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. Also attached is the full Dialogue program, which features the schedule, panel descriptions, discussion questions for consideration, participant biographies and presentation abstracts.

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. (For a fuller description of the panels and discussion questions for consideration by the Dialogue participants, please refer to the attached Dialogue program.)

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 pubic 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.

DIGITAL THREATS TO DEMOCRACY DIALOGUE

Dialogue Summary Report

LOWY INSTITUTE

DIGITAL THREATS TO DEMOCRACY DIALOGUE

Wednesday 12 October 2022

LOWY INSTITUTE

Welcome

I am delighted to welcome you to the Digital Threats to Democracy Dialogue hosted by the Lowy Institute.

The digital environment and digital communications technologies have undoubtedly brought benefits and advantages to the way we work, live and communicate. However, along with these benefits have come a myriad of challenges.

Once believed to hold the key to the expansion of global democracy, liberalism and a healthy civil society, the internet and digital technologies are now more often framed as threats to advanced and emerging democracies alike.

The Digital Threats to Democracy Dialogue aims to identify and examine the intersecting digital threats to democracy, specifically across four key issues: online disinformation, online hate and extremism, tech-enabled foreign interference and regulation of the digital sphere.

As societies grow more dependent on digital technology, we need to better understand these challenges and identify how our current digital infrastructure has the potential to undermine democratic governance.

This Dialogue brings together a distinguished and expert group of participants to examine and address the intersecting digital challenges to democracy.

The ambition of this Dialogue is to foster connections across subject matter and policy areas that will spark new ideas and approaches to meet these digital challenges to democracy.

Thank you for dedicating your time and efforts today.

In addition, I would like to acknowledge the funding from the New South Wales Department of Premier and Cabinet that has made this Dialogue possible.

Best wishes,

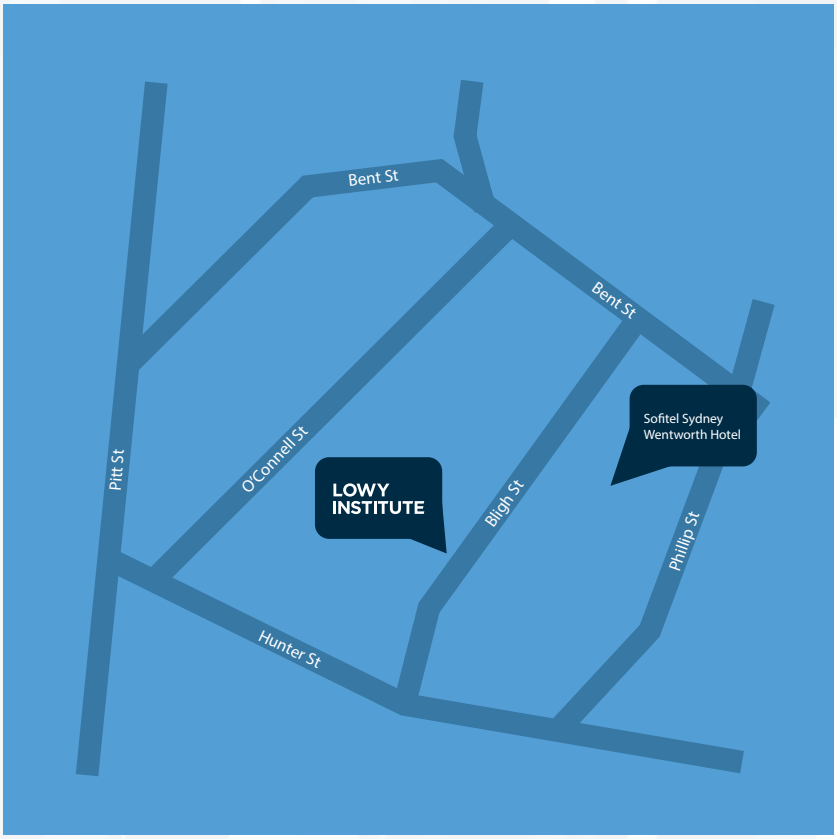
Lydia Khalil
Research Fellow, Transnational Challenges
Manager, Digital Threats to Democracy Project
Lowy Institute

INFORMATION

Date: Wednesday 12 October 2022
Time: 9:00am to 5:00pm
Reception drinks to follow

Location: Lowy Institute
31 Bligh Street
Sydney NSW

Map:



Participant arrival and registration starts at 8:40am. Please ensure your timely arrival as the Dialogue will commence promptly at 9:00am.

This Dialogue will be an off-the-record discussion to better facilitate frank and open conversation.

Should you need to contact the Institute about any logistics or need further information, please contact Lydia Khalil +61 457 358 187 or email lkhalil@lowyinstitute.org.

For technical assistance prior to or during the Dialogue please contact Josh Goding +61 405 127 433 or email jgoding@lowyinstitute.org.

AGENDA

0840 – 0900	**PARTICIPANT ARRIVAL AND REGISTRATION**
0900 – 0910	**WELCOME** **Michael Fullilove**, Executive Director, Lowy Institute **Michael Coutts-Trotter**, Secretary, NSW Department of Premier and Cabinet (DPC) **Lydia Khalil**, Research Fellow, Project Director, Lowy Institute
0910 – 1000	**OPENING KEYNOTE:** **HOW TO (REALLY) LOSE THE INFORMATION WAR** **Nina Jankowicz**, Vice President, Centre for Information Resilience Delegate response (Lydia Khalil) Q&A
1000 – 1100	**PANEL 1: TACKLING ONLINE DISINFORMATION** **Jeff Pope**, Deputy Electoral Commissioner, Australian Electoral Commission (AEC) **Jan Gerrit Voelkel**, doctoral candidate, Polarization and Social Change Lab, Stanford University **Tim Niven**, Research Lead, Doublethink Lab
1100 – 1120	**MORNING TEA BREAK**
1120 – 1220	**PANEL 2: UNDERSTANDING AND ADDRESSING ONLINE EXTREMISM** **Julian Droogan**, Associate Professor, Macquarie University **David Shanks**, Former Chief Censor, New Zealand Government **Erin Saltman**, acting Executive Director, Global Internet Forum to Counter Terrorism (GIFCT)
1220 – 1300	**LUNCH**

