation election integrity campaign by the Australian Electoral Commission or the Taiwanese approach of harnessing civil society — they have, on the whole, proved successful.

Challenges of disinformation and other forms of mal-information

- A key challenge is the spread of disinformation and other forms of mal-information. While the spread of disinformation and misinformation is not a new phenomenon, the digital environment has allowed for the production and consumption of mis, dis and mal-information at scale. This has had acute impacts on trust and levels of polarisation, which subsequently hampers the ability to engage in agonistic pluralism, let alone reach consensus, in democratic societies. The gamification and commodification of disinformation that is enabled by the digital environment has caused the spread and uptake of disinformation to increase and made its impacts more serious. Disinformation has become so acute that it has at times led to the fracturing of consensus reality (i.e., the Big Lie around the 2020 US presidential elections).

- The success of a disinformation operation is measured by how well it confuses, misdirects or sows doubt within the information environment. Success of a disinformation operation does not necessarily equate to persuasion to a point of view or framing of an issue.

- The Covid pandemic underscored the prevalence and dangers of disinformation and other forms of mal information spread on digital platforms. Covid disinformation has not only impacted the effectiveness of public health responses, it has also contributed to political violence and undermined social cohesion and democratic governance.

- Despite the significant threat posed by the rapid spread of disinformation via online platforms from foreign adversaries, many times, that threat is “coming from inside the house”. Political and partisan actors within democracies are also deploying disinformation campaigns, using similar tactics to those of foreign adversaries in online spaces against partisan opponents. Even combatting disinformation efforts have been weaponised in these partisan battles. This partisan-driven disinformation undermines democracy and is doing our adversaries’ work for them.

- Digital literacy, fact-checking, debunking and prebunking programs to address disinformation play an important role in addressing online disinformation, but there is no way to fact-check our way out of a crisis of truth and trust, nor can governments or individuals rely exclusively on content moderation and removal to address disinformation, extremist and other harmful content online. While these methods can be part of the solution, content moderation, fact checking, digital literacy education and awareness are not enough to address these challenges.

- Too often, the focus is on addressing the veracity of content, but not the sociality or emotion behind it. Humour and emotion are important and underappreciated components of effective communication and should be more effectively harnessed to address disinformation and other forms of mal-information.

- While the “whack-a-mole” approach or reliance on policing online content has been identified as insufficient, other evidence presented at the Dialogue demonstrated that responding swiftly to instances of online disinformation with humour, consistency and directness engenders trust and goes towards building a reputation of forthrightness and accuracy for government agencies. This approach will have the cumulative effect of lessening the impact of digital threats to democracy in future. In other words, consistent reactive action paradoxically has the effect of becoming a preventative approach.

- There continues to be support for undemocratic candidates in electoral democracies. Support for undemocratic candidates is: (1) a function of the lack of support or value placed on democratic principles; (2) based on a sense of the lack of suitable alternatives to vote for; and (3) mis- and disinformation or lack of knowledge that candidates are engaging in undemocratic practices.

- Disinformation and other narratives around election interference and fraud have led to growing distrust in the integrity of elections, highlighted by the 2020 US presidential elections and the Big Lie. This is a particularly damaging trend. Therefore, not only do election operations and procedures have to be impeccably conducted, but the communications strategy around election processes must be robust and proactive in order to pre-emptively guard against election disinformation campaigns. Australia’s compulsory voting system, the integrity of the AEC, the NSWEC and other state electoral commission, and AEC’s past track record of maintaining election integrity and addressing disinformation around election systems and procedures have been particularly important in the Australian context as a protective factor against digital threats to democracy.

Rethinking digital infrastructure for a stronger democracy

- The vast majority of digital infrastructure (assets related to mobile and internet communications or platforms that provide services online and through software applications) is owned by for profit private corporations with insufficient oversight or regulation by the state. This underlying fact has contributed to the digital threats and challenges democracies now face. This should lead states to consider developing and funding more public digital infrastructure. Digital public infrastructure, as defined by head of the Institute for Digital Public Infrastructure Ethan Zuckerman, is comprised of spaces that operate with norms and affordances designed around a set of democratic civic values; public service digital spaces that let us engage in public and civic life.

