AUSTRALIAN SECURITY LEADERS CLIMATE GROUP

THE CLIMATE DISINFORMATION WAR

HOW TO FIGHT BACK FOR AUSTRALIA'S DEMOCRACY AND SECURITY

MARCH 2026

aslcg.org

Written by Anastasia Kapetas. Published March 2026
by Australian Security Leaders Climate Group, Canberra ACT.

EXECUTIVE OVERVIEW

Australia faces a rapidly escalating breakdown in information integrity.

- Power in this digitally networked age comes from dominance in the information space and Australians are now living in a world increasingly shaped by propaganda and disinformation rather than factual information. Anti-climate-action propaganda and disinformation networks have grown into multi-billion dollar permanent campaigns, largely funded by fossil-fuel interests and their allies. These campaigns may be best understood through a lens of information warfare, combining traditional media influence, coordinated online activity and algorithmic amplification to shape narratives and perceptions at scale.
- The overall objective is not simply to convince, but to degrade the information environment itself, creating confusion, mistrust and institutional delegitimisation that weakens democratic decision-making on complex issues including climate and energy. The problem is becoming more acute with the emergence of even more powerful anti-climate-action coalitions, expansion of generative AI, and the global corporate consolidation of information power.
- Climate disinformation is evolving from a communications issue into a national security challenge, with implications for Australia's sovereignty, economic resilience, disaster readiness, institutional trust, and strategic autonomy in shaping its energy transition amid intensifying geopolitical competition. The response requires coordination not only across civil society and industry, but across security, economic, and governance institutions.
- Government efforts so far are not commensurate with the sheer scale, resourcing and coordination of disinformation networks. While the not-for-profit and renewable-energy-industry sectors are becoming much more aware of the climate disinformation problem, they are struggling to respond in the face of the dominance and legacy resources of the fossil-fuel industry in the information space.

KEY RECOMMENDATIONS

The task for government

- Rebuild accountability for climate information.
- Ensure credible information dominates during crises and disasters.
- Protect citizens, government, and decision-makers from manipulation.
- Safeguard those sharing factual information from intimidation.
- Prevent domestic policy distortion from foreign or coordinated influence.

Systemic approaches

Key measures include:

- Strong anti-trust rules, e.g., EU Digital Markets Act.
- Regulation of platforms, social media, and AI for transparency and liability.
- Urgent, enforceable rules for generative AI.
- Defamation law reform and improved election transparency.

Initial steps

- Invest in public resilience, research, independent journalism, and secure communication systems.
- Fund climate observatories, think tanks, and data collection infrastructure.
- Become a signatory to the UN Conference of Parties (COP) Declaration of Information Integrity on Climate.

THE PROBLEM: THE INFORMATION WAR ON CLIMATE & CLEAN TECH

Over the last two decades, anti-climate-action propaganda and disinformation networks have grown into multi-billion dollar permanent campaigns that run across the entire information ecosystem, with expenditure globally of up to seven billion dollars a year.[1] These campaigns may be best understood through the lens of information warfare, combining traditional media influence, coordinated online propaganda and disinformation, as well as algorithmic amplification to shape narratives and perceptions at scale. The opaque financial money networks funding this war are often aligned with both fossil-fuel interests and anti-democratic political projects.

Climate disinformation is now widely recognized as the most pressing challenge to climate change action,[2] just as disinformation more broadly now is prominent in global risk assessments.[3] Australians now live in a world increasingly shaped by propaganda and disinformation rather than factual information. The release of lightly regulated and unreliable generative AI (artificial intelligence) products has accelerated this trend, driving information systems deeper into a crisis of verification and accountability.

Currently there are offensives ranging across global information to turn back momentum on renewable energy and climate action, but also to attack democratic norms. The interests involved understand that power comes from dominance in the information space. The strategy is control over content production and dissemination, through networks of think tanks, public relations companies, control of social media, broadcast, cable and radio networks, the cultivation of online influencers in every major demographic, and the mass deployment of bots and other digital disruption techniques. The narratives at play here combine anti-climate-action sentiment with anti-immigration, anti-democracy, anti-journalism, anti-racial-equality, anti-LGBTQI, anti-science and anti-government tropes.