AGENDA

1300 – 1400	**PANEL 3: FOREIGN INTERFERENCE IN THE DIGITAL REALM** **Katherine Mansted**, Director of Cyber Intelligence, CyberCX **Anthony Coles**, First Assistant Secretary, Counter Foreign Interference Coordination Centre, Department of Home Affairs **Jennifer Hunt**, Lecturer, Macquarie University
1400 – 1420	**AFTERNOON TEA BREAK**
1420 – 1500	**AFTERNOON KEYNOTE:** **RETHINKING DIGITAL PUBLIC INFRASTRUCTURE** **Joan Donovan**, Research Director, Shorenstein Center on Media, Politics and Public Policy, Harvard University Delegate response (Jordan Guiao) Q&A
1500 – 1600	**PANEL 4: REGULATION AND TRANSPARENCY** **Julie Inman Grant**, Australia's esafety Commissioner **Chris Cooper**, Executive Director, Reset Australia **Malcolm Crompton**, Founder and Lead Privacy Advisor, Information Integrity Solutions Pty Ltd
1600 – 1700	**PANEL 5: DIGITAL CITIZENSHIP AND IMPACTED COMMUNITIES** **Jennifer Hsu**, Research Fellow, Lowy Institute **Rita Jabri Markwell**, Advisor, Australian Muslim Advocacy Network (AMAN) **Darren Bark**, CEO, NSW Jewish Board of Deputies
	CLOSE
	DRINKS RECEPTION

PANELS & DISCUSSION QUESTIONS

PANEL 1
TACKLING ONLINE DISINFORMATION

Jeff Pope, Australian Electoral Commission (AEC); Jan Gerrit Voelkel, Polarization and Social Change Lab, Stanford University; Tim Niven, Doublethink Lab

Disinformation is false, inaccurate or misleading information intentionally designed and promoted to cause public harm. Whistleblowers, independent researchers and leaked internal research from digital platforms themselves have shown that the algorithms, design logic and reliance on the attention economy have led to the rapid spread and consumption of disinformation. Disinformation impacts citizens' ability to access accurate information needed for deliberation and decision making in democracies. Disinformation is reducing trust in democratic governance and each other, increasing polarisation, corrupting our information ecosystems and even our consensus reality.

Questions:

- What are the affordances and logics of digital platforms that can lead to the spread and consumption of disinformation?
- How does disinformation undermine trust in democratic institutions?
- Is there particular risk around elections?
- What is the connection between the spread and consumption of disinformation online and greater societal polarisation and how does this impact democracy?
- Is there anything to be done to stop disinformation from proliferating on digital platforms? Should government policy focus be on enacting policies to mitigate the spread of disinformation online or on countering disinformation online and its effects?
- What are the elements of a successful countering disinformation program or policy?

PANELS & DISCUSSION QUESTIONS

PANEL 2
UNDERSTANDING AND ADDRESSING ONLINE EXTREMISM

Julian Droogan, Macquarie University; Paul Ash, Christchurch Call;
Erin Saltman, Global Internet Forum to Counter Terrorism (GIFCT)

Extremist actors have been some of the earliest adopters of the internet, recognising its potential as a communications and mobilisation tool. We have been grappling with the role of technology in extremism for some time, but particularly since the advent of social media and the ubiquitous use of the internet, which has led to the spread of, and exposure to, extremist content and the emergence of online extremist subcultures. Technology has played a significant role in the increase of extremism – from allowing the spread of extremist propaganda, to assisting in recruitment, mobilisation and financing. Indeed, a growing body of evidence demonstrates that internet technology can be an important factor in facilitating extremism. At the same time, there is an acknowledgement that we need to dig deeper into what that means for such a broad conclusion to make any kind of sense. Internet technology, while not necessarily causing violent extremism, can have multiple and various roles in facilitating radicalisation and mobilisation to violent extremism.

Questions:

- What role does the internet play in violent extremism? Is there such a thing as "online radicalisation"? What do we mean when we use that term?
- Does the digital environment play a unique role in the process of radicalisation and mobilisation to violent extremism?
- Is content moderation an effective or sufficient mechanism to counter the expression of violent extremism online?
- What else should we consider besides content moderation to counter online violent extremism?
- How does online extremism lead to real world harm?

PANELS & DISCUSSION QUESTIONS

PANEL 3
FOREIGN INTERFERENCE IN THE DIGITAL REALM

Katherine Mansted, CyberCX; Anthony Coles, Department of Home Affairs; Jennifer Hunt, Macquarie University

The digital environment has provided more opportunities for malign foreign interference. Foreign actors are exploiting the digital infrastructure — particularly social media — to conduct information warfare. The privately held, relatively free and open digital platforms used in democracies are particularly susceptible to tech-enabled foreign interference.

Through digitally enabled information warfare operations, elections interference, deep fakes and various other means of undermining democratic political processes and institutions, foreign actors are violating national sovereignty. Democracies, in responding to this challenge, must also respond proportionately and according to democratic principles.

Questions:

- What are the ways foreign interference manifests in the digital environment?
- How are digitally enabled disinformation, extremism and foreign interference linked?
- Are there more comprehensive policy responses we should consider to address these interrelated digital challenges to democracy?
- How does digitally enabled foreign interference undermine democracy? Is it more of a challenge than other types of foreign interference?
- Is there greater risk of digitally enabled foreign interference on or from platforms of competitor nation states or is the risk platform neutral? Do some platforms pose more of a risk than others? If so, why?

