

VOL
50



Disinformation and cognitive warfare

Alana Ford



Perth USAsia Centre
INDO-PACIFIC STRATEGY

INDO-PACIFIC ANALYSIS BRIEFS 2025

INDO-PACIFIC ANALYSIS BRIEFS 2025

The Perth USAsia Centre's Indo-Pacific Analysis Briefs seek to provide perceptive and contemporary insights from across the region. The series features leading analysts from Asia, Australia and the US to deliver up-to-the-minute assessments on issues of national and regional importance. This series will shine a light on the issues that remain critically important to Australia and the Indo-Pacific at a time when global events may otherwise dominate the news cycle.



AUTHOR

Alana Ford

Senior Research and Program
Fellow, Perth USAsia Centre

Alana leads the Centre's work on critical and emerging issues, with a particular focus on cyber and tech policy. She brings to the role extensive experience working on these issues for the Commonwealth Government in Australia and internationally, as well as passion for driving social impact and policy change at the intersection of technology and society.

Prior to joining the Perth USAsia Centre, Alana served as the Attorney General Department's representative to the United States in Washington D.C. In this role, she led the Australian Government's efforts to address online harms and criminal exploitation of technology, as well as other high profile national security, law enforcement and criminal justice matters.

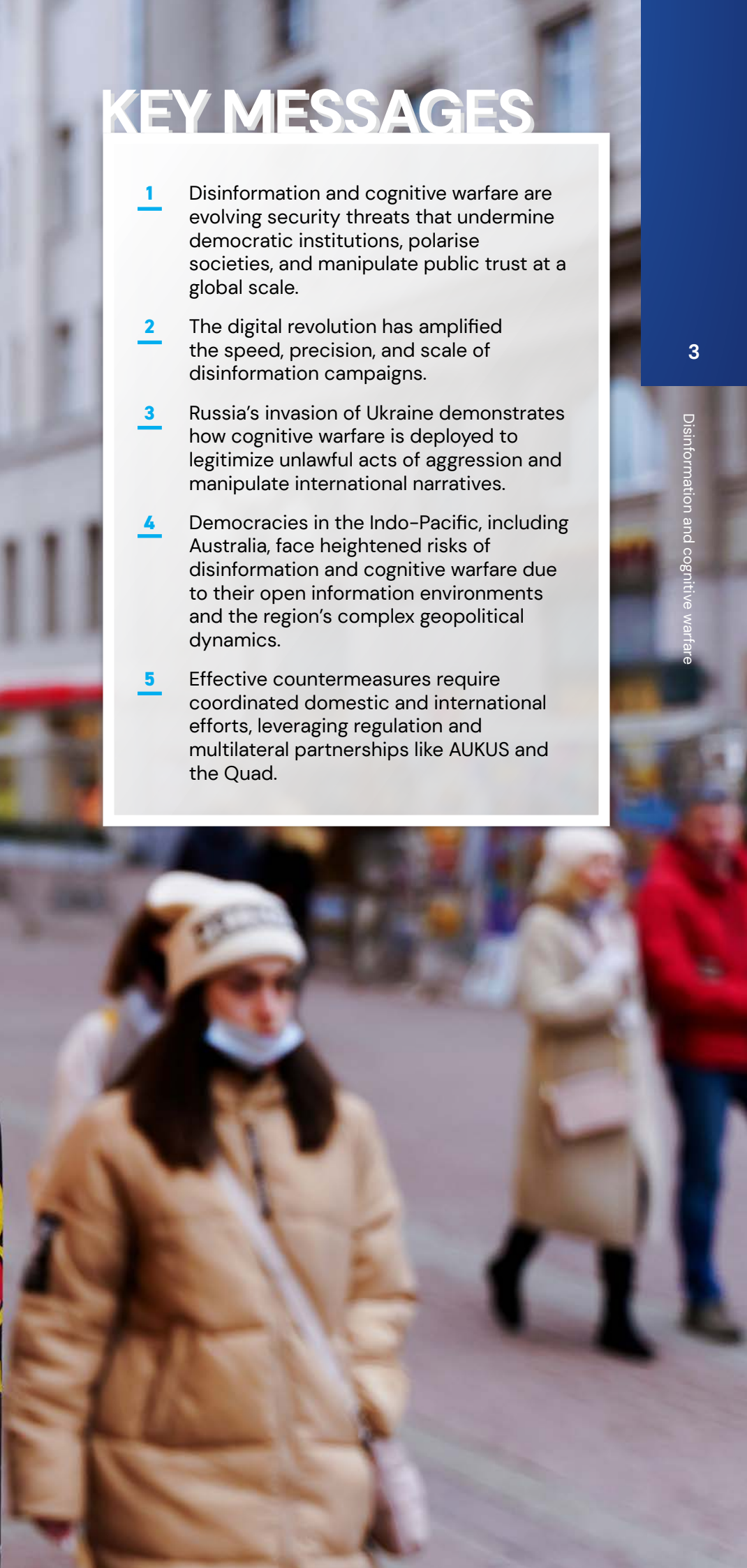
Previously, she served in the Department of Home Affairs, where she led work on a broad range of national security issues, including cyber and digital technology policy, law enforcement policy, countering online terrorism, child exploitation, and intelligence.

Alana's expertise extends beyond her public service, with a strong commitment to responsible tech advocacy and leadership through her position on the Board of Directors at the Data Federation Lab.