Misleading narratives do not arise only from false statements. By making climate too problematic to talk about without engendering outrage, these propaganda and disinformation strategies also utilise the deliberate omission of relevant information — sometimes described as "strategic silence", "selective disclosure" or "disinformation by omission" — to distort public understanding.

1 cssn.org/news-research/global-assessment; abc.net.au/news/2026-01-26/atlas-network-mont-pelerin-society-neoliberal-think-tanks/105700628; heated.world/p/fossil-fuel-propaganda-is-evolving
2 unfccc.int/news/countries-seal-landmark-declaration-at-cop30-marking-first-time-information-integrity-is-prioritized
3 For example, weforum.org/publications/global-risks-report-2025 and globalchallenges.org/gcr-2026.

When public officials repeatedly discuss events such as floods, fires or heatwaves while failing to mention their scientifically-established drivers, audiences can be left with a misleading impression about the causes and significance of those events. In communication theory, frameworks such as agenda-setting and framing theory understand the systematic omission of key context as a form of narrative shaping that influences how risks are perceived and prioritised. Persistent silence about relevant causal factors — particularly when the scientific link is well established — can function as a form of information distortion even when no explicit false statement is made. The refusal of the Australian Government to release a declassified 2022 climate and security risk assessment prepared by the Office of National Intelligence falls into this category. Such actions contribute to the "delayed disclosure trap", such that as undisclosed climate risk grows, the disincentive to disclose grows with it.[4]

The overall objective is not simply to convince people to believe false information, but to degrade the information environment itself, creating confusion, mistrust and institutional delegitimisation that weakens democratic decision-making on complex issues such as climate and the energy transition.

There are a number of global trends likely to drive even more climate disinformation and propaganda into the Australian information system in the near term: the emergence of new and even more powerful anti-climate coalitions, expansion of generative AI, and the global consolidation of information power by a small number of companies. In the last three years, new and formidable anti-climate-action and anti-renewable-energy alignments between far-right political movements, the digital tech sector and fossil-fuel states have emerged globally, exacerbated by the election of Donald Trump.

The current US administration has an aggressive anti-climate-action and anti-renewables agenda and is now a dominant purveyor of climate disinformation and propaganda, using the massive economic, administrative and security levers at its disposal to attempt to diminish the renewable energy industry and to destroy US government research and information resources on climate. This includes using the USA's market power to punish nations pursuing a renewable energy transition and anti-disinformation legislation, and to derail multilateral climate agreements. US foreign policy is now organised around increasing the USA's geopolitical dominance through forcing dependency on US tech companies and the fossil-fuel sector.

The rapid expansion of generative AI tools now allows the creation and distribution of vast quantities of synthetic content — text, images, video and audio — that can flood information ecosystems at unprecedented speed and scale, dramatically lowering the cost of coordinated propaganda campaigns. The widespread use of AI as a search engine is also hurting credible climate journalism by diverting user traffic to AI-scanned sources and depriving outlets of advertising revenue.

At the same time, consolidation of information power among a small number of global technology and media platforms has concentrated control over digital communication infrastructure in the hands of a small group of private actors, many of whom are reducing moderation of harmful disinformation and weakening cooperation with democratic governments attempting to regulate it. This consolidation is also harming climate journalism as these new media monopolies slash climate reporting teams in traditional media.

The result is a structural deterioration in accurate information and storytelling on the climate crisis and its implications.

4 strategicclimaterisks.substack.com/p/are-we-in-a-delayed-disclosure-trap

It is important when thinking about how to counter disinformation and propaganda to recognise how pleasurable disinformation can be. People inhabit disinformation spaces emotionally. They are sites that offer a sense of belonging and freedom from isolation, the emotional catharsis of feeling shameful emotions, anger, fear of others etc. without social sanction, the novelty and excitement of outlandish conspiracies, and escape from overwhelming painful realities that an individual may feel powerless to confront, like the climate crisis. Many anti-disinformation strategies work on the assumption that people always want to hear truths, factual information. Disinformation works because the opposite is often true.