PANELS & DISCUSSION QUESTIONS

PANEL 4
REGULATION AND TRANSPARENCY

Julie Inman Grant, Australia's esafety Commissioner; Chris Cooper, Reset Australia; Malcolm Crompton, Information Integrity Solutions (IIS)

After many years of a laissez-faire approach to the tech sector, there are increasingly louder calls for tighter regulation – and government have responded. There are a myriad of new regulations and anti-trust legislation across jurisdictions aimed at harnessing tech platforms. But there are a number of competing goals that regulation seeks to address — such as competition, privacy, security, and protection of rights and regulations, which have been enacted, sometimes, at cross purposes. 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.

Questions:

- How has insufficient regulation of digital platforms undermined democracy?
- Will greater regulation of digital platforms hamper competition? Or has lack of regulation created digital oligopoly?
- What are the tensions between safety regulations and concerns about privacy and freedom of expression and how can we best balance these competing priorities? Have efforts to regulate safety online impacted other democratic principles?
- What does transparency from digital platforms look like? What are we hoping to achieve by gaining a greater understanding of how digital platforms are run and function?
- How can we effectively regulate digital platforms and companies from headquartered or founded foreign jurisdictions and/or competitor nation states?

PANELS & DISCUSSION QUESTIONS

PANEL 5
DIGITAL CITIZENSHIP AND IMPACTED COMMUNITIES

Jennifer Hsu, Lowy Institute; Rita Jabri Markwell, Australian Muslim Advocacy Network (AMAN); Darren Bark, CEO, NSW Jewish Board of Deputies

In multicultural democracies and pluralistic societies, certain communities are targeted as a means to undermine democratic institutions and social cohesion. But civil society and individual citizens have found ways to harness the digital environment to better engage in deliberation, dialogue and address polarisation and other digital challenges. Through digital citizenship, people can better engage with each other and hold governments and tech companies to account.

Questions:

- How have communities that have been impacted by online harms mobilised to address these challenges? How can government support these efforts?
- How have citizens effectively used and harnessed digital platforms to engage in the democratic process?
- How has the digital environment impacted the way citizens relate to one another in a deliberative, participatory democracy?
- Are there lessons to be learned from impacted communities that can be used to address the effects and impacts of the digital environment writ large?
- How has the digital environment effected the concept and expression of citizenship in a deliberative, participatory democracy?

PRESENTATION ABSTRACTS

OPENING KEYNOTE:

How to (Really) Lose the Information War, Nina Jankowicz, Vice President, Centre for Information Resilience

In 2020, Nina Jankowicz published a book examining how targets of Russian disinformation attempted to counter the Kremlin's lies, often floundering along the way. In 2022, the Biden administration tapped her to lead the Disinformation Governance Board — an intra-departmental coordinating body at the Department of Homeland Security. Within hours of the announcement of the Board, partisan domestic disinformation actors labelled it a "Ministry of Truth", falsely claimed it would censor the American people, and directed lies, hate, harassment, and threats, towards Jankowicz. Rather than defend the effort and its director, or even communicate about its plans, the Department left an information vacuum that buoyed the lies and ultimately led the administration to scrap its plans for the Board. Weaving together her experience in US government as well as her extensive research across Central and Eastern Europe, Jankowicz will offer ideas and best practices for efforts to counter disinformation both within and outside of government structures, as well as predictions for the future of the problem.

PANEL 1: TACKLING ONLINE DISINFORMATION

Learning from the AEC Success Story, Jeff Pope, Deputy Electoral Commissioner, Australian Electoral Commission (AEC)

The AEC represented global best practice for electoral management in its approach to mis- and disinformation during the 2022 federal election. The development of an innovative Reputation Management Strategy, the cutting-edge use of all forms of social media including assertive handling of false information, the development of a published "disinformation register", and the use of the Electoral Integrity Assurance Task Force, were unique elements of the AEC's approach. Developing this approach required deep knowledge of the communication ecosystems surrounding elections more broadly, and the ability to engage with high levels of risk.

Crowd Sourcing Solutions: The Strengthening Democracy Project, Jan Gerrit Voelkel, Doctoral Candidate, Polarization and Social Change Lab, Stanford University

Deep partisan conflict in the mass public threatens the stability of democracy. We conducted a megastudy on a national sample of American partisans (n = 32,059) testing 25 interventions designed to reduce anti-democratic attitudes and partisan animosity selected from a pool of 252 interventions submitted by social scientists, practitioners, and activists as part of the Strengthening Democracy Challenge. Contrary to the pessimistic expectations of expert forecasters, we find that nearly every selected intervention (23 out of 25) significantly reduced partisan animosity as well as reduced support for undemocratic practices and partisan violence. These findings highlight the effectiveness of crowdsourcing solutions and providing a toolkit of promising interventions for practitioners.

PRESENTATION ABSTRACTS

Lessons from Taiwan, Tim Niven, Research Lead, Doublethink Lab

Doublethink Lab is one of a number of civil society organisations addressing PRC information warfare attacking Taiwan's democracy. Taiwan's approach to confronting this threat relies heavily on civil society, which we will argue is a strength. This presentation will give an overview of Taiwan's political and information environment context and share what DTL has learned about PRC information warfare targeting Taiwan, including goals and methods. DTL will also share the assumptions underlying their approach to confronting these threats, and relevant findings from their (and others') research. Although the Taiwanese and Australian contexts are indeed very different, we hope to be able to draw some general insights that will be of benefit to Australia.