- To create digital public infrastructure in a way that will benefit or service democracy or contribute to public health, the focus cannot just be on users and content.

It must centre on people — their skills, abilities, training, imagination, knowledge and protocols — as well as the rules, ethics, routines, standards, policies, expectations and norms of the infrastructure.

- Government intervention has been focused on protecting against threats to private information and data, which is critical in safeguarding our ever-eroding privacy in the digital age. However, the same priority should be considered for public information. The public information space is a public good and consideration should be given to how it is safeguarded, in the same way individual private information and privacy is prioritised.

- Big Tech's unfettered business model, which is based on what Harvard professor Shoshanna Zuboff has termed "surveillance capitalism" and the commodification of attention, has created many harms and risks. Examples include polarisation and fragmentation of the public, proliferation of hate speech, the spread of disinformation, as well as the datafication and commodification of the public at scale, their interests, vices and vulnerabilities, all of which can be exploited. In addition to the consideration of digital public infrastructure, the regulation of online advertising, privacy and use of personal data — particularly of children — is critical to addressing these challenges in the future.

Regulation to defend democracy

- Current policy settings deal with the symptoms and effects of tech rather than setting principles and guidelines that determine what capabilities and values digital technologies should have in order to service democratic societies.

- Many democracies are operating under a patchwork system of regulatory frameworks. The regulation architecture that currently exists is for a media and information environment that is decades old and that was developed when the internet was in its infancy. The world is now dealing with challenges that current legislative and regulatory frameworks are ill-equipped to handle.

- The tech industry has traditionally resisted regulation. However, tech exceptionalism in industry regulation has come to an end, especially given the scale on which many digital platforms operate. Mainstream platforms allow actors to reach millions, sometimes billions, of people, therefore more comprehensive regulation is required.

- Tech platforms not only need to assess the risks of their platforms, services and technology, but should proactively incorporate "safety by design" and to take an ethical and human-centric approach to their technology design and capabilities. The only way to make online spaces safer is to "build it in rather than bolt it on".

- Regulation norms should be driven by democratic values and princples in order to mitigate harms in a way that respects human rights, privacy and freedoms of expression and association.

Impacted communities

- Targeting of minority or vulnerable communities and identities — via dehumanisation, hate speech or conspiracy theories — threaten social cohesion and can even be the first signs of more fundamental authoritarian and fascist threats and challenges to democratic societies. The digital environment, by acting as a shield from the direct consequences of interpersonal communication and interaction, has accelerated dehumanising content that targets these communities.

- Free speech absolutism can lead to marginalisation of minorities and vulnerable groups. It can serve to limit speech and silence certain communities. Data shows that it particularly affects women and girls, and ethnic, racial and LGBTQI minorities. Gendered online abuse is a significant issue that shuts down voices and deliberation in the public sphere.

- There is also evidence that women and diverse peoples are being dissuaded from leadership roles due to online abuse. This impacts the ability of all members of a pluralistic democratic society to participate to their full potential.

- The current legal framework for dealing with online harms is comprised of: (1) the Anti-Discrimination Act, which is complaint-driven and puts the burden on individuals to report behaviour, leading to the whack-a-mole approach; (2) various criminal laws, which do not deal sufficiently with borderline behaviour; and (3) various codes of practice, the Online Safety Act and Broadcasting Services Act, all of which only deal with the highest threshold of serious harms.

- Australia has appointed the world's first eSafety Commissioner to keep citizens safe from online harms. The work of the Commissioner is ongoing, evolving and done in consultation with community.

Digitally enabled foreign interference

- Government agencies have assessed the level of malign foreign influence operations (FIO) directed at Australia as extensive and occurring at every level of society. FIO is also a shared challenge across global democracies.