NATIONAL SECURITY IMPLICATIONS

Climate disinformation is evolving from a communications issue into a national security challenge, with implications for Australia's sovereignty, economic resilience, disaster readiness, institutional trust, and strategic autonomy in shaping its energy transition amid intensifying geopolitical competition.

Where sustained information operations shape national energy policy, undermine renewable energy investment stability, erode trust in scientific and governmental institutions, and polarise communities around infrastructure projects, the implications extend beyond public debate into the realm of national security, democratic stability and economic resilience.[5]

Climate systems, energy transitions, and digital information platforms now sit at the centre of geopolitical contests. Control over fossil-fuel supply chains, renewable technology markets, AI development and global media infrastructure increasingly determines economic advantage and strategic leverage. In this context, coordinated anti-climate-action and anti-energy-transition propaganda campaigns operate not merely as domestic political interventions, but as instruments within broader geopolitical struggles.

In Western democracies, networked movements combining anti-climate-action, anti-regulatory, and anti-democratic agendas have demonstrated a sophisticated capacity to use information power across print, broadcast, social media, and generative AI systems. Where such campaigns are linked — directly or indirectly — to fossil-fuell interests, foreign interference, or states seeking to reshape global energy alignments, the boundary between political persuasion and strategic interference becomes increasingly blurred.

For Australia, the risks are multidimensional.

First, there is a **sovereignty risk**. When external or transnational actors are able to influence domestic energy choices, regulatory frameworks, or public consent for major infrastructure projects through coordinated information operations, this constrains Australia's strategic autonomy in determining its own economic and energy future.

Second, there is an **economic security risk**. Delays or reversals in the renewable transition — whether through policy paralysis or destabilised social licence — have consequences for productivity, trade competitiveness, investment confidence, and exposure to climate-related economic shocks. Information-driven disruption of transition planning therefore has material economic effects.

Third, there is a **disaster and defence readiness risk**. As climate-driven extreme weather events intensify, effective emergency response depends on public trust in scientific institutions and government communication. Sustained erosion of institutional credibility through disinformation campaigns weakens national resilience in times of crisis.

Fourth, there is an **institutional legitimacy risk**. Persistent polarisation, disinformation and diminution of expertise reduce the state's capacity to implement long-term policy in the face of existential challenges. Over time, this impairs governance continuity and democratic stability.

The Senate Select Committee inquiry on Information Integrity on Climate Change and Energy has heard evidence that internationally connected climate disinformation operations are active within Australia.[6] However, the broader policy question is whether such dynamics should be assessed solely through regulatory and communications frameworks, or whether they warrant treatment within Australia's national security architecture.

If climate disinformation functions as a strategic lever capable of shaping energy systems, economic trajectories, and public trust, then responding to it requires coordination not only across civil society and industry, but across national security, economic, and governance institutions.

5 newclimate.org/news/how-climate-disinformation-is-reshaping-geopolitics-and-europes-role-in-fighting-it
6 abc.net.au/news/2026-02-19/climate-disinformation-senate-committee-dr-karl-atlas-network/106350002

THE TASK: GOVERNMENT ACTION

Australia has a long history of anti-climate disinformation activity[7], and the federal government has undertaken a number of welcome measures in the last decade to manage disinformation and other online harms, including expanding the role and funding of the Office of the eSafety Commissioner, developing a voluntary code of conduct for social media companies monitored by the Australian Communications and Media Authority and experimenting with digital literacy programs.

However, these efforts are not remotely commensurate with the sheer scale, resourcing and coordination of anti-climate-action and clean-tech disinformation networks in the Australian information environment.

NGO and renewable industry sectors are becoming much more aware of these networks and their impacts, but are struggling with their limited resources to respond effectively in the face of the dominance and legacy resources of the fossil-fuel industry. Their efforts are vulnerable to being overwhelmed by the speed and volume of disinformation as they tend to be largely defensive in nature, trying to respond to disinformation narratives as they arise, often without collaborating across their sector to amplify messages.

These sectors are also hampered by using normal communications practices to respond to information warfare tactics in a disordered information environment. They don't have the right expertise to analyse disinformation networks so that responses can be efficiently targeted for maximum strategic effect. Some do not have an effective digital and social media presence, and put faith in facts and good faith arguments to combat disinformation operations that use more powerful emotive appeals.