PANEL 2: UNDERSTANDING AND ADDRESSING ONLINE EXTREMISM

What Do We Know About Online Radicalisation, Julian Droogan, Associate Professor of Terrorism Studies and Director of Research and Innovation at the Department of Security Studies and Criminology, Macquarie University

Internet-based propaganda operations by violent extremists have led to widespread concern about online radicalisation to violence, particularly among Australian youth. However, processes of online radicalisation are neither simple nor well understood, and the threats posed to national security by online extremists go beyond concerns about "vulnerable youth". This presentation will look at what we know about processes of online radicalisation in Australia. Drawing upon new research, it will discuss what young Australians report about their experiences of online terrorist materials and how they navigate these dangerous spaces. It will then look at parallel research demonstrating the wider challenges to liberal democracy and social cohesion presented by online ecosystems of hate that spread conspiratorial narratives and extremist disinformation.

Progressing the Christchurch Call to Action, Paul Ash, New Zealand Prime Minister's Special Representative on Cyber and Digital, Christchurch Call and Cyber Coordinator

The Prime Minister of New Zealand and President of France hosted the fourth Christchurch Call Leaders' Summit on 20 September 2022 in New York. At this multistakeholder event, leaders reflected on progress delivering the 24 Call commitments to eliminate terrorist and violent extremist content online, and discussed next steps. This presentation will provide an overview of the Call and outline the priorities for action. Some reflect lessons learned from the May 2022 terrorist attack in Buffalo, New York and focus on addressing the proliferation of content on small platforms and unmoderated or "alt-tech" platforms, day-to-day and during crises. Another area of focus is prevention, where work is underway on overcoming well-known obstacles to independent research on algorithms and the role they might play in radicalisation. This is a critical step towards designing effective interventions. There is also a need to understand and address risks to children and young people, including in the context of new technologies, and how terrorist and violent extremism intersects with online hate and harassment against women and LGBTQI+ people, and real-world harm.

PRESENTATION ABSTRACTS

Beyond Content Moderation, Erin Saltman, acting Executive Director, Global Internet Forum to Counter Terrorism (GIFCT)

Counter-extremism and counter-terrorism efforts online have evolved dramatically in the last ten years. Dr Erin Saltman will discuss some of the ways in which the field has moved beyond content takedowns as the primary means to challenge the threat, and review recent outputs by the GIFCT Working Group on Positive Interventions and Strategic Communication. This includes both the ability of tech companies to take more nuanced actions on content, such as downranking and demonetising, as well as more innovative ways to deploy counterspeech or alternative narrative campaigns online. While advancement is noted, these efforts must constantly evolve due to platform diversification, adversarial shifts aimed at avoiding detection, and regional variations in violent extremism and terrorism.

PANEL 3: FOREIGN INTERFERENCE IN THE DIGITAL REALM

Keeping Up with an Evolving Threat Landscape, Katherine Mansted, Director of Cyber Intelligence, CyberCX

Australia has been a world-leader in adapting its policy settings to confront foreign interference, especially since 2017. But this is a challenge that evolves quicky, as geopolitics, technology and society change. What does Australia need to do to keep pace? This presentation will present some policy options and considerations for addressing digitally enabled foreign interference into the future.

Understanding and Addressing Foreign Interference in Australia, Anthony Coles, Deputy Counter Foreign Interference Coordinator, Department of Home Affairs

The presentation will address the evolution of the foreign interference threat environment in Australia, the implications for critical infrastructure and technology, and social cohesion, and key aspects of the Commonwealth response. Key issues covered will be: the role and implications of approaches based of partnership between government and the private sector, cooperation between Commonwealth, State and Territory governments and an outline of Commonwealth priorities.

Fighting Disinformation: Taking Lessons From Cyber Conflict, Jennifer Hunt, Lecturer, Macquarie University

Cyber-enabled disinformation, a campaign of carefully constructed false messages distributed through an adversary's information ecosystem in order to deceive the decision-making elite or the public, is best understood as a form of information warfare. This talk identifies the techniques of modern information warfare and the core attributes of these campaigns across disparate topics and targets. It offers a comparative analysis of cyber

PRESENTATION ABSTRACTS

conflict and information warfare to locate potential defensive measures. Throughout, the second and third order consequences of information warfare for democracy are examined, with lessons learned from recent case studies. What have recent campaigns taught us about the conduct and defence against information operations? How is success measured in information warfare? What are the second and third order impacts for democracy?

AFTERNOON KEYNOTE:

Rethinking Digital Public Infrastructure, Joan Donovan, Research Director, Shorenstein Center on Media, Politics and Public Policy, Harvard University

For the last decade, the internet has slowly become the critical public infrastructure across the globe. How has that transformation created a wellspring of new opportunities and unforeseen dangers? Particularly, broad public debate over defining these threats and reforming technology has lead to many different laws globally, but does not seem to have broadly addressed the fundamental issues embedded in the design of social media.

PANEL 4: REGULATION AND TRANSPARENCY

The Power of Three Ps in Shaping a New Online World Order, Julie Inman Grant, Australia's esafety Commissioner

Regulating user safety in a rapidly devolving and expanding online world is an increasingly vexed question. The eSafety Commissioner is the world's first government regulator with functions to keep people safe online. New powers under the Online Safety Act mean eSafety can hold big tech to account when it comes to the most serious of online harms. But even with these world-first powers, enforcement can be a piecemeal exercise when it comes to locating and removing the most harmful online material, such as pro-terror content. So, how is eSafety changing the rules of the game? A combination of Prevention, Protection, and Proactive and Systemic Change.

Future Citizens: Protecting Young People from Digital Harms, Chris Cooper, Executive Director, Reset Australia

Young people tend to be more susceptible to the addictive design features of technology, are exposed to targeted advertising by harmful industries, and are having their perspectives and values shaped by unchecked algorithms and echo chambers — often leading to distrust in authority and institutions. These harms pose an immediate threat to their individual wellbeing and resilience, as well as their participation and trust in our democracy. Without adequate controls and appropriate consent measures in place, a lack of regulatory action risks exposing them to far greater harms that could impact their life outcomes in numerous ways. Passing new regulation to protect young people is an opportunity to address some of the most significant harms facing our future citizenry, while also establishing new norms to shape the national conversation for the kind of privacy and control of personal data that all Australians should enjoy. This presentation will provide an overview of Reset's work in this

area, its relevance for our democracy, as well as some of the solutions that are already being considered and legislated in other jurisdictions.