- FIO are often deniable, integrated, incremental, multi-layered and many times enacted in the digital realm. Taken in parts, FIO may be benign or not "that bad", but in aggregate, the result of a multi-layered FIO campaign is cumulatively damaging. Additionally, online information operations and foreign influence operations have become more diffuse and sophisticated as foreign adversaries have adapted their tactics and operations to evade scrutiny.

- Australia has been a global first mover in updating its legislation, policy frameworks and bureaucratic structures to deal with FIO risks by focusing on the most destabilising kind of malign foreign influence — foreign interference. But there is also a "grey zone" of unacceptable foreign influence. "Grey zone" operations deliberately exploit and evade existing legal regimes and response thresholds. As a result, understanding cultural and political norms, and addressing broader economic structures and data protection measures, in addition to introducing screening programs and legislative bans on certain activities, are critically important in countering FIO.

- Not only are there inauthentic accounts and networks (bots) being used for foreign influence and information operations, increasingly, adversarial online information operations are infiltrating authentic activism.

- Cybersecurity is a key concern and cyber intrusions can be a means of foreign interference. But often times, those who exploit the internet are not conducting any ‘hacking’ or intrusion. Rather they are simply using and exploiting the affordances of current digital platforms and infrastructure to conduct foreign interference.

Extremism and other harmful content and behaviours

- There is much online behaviour and content that sits outside what is expressly illegal, but that still leads to significant harm. It is known as “borderline content”. This “awful but lawful” content, discourse and behaviour is dehumanising and damaging to individuals and groups and negatively impacts social cohesion and the health of our democracy.

- The concept of online radicalisation is contested, the process of online radicalisation is not homogeneous or linear and there is a complex interplay between online and offline factors in the radicalisation process.

- Online extremist activity, networking and extremist content consumption do not necessarily lead to offline action. In most cases, being extremist online does not lead to violent action offline. However, research evidence demonstrates that immersion in extremist online communities and engagement with extremist content online can play an important role for violent extremist actors and terrorists.

- Terrorist or extremist violence is not the only harm that is concerning or negatively impacting democracies as a result of online extremist content and ecosystems. A focus on violence obscures broader challenges to social cohesion and democracy as well as the cumulative ill effects that engaging with extremist content and within online extremist communities can have on interpersonal relationships.

- Ideologically motivated and targeted violence remains a critical concern, but the growth of extremist communities online is the more systemic threat to democratic social norms. These communities are increasingly conspiratorial, anti-democratic, transnational, and often justify the use of violence. They also present an opportunity for foreign actors to engage in influence operations and entice the participation of domestic bad faith political actors and elected officials who are not committed to democratic values.

- Online radicalisation is not only occurring on specific platforms. Though some platforms offer more affordances, online radicalisation, recruitment and mobilisation occurs across digital platforms more broadly. Violent extremists use many different online platforms for various operational, recruitment and propaganda purposes. Therefore, the signals of violent extremism expression online can look different depending on the platform.

- There are several challenges in addressing online extremism. They include: the need to balance privacy and human rights with content moderation and deplatforming; the lack of a consistent definition of terrorism that can be agreed upon by platforms and governments; determining the link between online and offline violent extremism; and the need to understand the role of algorithms in radicalisation and amplification of extremist content, which is currently incomplete as tech platforms are unwilling to “open the black box”. However, there are more opportunities for intervention and prevention earlier in the process of observed radicalisation and engagement with online extremist content.

- Mainstream tech platforms, such as those belonging to the Global Internet Forum to Counter Terrorism (GIFCT), are taking steps to counter disinformation, violent extremist content and hateful and harassing content, and have developed incident response protocols. However, even though these companies have a large portion of the market share, they do not represent the entirety of the online ecosystem and there are a number of other platforms (Telegram, chans, etc.) where dangerous content thrives that are not enacting similar measures.