Currently NGO and industry sectors rely on institutional truth-tellers in the information environment to bolster credible climate narratives and information: governments, regulators, academics, traditional news media, public broadcasters and others. However, trust in many of these institutions is eroding, and they may not occupy commanding heights of the information environment for large sections of the population.

It is clear that civil society cannot currently take on disinformation networks alone. The task for government then becomes working across sectors to:

- Rebuild an ecosystem of accountability for climate information, an ecosystem that can be trusted by governments and markets, and the broader Australian community as climate change impacts accelerate. The Australian community has a right to understand the reality of the climate threats facing them in a timely manner in order to be appropriately prepared.
- To ensure that credible information overwhelms disinformation in times of national crisis and natural disaster.
- To protect citizens, government and economic decision makers from extreme cognitive manipulation on critical climate and energy issues.
- To ensure that citizens promoting factual climate information, including public officials, are not subject to punitive online campaigns, threats, harassment and intimidation.
- To ensure that citizens' rights to genuine climate protest action is not suppressed.
- To restore Australia's information sovereignty in the climate and energy debate, ensuring that domestic policy decisions are not distorted by coordinated foreign or transnational information operations.

7 aph.gov.au/Parliamentary_Business/Committees/Senate/Information_Integrity_on_Climate_Change_and_Energy/ClimateIntegrity/Submissions

THE TOOLBOX: ADDRESSING SYSTEMIC RISKS

The Australian Government should recommit to putting in place systemic protections against disinformation. Climate propaganda and disinformation cannot be properly addressed without government action to combat disinformation as a whole across the information ecosystem.[8] The main approaches in the systemic risk toolbox include the following.

ANTI-TRUST MEASURES

Governments around the world are either considering or implementing anti-trust measures aimed at breaking up monopoly power and the anti-competitive practices of the world's biggest tech companies in the interests of consumers. An example of a comprehensive anti-trust architecture is the current EU Digital Markets Act.[9] However, other countries such as the USA have pursued major anti-trust litigation cases against companies to restore competitive practices to the sectors in which they operate.

In addition, calls to repeal anti-circumvention laws[10] — which prohibit modifying existing digital products — are gaining traction. Repeal of these types of laws would support the concept of the right to repair, but also may help states to more easily regulate monopoly tech companies and further develop their own national digital industries that suit their own national interests better, that is, to strengthen their digital sovereignty. Anti-trust measures may be necessary when tech companies get too powerful to make meaningful regulation possible, including on accountability for their products enabling the mass dissemination of disinformation.

DIGITAL PLATFORM REGULATION, SOCIAL MEDIA AND AI

The EU Digital Services Act (DSA), sister legislation to the Digital Markets Act, is the most comprehensive attempt to date to assist social media companies take responsibility for online disinformation and other harms. Elements of the DSA and its principles of liability, user control, transparency and systemic risk have informed other regulatory frameworks around the world.

In terms of liability, some approaches seek to treat social media companies as publishers: in the USA, some politicians across the spectrum are calling for a repeal of Section 230 of the Communications Decency Act, to hold digital platforms liable for all third-party speech. The DSA has a more limited view of liability, that companies are not liable for the content they host unless illegal under existing EU and national laws on hate speech or targeted foreign interference. It is worth noting that the DSA bans the monitoring of general content, to protect the free speech of individuals.

User control: To avoid a purely top-down approach, frameworks such as the DSA have strong provisions supporting user rights to challenge moderation decisions, including through courts, stronger privacy settings, clear and legible terms of service, citizen ownership of their online data.

8 asiapacific4d.com/idea/information-environment/
9 digital-markets-act.ec.europa.eu/index_en
10 theguardian.com/commentisfree/2026/jan/10/trump-beginning-of-end-enshittification-make-tech-good-again

Transparency: Measures include requiring social media companies to:

- Keep up-to-date records of disinformation on their networks.
- Ensure algorithmic transparency so that the public have some idea of what sort of content digital platforms are actively promoting and third-party data sharing to see how users may be targeted though their data profiles.[11]
- Make social media data available to researchers.
- Label political, AI and other inauthentic coordinated content.