The Importance of Privacy in Democracy, Malcolm Crompton, Founder and Lead Privacy Advisor at Information Integrity Solutions Pty Ltd

Ensuring each individual has the private space to freely read, think and debate the world around them is fundamental to democracy. Privacy is more nuanced than just "the right to be left alone". More usefully, the privacy of personal information can be conceived as "the controlled sharing of personal information". The "attention economy", "social media", "surveillance capitalism", "fake news" and "dark patterns" are just some of the digital means used to abuse our privacy and manipulate democracy. Yet in Australia, we have treated personal information as a third order issue. We must treat personal information as the extremely valuable commodity that it is: in the law and the enforcement of that law.

PANEL 5: DIGITAL CITIZENSHIP AND IMPACTED COMMUNITIES

WeChat — Challenge or Facilitator of Democracy?, Jennifer Hsu, Research Fellow, Lowy Institute

For Australians with ethnic Chinese heritage, WeChat is a dominant source of news and information, and an important communication tool. Owned by a Chinese company that is subject to Chinese intelligence and national security laws, WeChat challenges Australia's national security. However, the broader Australian public discussion ignores how WeChat is used and the extent to which such platforms may facilitate social engagement and civic participation for newly arrived migrants. This presentation will provide a deeper dive into the data collected by the Lowy Institute's *Being Chinese in Australia* survey of the past two years by focusing on Chinese-Australians across demographics and their WeChat use, engagement with news and politics and perceptions about life in Australia. Qualitative data drawn from focus groups will contextualise these findings.

Countering Online Dehumanisation, Rita Jabri Markwell, Advisor, Australian Muslim Advocacy Network (AMAN)

Awareness continues to increase about the harms of "borderline" content that sits between hate speech, disinformation and terrorist content. Consensus on how to address these harms, however, is much harder to achieve. Dehumanisation of group identities is a common tactic used by ISIS, racist nationalists and other actors. Not only is it a tactic to mobilise and radicalise to the point of violence, but a form of psychological violence. Dehumanising speech and discourse (including conspiracy theory) is published and disseminated online, explicitly and through the curation of information overtime. Having tested Australian laws and engaged widely with platforms, law enforcement and regulators to solve this problem, this presentation will speak to challenges to be considered in designing public policy and laws to disrupt dehumanisation.

PRESENTATION ABSTRACTS

Addressing Confirmation Bias Online to Bolster Democratic Reslience, Darren Bark, CEO, NSW Jewish Board of Deputies

Through confirmation bias, we adopt the tendency to process information by seeking (either consciously or unconsciously through AI and algorithms), and interpreting, information that is consistent with our existing views and beliefs. What is the outcome for a society that unknowingly consumes only the news, social media and information that suits our political, religious, or social inclination from our inception of using digital platforms? Confirmation bias is a principal element utilised in supporting the dissemination of false narratives, dis- and misinformation through digital and online platforms. It is important that we understand the underlying social mechanisms and dynamics in order to understand the proliferation and effects of online disinformation towards online hate and extremism. Today we are facing unprecedented levels of change, uncertainty, and doubt. The less accurate and credible the information we have, and the less confidence we have in it, the more likely we'll rely on confirmation bias to fill in the blanks, thus reducing our effectiveness, our interpretation, our resolve — and thus diminishing our resilience, and our ability to be educated and empowered to counter bigotry and hate through respect and understanding.

Darren Bark
CEO, NSW Jewish Board of Deputies

Darren Bark is the CEO of the NSW Jewish Board of Deputies and Deputy Chairman of the Biometrics Institute. In his role as CEO, Darren advocates on behalf of the NSW Jewish community. Darren worked for the NSW Government for over 10 years, including as Executive Director of the NSW Police Force, Director at the NSW Department of Justice and Chair of the NSW Identity Security Council. Darren was also Chief of Staff to NSW Government Ministers and Deputy Chief of Staff and Policy Director to the Deputy Premier. Prior to Government, Darren was an IT consultant and lawyer. He also developed Cyber Bullying Workshops, Cybersafety Solutions and Educational Resource for young people, parents and teachers.

Creina Chapman
Deputy Chair, Australian Communications and Media Authority

The ACMA is an independent Commonwealth statutory authority which regulates communications and media services. The ACMA oversees the 2021 Australian Code of Practice on Disinformation and Misinformation and administers elements of the News Media Bargaining Code. Creina Chapman has held a number of senior executive and strategic adviser roles at commercial media companies; Southern Cross Austereo, News Corp, Publishing & Broadcasting Limited and the Nine Network. Her experience in the media and communications sector is gained from organisations spanning television, radio, print, mobile services, podcasting and online services which serve metropolitan, regional and remote Australian markets. Creina has also been a senior policy adviser to a number of Federal members of Parliament.

Anthony Coles
First Assistant Secretary, Counter Foreign Interference Coordination Centre, Department of Home Affairs

Anthony Coles is the First Assistant Secretary, Counter Foreign Interference Coordination Centre, Department of Home Affairs. Before taking up this role, between early 2018 and mid-2021 Anthony held senior leadership positions in the Department of Home Affairs with responsibility for policy and legislation relating to law enforcement, transnational crime, and intelligence powers. Prior to joining the Department of Home Affairs, Anthony spent 15 years in the Commonwealth Attorney-General's Department in a range of roles focused on serious and organised crime and national security policy. During that time he was Australia's Head of Delegation to the Financial Action Task Force, and the OECD Working Group on Bribery. He holds a Bachelor of Arts (Hons) and Bachelor of Laws (Hons) from the Australian National University.