For future consideration

In the process of robust discussion and dialogue, the DTD Dialogue generated a number of recommendations from participants. Below is a summary of those recommendations for consideration. These ideas for future consideration should not be taken as endorsed or agreed upon by all Dialogue participants.

On addressing disinformation and mal-information

- Disinformation or conspiratorial narratives spread online are often a hodgepodge of disjointed, even contradictory claims. These narratives do not need to make sense to their believers, rather individuals engage in disinformation and conspiracy theories to fulfill other psychosocial needs and to participate, coalesce and cohere around communities and social movements. Therefore, in order to address disinformation, actions beyond mere fact-checking and debunking campaigns must be used to counter damaging disinformation and conspiracy theories. Instead, governments and civil society actors must address the sociality of disinformation and conspiracy beliefs rather than their veracity.

- Government needs to communicate proactively, clearly and consistently with the public about its countering disinformation efforts. Democratic citizens are within their rights to question government efforts to influence or regulate discourse and behaviour. Therefore, governments need to clearly communicate why and when such actions are taken.

- It is also important to establish a threshold for when disinformation targeting government agencies or programs requires a response from government. Not all low-level disinformation will require a response — sometimes a response will only serve to amplify the disinformation. But when it does reach that identified threshold, governments should ensure that there is an agile and efficient response in place.

- Be prepared and be proactive. Government agencies and officials need to plan and have strategies ready for online malign foreign influence and disinformation campaigns targeting government and institutions. Government agencies and responsible civil society actors should project domain expertise so that the void is not filled by disinformation or other forms of mal-information.

- Prebunking has been shown to work more effectively than debunking mis- and disinformation narratives and campaigns. The way that social media platforms are currently designed gives advantage to first movers, so prebunking or information inoculation can be more effective in addressing the harms of disinformation and other forms of mal-information.

- There needs to be a greater focus on building citizen resilience to disinformation and other online harms rather than relying primarily on content moderation and counter-disinformation campaigns.

- It is important to go where the people are — fact sheets on government websites are insufficient as often people may not go to official government agency websites as the first port of call to obtain information. Government communications campaigns need to incorporate concurrent opportunities to engage on social media and legacy media, and via both online and offline local community organisations and hubs.

- Creating disinformation registers can highlight and help debunk disinformation campaigns and narratives. Disinformation registers can also serve as important resources for researchers and analysts.

- Public interest journalism is an effective antidote to disinformation and other forms of mal-information. Providing more awareness and training for journalists can be an effective means of countering the spread and harmful effects of disinformation. It is also important to provide awareness for journalists on how legacy and mainstream media can inadvertently spread and amplify disinformation and other harmful content.

- Unfortunately, the more the issue of disinformation is raised, the more distrust is potentially engendered among the public around official sources of information and mainstream news. One suggested work-around is to encourage the active consumption of information (i.e. asking who is writing it and who is funding it.)

On safeguarding democratic institutions and values

- Generalised civics education can play an important role in addressing these intersecting challenges to democracy. Educating the public on the functioning of parliamentary democracy, levels of government, the functioning of bureaucracies, elections and representation may help buffer disinformation around political power and authorities.

- Government should back and defend public-facing civil servants and public institutions, proactively safeguarding their reputation and integrity instead of reactively responding to crises or attacks.

- Government agencies should build their reputation for the long term by building a track record of engagement and trust with the public. This will lend greater credibility to government communications when officials or agencies need to respond to a major event or crisis or to counter disinformation. They must be continuously engaging in the information space rather than reacting when issues arise.

- It is possible to reduce support for undemocratic candidates and reduce polarisation using short and scalable online interventions, but there is no one-size-fits-all approach and different causes require different interventions. The most successful online interventions have involved reducing tolerance for undemocratic practices and strengthening support for democratic principles. Other successful interventions have focused on reducing or correcting anti-democratic misperceptions of political opponents. Further successful online interventions included those aimed at decreasing dislike for political opponents and addressing bias evaluation of politicised facts through the cultivation of joint or uniform identity among the citizenry.