Another important area is regulating coordinated bot and spam activity, which are major vectors of disinformation. Generative AI has made this more urgent, with the ability to create bot swarms that more closely mimic human activity, making them harder to detect.

SYSTEMIC RISKS

Large social media companies need to take responsibility for the ongoing and possible future systemic social, economic and political risks that their services might produce, and to do so formally, in an annual report to the regulator, with similar reports submitted from civil society and researchers.

Many countries have attempted to incorporate similar elements into their own national anti-disinformation frameworks, but with extremely mixed success. In Australia, these efforts seem to have been abandoned with the withdrawal of the 2024 Combatting Misinformation & Disinformation Bill, which failed ostensibly over free-speech concerns. But the need to protect information integrity in Australia is only growing. And elements of this bill that don't touch on free speech issues, such as its transparency provisions, could be reintroduced.

REGULATION OF GENERATIVE AI

Australia also needs specific, strong, enforceable regulation of generative AI as a matter of urgency. The use of these AI chatbots and image generators have unleashed new frontiers of disinformation at previously unimagined scale. At the same time, AI chatbots are prone to sycophancy, hallucination and bias, but are now used everywhere as a single source of truth in the institutions that people rely on to produce accurate and truthful information, such as government departments, universities and research institutions, and increasingly in court cases and in journalism.[12] They also make it easier to fabricate research.[13]

This synthetic AI research can then be used to create an evidence base for climate denialism that sounds authoritative and to subvert government inquiries into climate issues; and once on the public record, will then likely feed back into AI training data. And finally, overt attempts are being made by some chatbot companies such as xAI to rebuild chatbots to present far-right ideologies as fact. All this is contributing to the crisis of verification and accountability afflicting our information ecosystems.

Again, the EU Artificial Intelligence Act provides an example of what a regulatory architecture might look like. In particular, the Act contains strong prohibitions against impersonating a real person with AI, coordinating bot activity aimed at cognitive manipulation, as well as all the things AI systems can do to create a SkyNet-like digital framework to survey and manipulate citizens. These include subliminal manipulative and deceptive AI, biometric categorisation systems, social scoring, and compiling facial recognition databases.

Other measures include labelling of AI content, copyright provisions, and mandating training data transparency.[14] AI literacy programs to help citizens navigate AI harms would also be a critical part of this type of framework. And the government could also consider how to support a national AI sector that better serves its democratic public interest.

11 algorithmwatch.org/en/dsa-explained/
12 csiro.au/en/news/All/Articles/2025/March/AI-can-fuel-research-misconduct
13 cedmohub.eu/experts-warn-ai-written-paper-is-latest-spin-on-climate-change-denial/
14 As image generation improves, it is becoming more difficult to identify fake images by automated technological means alone.

OTHER LEGISLATION

The government also needs to address the exploitation of defamation law in Australia by powerful interests. Strategic Lawsuits Against Public Participation (SLAPPs)[15] have been used against journalists and civil society who attempt to speak out in the public interest to great effect on climate issues. Even when suits are unsuccessful, the costs involved are a potent deterrent. In the same vein, federal protections should be strengthened to allow citizens to engage in lawful protest, rights that have been wound back in so many Australian states.

A final legislative piece should promote greater election transparency, specifically around truth in political advertising and increasing public oversight of political donations. Current laws only cover political advertising during elections, but as has been noted by civil society organisations, climate disinformation networks operate constantly, often in the field years before an election is called, attempting to seed and frame the information environment in their favour. In the same way, civil society organisations need to be able to put factual content on climate during election campaigns, but current restrictions prohibit them from doing so and should be repealed.

INITIAL STEPS

The actions above outline the breadth and depth of legislative reform needed to restore integrity to our information systems, and may require a longer-term deliberative effort. This means that other, potentially easier, implementable measures need to be pursued at the same time, as part of an information integrity package that could also build momentum for tougher legislative reform.