Chris Cooper
Executive Director, Reset Australia

Chris Cooper is the Executive Director of Reset Australia, a policy think tank and advocacy organisation working to counter digital threats to democracy, specifically the harms caused by unregulated big tech. Chris has over 15 years experience working at the intersection of strategic communications, advocacy and digital media to leverage culture and storytelling to shape policy, behaviour and systems on a range of social issues areas across the globe. Chris is also Senior Campaigns Director at the global social impact agency, Purpose.

Michael Coutts-Trotter
Secretary, NSW Department of Premier and Cabinet

Michael Coutts-Trotter was first appointed to head a NSW Government department in 2004 and has since led six agencies. He is now the Secretary of the NSW Department of Premier and Cabinet. Before joining the public service, Michael was chief of staff to a NSW Treasurer for seven years. Michael is a fellow of the Institute of Public Administration of Australia.

Malcolm Crompton
Founder and Lead Privacy Advisor, Information Integrity Solutions Pty Ltd

Malcolm Crompton AM is Founder and Lead Privacy Advisor at Information Integrity Solutions Pty Ltd, iispartners.com. Malcolm was Australia's Privacy Commissioner from 1999 to 2004 and led implementation of the nation's first broad based private sector privacy law. He has sat on advisory bodies around the world, including the European Union, OECD, APEC and large global companies.
He is a member of the New South Wales Information and Privacy Advisory Committee and the NSW Digital Identity Ministerial Advisory Council.

Joan Donovan
Research Director, Shorenstein Center on Media, Politics and Public Policy, Harvard University

Dr Joan Donovan is a leading public scholar of disinformation. She is the Research Director of the Harvard Kennedy School's Shorenstein Center on Media, Politics and Public Policy and the Director of the Technology and Social Change project (TaSC). TaSC conducts research, develops methods, and facilitates workshops for journalists, policymakers, technologists, and civil society organisations on how to detect, document, and debunk media manipulation campaigns. She is also co-founder of Harvard Kennedy School's Misinformation Review. Dr Donovan has laid out the conceptual framework for understanding disinformation and coined many of the terms that the disinformation research field and mainstream media use to understand technology's impact on society. Dr Donovan is the co-creator of the beaver emoji.

Julian Droogan
Associate Professor, Macquarie University

Dr. Julian Droogan is Associate Professor of Terrorism Studies and Director of Research and Innovation at the Department of Security Studies and Criminology, Macquarie University. He is also Editor of the *Journal of Policing, Intelligence and Counter Terrorism*. Julian has been chief investigator on numerous funded research grants. Topics include investigating how young people engage with online violent extremist content; examinations of online right-wing extremist and conspiratorial communities across multiple social media platforms; online jihadist propaganda; and evaluating countering violent extremism programs. He maintains a number of international agreements and partnerships with academic and practitioner counter-terrorism and countering violent extremism organisations in Europe, the Middle East, and South Asia.

Michael Fullilove
Executive Director, Lowy Institute

Dr Michael Fullilove AM is the Executive Director of the Lowy Institute. Over the past two decades, Dr Fullilove has played a leading role in the establishment and development of the Lowy Institute. He wrote the Institute's feasibility study for Sir Frank Lowy in 2002 and served as the Director of its Global Issues Program from 2003 until his appointment as Executive Director in 2012. He has also worked as a lawyer, a visiting fellow at the Brookings Institution in Washington, DC, and an adviser to Prime Minister Paul Keating. He currently serves as a Commissioner of the CSIS-Chumir Global Dialogue and a member of the Advisory Council of the International Institute for Strategic Studies (IISS) in London. Dr Fullilove writes widely on Australian and US foreign policy and global issues, and is the author of a number of books in the foreign policy field.

Jordan Guiao
Research Fellow, The Australia Institute's Centre for Responsible Technology

Jordan Guiao is a Research Fellow at The Australia Institute's Centre for Responsible Technology. He is the author of the upcoming book *Disconnect: Why we get pushed to extremes online and how to stop it* through Monash University Press. Jordan is also the former Head of Digital/Social Strategy at the Australian Broadcasting Corporation. He lived and worked in Silicon Valley and gained unique insights into the technology capital of the world.

Malcolm Haddon
Associate Director, Community Resilience, Multicultural NSW

Dr Malcolm Haddon is Associate Director, Community Resilience, at Multicultural NSW. Working closely with community partners, religious leaders, academic experts, digital industry partners, police and government agencies, his team develops evidence-based policy and delivers key strategic projects that have been cited as good practice in social cohesion and community resilience-building in a wide range of international publications and forums.

Catherine Hawkins
First Assistant Secretary, Social Cohesion and Multicultural Affairs Division, Department of Home Affairs

Catherine Hawkins has extensive policy experience working for the Australian government. She recently joined the Department of Home Affairs to set up the proposed new Strategic Research and Communication Division and is also currently leading the Social Cohesion and Multicultural Affairs Division. More recently she led the Office for Women in the Department of Prime Minister and Cabinet. Prior to that she led many teams over nearly 25 years in the Attorney-General's Department working on diverse issues including transnational crime, anti-money laundering, anti-corruption, overseas law and justice aid work, access to justice, copyright and human rights. Catherine has an Arts/Law degree from the University of Sydney and a Master in Public Policy from Princeton University.

Lesley Honeyman
Director Operations, Department of Customer Service

Lesley Honeyman joined the Department of Customer Service in January 2019 as the Director Operations. In this role she is responsible for several functions which include intelligence, incident response, capability development, infrastructure security and vulnerability scanning. Together with her team she has established the first state government vulnerability scanning capability — Bathurst Vulnerability Management Centre. She has over 25 years of experience in the intelligence and security field, both at the state and federal level. Her experience includes providing leadership and coordination to cyber incident response, special events and operations managed by NSW Police Force (Lindt Café, World Youth Day and the 2000 Sydney Olympics). For that work she received a Deputy Commissioner's Commendation and an award of meritorious service.