- Harnessing and encouraging the power of civil society is a key approach that should be utilised more often by democratic governments and societies. Civil society organisations (CSOs) that address digital challenges to democracy are able to keep an appropriate distance from government, which helps their credibility and creates organic synergies. Working with CSOs can also assist government agencies in outreach efforts. However, these efforts are resource-intensive and often underfunded. Government can play a role by funding or working in coordination with these CSO efforts.

- Governments are well versed in citizen consultation and engagement. However there should be consideration for governments to actively pursue further opportunities for shared decision making. This can include considering deliberative democracy and participatory democracy models as a method of engendering trust and engagement with democracy.

On addressing digitally enabled foreign interference

- The country agnostic approach to public discussion and government strategies hampers a risk management-based approach to addressing FIO by non-government actors. Consideration should be given to adjusting this country agnostic approach in favour of identifying the countries from which FIO are coming from in order to more efficiently and appropriately allocate resources to manage the associated risks.

- Countering foreign interference (CFI) strategies must also manage social cohesion risks as more forward leaning CFI approaches could result in perverse outcomes for impacted communities.

- Investment should be made in community-level understanding to help address the challenge of FIO. Public engagement, public education and empowering decentralised responses are important ways to counter FIO. A risk mitigation rather than risk elimination approach that incorporates these greater public engagements would harness the strengths of democratic societies and structures.

- Government should consider a national public facing counter-foreign interference strategy, just as government has done with its national counterterrorism strategy. There are well-established cross-jurisdictional structures to deal with other national security threats, such as terrorism, and they could be similarly applied to addressing malign FIO and foreign interference.

Considering more robust regulation and public infrastructure

- The following principles could effectively guide Big Tech regulation: (1) expand regulation to include mitigation of risks from platform systems and processes; (2) expand regulation to include addressing risks and harms to community and society in addition to risks and harms to individuals; (3) ensure platform accountability and transparency rather than the current setting, which places the burden of responsibility on individual actors; (4) work towards comprehensive regulation that addresses gaps in the regulatory framework; (5) move away from self-regulation, self-reporting, voluntary transparency reporting and voluntary codes of conduct and instead move towards co-regulation and/or enforced/mandated regulation; and (6) resource and join up government regulators.

- Government could consider potential pathways for developing and funding more public digital infrastructure. Much in the same way there is publicly funded broadcasters, publicly funded public service digital spaces could potentially help mitigate the digital threats to democracy examined in this dialogue.

- Independent civil society and/or academic research audits of social media platforms can serve an important function to address platform risks and digital threats to democracy.

- Mainstream social media platforms maintain that they are not publishers and are therefore not liable for content on their platforms, claiming that it is the individual users who post content that are individually liable. This removes the onus of responsibility from digital platforms. One potential approach would be to introduce a duty of care provision for digital platforms to reduce harms and threats to democracy.

- Extremism will always be a contested concept, whereas dehumanisation is a more easily defined and understood one. Addressing harmful online content and behaviour through this dehumanisation lens would be one way to disrupt the challenges and limitations of programs and policies that aim to combat extremism. Using the dehumanisation rather than extremism paradigm could also allow for more pre-emptive rather than reactive responses and address these harms in a way that increases and maintains social cohesion.

- Working across international jurisdictions and likeminded democracies is critical as most digital platforms in use today are multinational private companies headquartered outside Australia. Domestic efforts need to be supplemented and linked to international efforts among likeminded democracies.

Disclaimer: This summary report does not represent the views of the Lowy Institute or the NSW Department of Premier and Cabinet.

The Digital Threats to Democracy Project is supported by the New South Wales Department of Premier and Cabinet. The information, advice and/or views expressed in this project are those of the project author/s and participant/s and do not necessarily reflect the views of the Lowy Institute or the NSW government.

LOWY
INSTITUTE

DIGITAL THREATS TO DEMOCRACY DIALOGUE

Dialogue Summary Report

LOWY
INSTITUTE