These initial measures could include:

- Strengthening public resilience to disinformation through improved civic education and digital literacy. Literacy programs should be rolled out across all tiers of education to help citizens learn to promote critical thinking skills that will help them recognise propaganda and disinformation from an early age, and as a preventative against online radicalisation. Training in countering disinformation should also be available across all levels of government. The public service is not the only sector vulnerable to disinformation, and political, military and economic decision makers are increasingly vulnerable. As one example, Finland's media literacy education system is an important part of its effort to strengthen societal resilience to systematic and targeted dissemination of disinformation and anti-democratic messages and continues a decades-long effort to promote democratic participation and reduce polarization in Finnish society.[16]
- Funding to support an ecosystem of credible disinformation observatories and fact-checking organisations, that are able to work together to pre-bunk disinformation and provide publics and governments with open source intelligence on disinformation operations and influence campaigns. This funding needs to come with legal protections such as anti-SLAPP laws discussed above to protect these organisations from excessive harassment. Fact-checking organisations in Australia have folded due to bad-faith targeting by well-funded organisations that traffic in propaganda and disinformation. Similarly, disinformation researchers have been harassed, threatened and accused of being part of an "industrial censorship complex" by anti-climate propagandists, both in Australia and internationally. For example, disinformation researchers are now refused visa entry into the US.[17]

15 hrlc.org.au/news/2024-10-31-anti-slapp-laws/
16 oecd.org/en/publications/mis-and-disinformation_b00de6dc-en/media-literacy-education-system_d067f517-en.html
17 reuters.com/legal/government/lawsuit-challenges-us-policy-barring-visas-social-media-researchers-2026-03-09/

On climate, and the clean-tech sector in particular, there is much more that the government can do to increase the volume of accurate, evidence-based climate and energy transition in the information ecosystem. Some examples include:

- Developing requirements for renewable companies to build a stronger licence for renewable energy projects and to assist by funding localised information hubs in renewable energy zones to inform citizens factually on projects and to provide conduits for feedback on local concerns around projects.
- Funding climate policy think tanks to tackle complex issues around disaster relief, climate risk and security, climate and economic risk, clean-tech innovation and regulation, as well as analysis of climate disinformation threats.
- Developing green tech investment and R&D centres of excellence.
- Building information and communication systems for disaster relief that are resilient to disinformation. Climate and other disinformation operations increasingly target natural disasters. The shock, confusion and high attention surrounding disasters make perfect seeding grounds to push anti-climate-action, anti-government and other types of disinformation and conspiracism.[18]
- Funding a dedicated network of climate disinformation observatories in Australia and potentially across the region, where possible attached to climate research in the tertiary sector.
- Supporting independent journalism, research institutions and public-interest media capable of producing credible climate reporting and analysis in an increasingly fragmented information environment.
- Become a signatory to the UN Conference of Parties (COP) Declaration of Information Integrity on Climate. Current signatories include: Brazil, Chile, Denmark, France, Morocco, the United Kingdom, Spain, Sweden, Uruguay, Belgium, Canada, Finland and Germany, Austria, the Netherlands, Slovenia, Czechia, Estonia, and has been endorsed by the European Union.[19]

Possibly one of the most important actions the Australian Government should take right now is to commit resources to do its part in shoring up the collection and analysis of national and globally-relevant climate data. With the continued destruction by the USA of climate and clean-tech data and research at NOAA, NASA, NCAR and more broadly, Australia and the rest of the world is losing a vital resource to combat climate change and to drive clean-tech innovation. The government could commit to further strengthening the capabilities of Australia's climate sensor and satellite programs, at the CSIRO and BoM, and by establishing an Australian Institute for Earth System Science.[20]

18 For example, a significant blackout in Spain triggered a firestorm of disinformation: reneweconomy.com.au/spains-blackout-has-already-triggered-a-firestorm-of-disinformation

19 brusselstimes.com/1941251/eu-throws-weight-behind-global-pledge-to-combat-climate-disinformation

20 science.org.au/our-work/resources-reports/reports-publications/decadal-plan-australian-earth-system-science-2024-2033

THE PATHWAYS: STRATEGIC DIRECTIONS

The Senate Select Committee inquiry on Information Integrity on Climate Change and Energy has platformed many worthwhile suggestions to tackle climate change disinformation. But successful implementation requires some reflection on the last few years of lost momentum on pro-climate-action and anti-disinformation measures. How to turn these proposals from wish lists into political realities?