Jennifer Hsu
Research Fellow, Lowy Institute

Jennifer Hsu is a Research Fellow in the Public Opinion and Foreign Policy Program. She is currently working on a project which explores the intersections of Australia's multiculturalism and foreign policy. Prior to joining the Institute, Jennifer was a Policy Analyst with China Matters. After completing her PhD at the University of Cambridge in Development Studies, she researched and taught in development studies, political science and sociology in universities in North America and the UK. Jennifer is also a Visiting Fellow at the Social Policy and Research Centre at the University of New South Wales. Her research expertise broadly covers state-society relations, state-NGO relations, civil society and the internationalisation of Chinese NGOs, and she has published widely in these areas.

Jennifer S. Hunt
Lecturer, Macquarie University

Dr Jennifer S. Hunt is a lecturer in Security Studies at Macquarie University specialising in cyber conflict and information warfare. She has led grants on cyber war and foreign interference (Defence Strategic Policy Grant) and countering election-related disinformation with the Australian Electoral Commission. Dr Hunt has served as a delegate at the Shangri-la Security Dialogue, the World Economic Forum in Abu Dhabi, and participated in CyCon at the NATO Cyber Center of Excellence in Estonia. Since 2020, Dr Hunt has worked closely with military, civil and health institutions to counter disinformation around Covid-19. She regularly provides expert commentary on the ABC, BBC, SBS and the History Channel. Dr. Hunt holds degrees from the University of Sydney and UNC Chapel Hill.

Julie Inman Grant
Australia's eSafety Commissioner, eSafety

Julie Inman Grant is Australia's eSafety Commissioner. In this role, Julie leads the world's first government regulatory agency committed to keeping its citizens safer online. Julie has extensive experience in the non-profit and government sectors and spent two decades working in senior public policy and safety roles in the tech industry at Microsoft, Twitter and Adobe. The Commissioner also serves on the World Economic Forum's Global Coalition for Digital Safety and on their XR Ecosystem Governance Steering Committee on Building and Defining the Metaverse. As Commissioner, she has led work to stand up novel and world-first regulatory regimes under the new Online Safety Act 2021, with implementation of a sweeping new set of reforms beginning on 23 January 2022.

Rita Jabri Markwell
Advisor, Australian Muslim Advocacy Network (AMAN)

Rita Jabri Markwell is a lawyer, public policy advisor, scholar and community advocate. A solicitor with Sydney law firm Birchgrove Legal, it is her pro bono work with the Australian Muslim Advocacy Network that has given her broad and deep insights into community experience. On behalf of AMAN, she has current test cases against Twitter and Facebook using discrimination law. She is published in the areas of dehumanisation of minorities online and has facilitated critical research into terrorism law and extremism definitions within the Global Internet Forum to Counter Terrorism (GIFTCT) to deal with the limitations of terrorism designation lists. She led a recent Christchurch Call Advisory Network report on dehumanisation and is involved in independently evaluating the Australian government's work under the Christchurch Call.

Nina Jankowicz
Vice President, Centre for Information Resilience

Nina Jankowicz is an internationally recognised expert on disinformation and democratisation and the author of two books: *How to Lose the Information War* and *How to Be A Woman Online.* Currently the Vice President at the UK-based Centre for Information Resilience, a social enterprise focused on countering disinformation, Jankowicz's expertise spans the public, private, and academic sectors. She has advised governments, international organisations, and tech companies; testified before the United States Congress, UK Parliament, and European Parliament; and led accessible, actionable research about the effects of disinformation on women, minorities, democratic activists, and freedom of expression around the world. In 2016-17, she advised the Ukrainian Foreign Ministry on disinformation and strategic communications under the auspices of a Fulbright-Clinton Public Policy Fellowship.

Lydia Khalil
Research Fellow, Lowy Institute

Lydia Khalil is a Research Fellow at the Lowy Institute. She focuses on transnational issues and manages the Digital Threats to Democracy Projects and convenes the Lowy Institute's partnership with the Global Network on Extremism and Technology. She is also a Research Fellow at Deakin University. She is a recognised expert on terrorism and extremism, having worked for the White House Office of Homeland Security, US Department of Defense, the New York Police Department, Boston Police Department and the Council on Foreign Relations. She is the author of the recently published *Rise of the Extreme Right: The New Global Extremism and the Threat to Democracy*. She is a frequent media commentator and has been widely published in both academic and popular press.

Katherine Mansted
Director of Cyber Intelligence, CyberCX

Katherine Mansted is Director of Cyber Intelligence at Australia's largest independent cybersecurity services company, CyberCX. She is also Senior Fellow in the Practice of National Security at the ANU National Security College. Previously, she led the ANU National Security College's Public Policy team. Katherine regularly briefs government, business and public audiences on national security and technology policy issues, including cybersecurity, information geopolitics and foreign interference. Katherine is also a Nonresident Fellow at the Alliance for Securing Democracy at the German Marshall Fund of the United States and a presenter on the National Security Podcast. Katherine holds a Master in Public Policy from the Harvard Kennedy School of Government. She holds Bachelors of Laws/ International Relations (Business) from Bond University.

Gareth Meyer
Assistant Director-General, Office of National Intelligence (ONI)

Gareth Meyer joined the then Office of National Assessments as Assistant Director-General, International Economy Branch (IEB), in January 2012. Prior to that, he worked for the Department of Treasury, Department of Prime Minister and Cabinet, and the Department of Foreign Affairs and Trade. He undertook postings in Moscow (1998-2002) and Geneva, participating in negotiations at the World Trade Organization (2005-2008). Gareth was appointed Deputy Head of Assessments in 2019 and has oversight of ONI analysts covering the international economy and geo-economics, climate change, cyber and critical technology, strategic and military analysis, and transnational crime. He has also overseen ONI's analytical tradecraft and outreach to think tank and business communities.

Tim Niven
Research Lead,
Doublethink Lab

Tim Niven has a background in both philosophy and computer science. He has been with Doublethink Lab for over two years. In his role as Research Lead, Tim oversees all aspects of Doublethink Lab's research. He also leads a number of projects that apply advanced technology to PRC information warfare in improving our capacity to detect and attribute information operations.

Roger Noble
Ambassador for Counter-Terrorism, DFAT

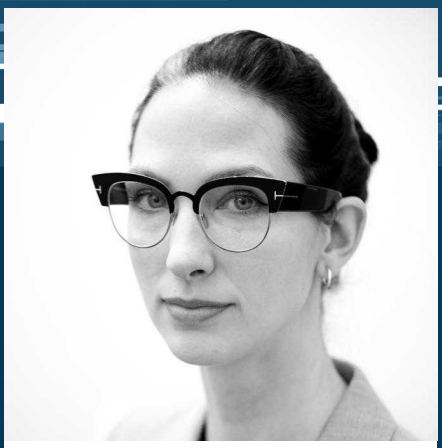
Mr Noble is Australia's Ambassador for Counter-Terrorism and is responsible for leading Australia's international engagement on counter-terrorism and represents Australia at bilateral, regional and multilateral forums. He also sits on Australian government domestic counter-terrorism forums. Mr Noble has had a distinguished military career, most recently serving as a Major General and Head of Military Strategic Commitments at Australian Defence Force Headquarters. Previous senior ADF roles include Deputy Chief of Joint Operations and deployments to Iraq as Deputy Coalition Land Force Commander and to Afghanistan with the International Security Assistance Force.

Sophie Oh
Co-founder, Susan McKinnon Foundation

Sophie Oh and her husband, Grant Rule, founded and fully funded the Susan McKinnon Foundation. SMF focuses on three key areas – effective elected representatives, robust state institutions and quality policy dialogue. We are deeply committed to strengthening and supporting democracy and government. We take a rigorous, pragmatic, non-partisan and long-term view of our mission. And so are keenly interested in understand the challenges from social media.

Jeff Pope
Deputy Electoral Commissioner, Australian Electoral Commission (AEC)

Jeff Pope is the Deputy Electoral Commissioner and in this role he has guided the AEC through an unprecedented period of change to successfully deliver the 2019 and 2022 federal elections. He is also the Chief Operating Officer for the AEC. Since 2018 Mr Pope has been the co-chair of the Board for the Electoral Integrity Assurance Taskforce (EIAT) which is a highly effective collaboration of a number of Commonwealth government agencies. The EIAT supports the AEC to deliver elections with integrity in this challenging communications and interference environment. Prior to joining the AEC, Mr Pope had a distinguished career with over 23 years in law enforcement and was awarded an Australian Police Medal for his outstanding contribution to law enforcement.



Erin Saltman
Acting Executive Director, Global Internet Forum to Counter Terrorism (GIFCT)

Dr Erin Saltman is the Director of Programming at the Global Internet Forum to Counter Terrorism (GIFCT). She was formerly Facebook's Head of Counterterrorism and Dangerous Organizations Policy for Europe, the Middle East and Africa. She has worked across sectors building out counter-terrorism strategies and CVE programs internationally. Dr Saltman's background and expertise includes both white supremacy and Islamist extremist processes of radicalisation within a range of regional and socio-political contexts. Her research and publications have focused on the evolving nature of online extremism and terrorism, gender dynamics within violent extremist organisations and youth radicalisation.

John Schmidt
Commissioner, NSW Electoral Commissioner

John Schmidt was appointed NSW Electoral Commissioner by the Governor of New South Wales and began his term on 8 August 2016. From 2009 to 2014 John was the Chief Executive Officer of the Australian Transactions Reports & Analysis Centre (AUSTRAC), after serving in senior NSW Government positions within the Department of Premier and Cabinet and the Department of Fair Trading.

David Shanks
Former Chief Censor, New Zealand Government

David Shanks was formerly New Zealand's Chief Censor. He was appointed to the role in May 2017 and led the Office of Film and Literature Classification, which is an Independent Crown Entity. He's responsible for protecting New Zealanders from harm, especially harm to children and young people. This balances with upholding New Zealander's right to freedom of expression and recognising the diverse views of all Kiwis. David's career has spanned senior leadership and legal positions in both the public and private sectors; he is a barrister and solicitor of the High Court of New Zealand. He has run some of the largest public legal teams in the country, and conducted national inquiries as Chief Legal Advisor for the State Services Commission. He sees his current role as the perfect opportunity to bring together his interests in regulation, public policy and technology. As a parent, David has a passion for the job and a determination to modernise the approach to the changing world of media content.

Jan Gerrit Voelkel
Doctoral candidate, Polarization and Social Change Lab Stanford University

Jan Voelkel is a PhD candidate in Sociology and a member of the Polarization and Social Change lab at Stanford University. Jan's research studies intergroup and interpersonal relationships with two guiding questions. First, what causes people's willingness to harm others and defend inequalities? Second, how can personal or societal change be achieved that increases equality and/or reduces harm? Jan is also interested in meta-scientific questions about how to make scientific progress more reliable. His research has been published in journals, such as *Proceedings of the National Academy of Sciences*, *Nature Human Behaviour*, and *Psychological Science*, and been featured in popular publications.

Pia van de Zandt
Director, NSW Department of Premier and Cabinet

Pia van de Zandt is the Director of the Connected Communities team, Social Policy Branch at the NSW Department of Premier and Cabinet. The team delivers strategic policy advice and designs and delivers programs to promote community safety, cohesion and inclusion, and to counter violent extremism.

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