While the chaotic current political environment seems unpromising for these sorts of reforms, there is no time to waste. The increasingly disordered information environments that are helping drive current geopolitical chaos and the rise of authoritarian movements may make implementation more difficult the longer that action is delayed.

There are opportunities, too. The public is increasingly anxious about disinformation and reform in these areas is politically popular. And events that throw fossil-fuel energy systems into crisis like the attack on Iran by the USA and Israel in March 2026 bring the limitations of those systems into stark relief.

But at the same time, fossil-fuel companies, flush with high oil and gas prices, are already spreading narratives about the inevitability and stability of fossil fuels, and necessity of retaining the energy status quo in a time of uncertainty.[21] There was a similar playbook on oil and gas price inflation in the wake of Russia's invasion of Ukraine. This means that pro-climate-action and clean-tech actors in government, in civil society and in the private sector need to be ready to compete on the information terrain to contest fossil-fuel narratives and need to put developing information power at the centre of their agendas.

It is also necessary to confront the extremely effective but bad-faith narratives around free speech and censorship. Drawing attention to easily disprovable disinformation on climate and energy is not censorship. Pro-climate action forces should lean into the UN assertion that the rights to reliable information are completely intertwined with rights to freedom of expression.[22]

Adequate resources need to be allocated to build enforcement and compliance mechanisms for structural disinformation reforms that can be delivered in a timely, transparent and credible manner. Effective enforcement is needed to build trust in regulatory systems, and investigatory skill sets need to be developed.

The issue of cost should not be prohibitive. Building these systems will not be nearly as expensive as allowing Australia's information systems to continue to degrade. And arguments that regulation always strangles innovation are not accurate. Well designed regulation can actually push the innovation bar higher, by encouraging innovators to consider the social and safety implications of their products.[23]

And finally, climate disinformation reforms can mean taking on extremely powerful actors who may possess many avenues of leverage over governments. This being the case, it can make sense to build international alliances and regulatory regime alignment including on investigatory and enforcement capability.

21 heated.world/p/fossil-fuel-propaganda-is-evolving
22 ohchr.org/en/press-briefing-notes/2021/07/access-reliable-information-sources-obvious-antidote-disinformation
23 linkedin.com/pulse/how-regulation-standards-can-driver-innovation-innovateuk-gf6me

ABOUT ASLCG

The Australian Security Leaders Climate Group is a non-partisan network of Australian security and policy professionals that is working to reframe the climate debate and make climate an immediate security priority in Australia, through assessing the full level of risk posed by climate change and building resilience for local and global protection.

ABOUT THE AUTHOR

Anastasia Kapetas

Anastasia Kapetas is a political communications consultant and geopolitical analyst working on technology, climate and conflict. She is on the advisory board at the Climate Security Network, and was a Senior Advisor for AP4D on the geopolitics of disinformation and climate security issues. Until July 2022, Anastasia was the National Security Editor at the Australian Strategic Policy Institute (ASPI), as well as an associate of ASPI's Climate and Security Policy Centre. Prior to joining ASPI, Anastasia has been an advisor to the National Security College Futures Hub, and an intelligence manager at Defence, working across a range of geopolitical, scientific, technical and operational areas, as well as the editor-in-chief at *The Diplomat*. Anastasia brings extensive experience in intelligence assessment, geopolitical risk analysis, and cross-sector strategic briefings, including engagement with policymakers, defence stakeholders, media leaders, and international partners.

ADVISORY CONTRIBUTOR

Admiral Chris Barrie AC
Former Chief of the Defence Force (Retd)

Chris Barrie retired in 2002 after 42 years in the RAN, ending in four years of service as the Chief of the Defence Force (CDF). Since then, he has worked on strategic leadership issues as consultant, teacher and mentor at Oxford University, the National Defense University in Washington DC and at the Australian National University. In 2015 he was an author of a report "Climate Change, Security and the ADF". Chris is the Australian chair of the Global Military Advisory Council on Climate Change.

AUSTRALIAN SECURITY LEADERS CLIMATE GROUP