KEY MESSAGES

- 1 Disinformation and cognitive warfare are evolving security threats that undermine democratic institutions, polarise societies, and manipulate public trust at a global scale.
- 2 The digital revolution has amplified the speed, precision, and scale of disinformation campaigns.
- 3 Russia's invasion of Ukraine demonstrates how cognitive warfare is deployed to legitimize unlawful acts of aggression and manipulate international narratives.
- 4 Democracies in the Indo-Pacific, including Australia, face heightened risks of disinformation and cognitive warfare due to their open information environments and the region's complex geopolitical dynamics.
- 5 Effective countermeasures require coordinated domestic and international efforts, leveraging regulation and multilateral partnerships like AUKUS and the Quad.

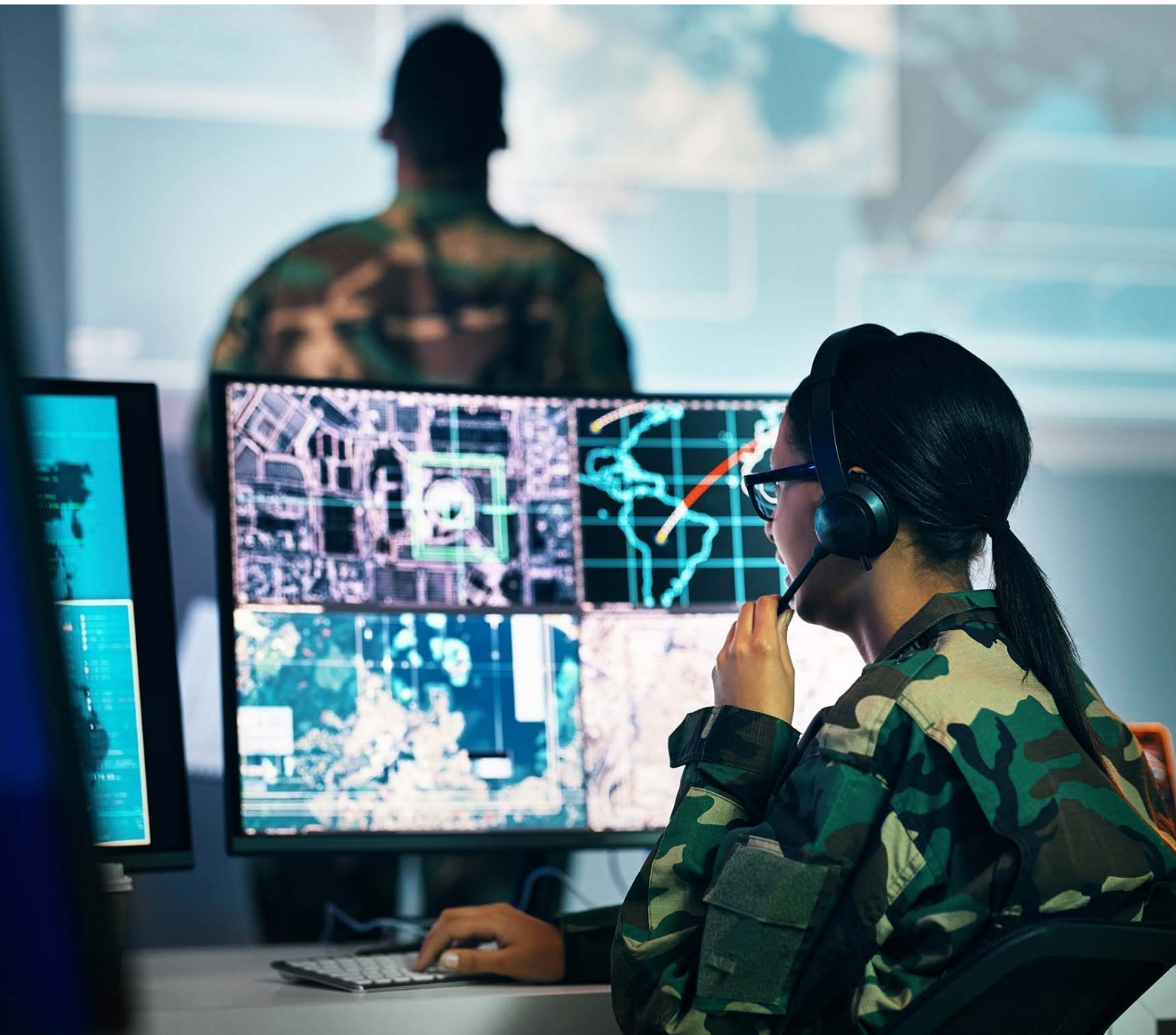




Disinformation and cognitive warfare are not new concepts; they have been tools of manipulation and control for centuries, from ancient military strategies to Cold War propaganda. With the rapid advancement of technology, these tactics have evolved into sophisticated and pervasive security threats that transcend traditional boundaries.

Modern disinformation campaigns exploit digital technologies to target individuals, societies, and institutions with unprecedented precision, speed and scale.

Beyond its role in modern warfare, the implications of disinformation extend far deeper, threatening the foundations of democratic institutions and eroding public trust. In an era where information flows freely and rapidly, adversaries weaponize misinformation to manipulate public opinion, polarise societies, and undermine confidence in governments and electoral processes. Understanding and countering these threats is not only critical for national security but also essential for safeguarding the stability, resilience, and integrity of democratic systems across the Indo-Pacific and globally.



Definitions and examples

There are many terms used to describe false, biased or misleading information shared for manipulative, ideological or strategic purposes. Not all types involve falsehoods (some use selective truths in harmful or manipulative ways) and it is not always spread with an *intent* to deceive or cause harm. Some of the most frequently used terms are:

Disinformation	False, misleading or biased information deliberately spread with the intent to deceive or harm.	In the lead up to the 2024 US presidential election, Russian actors disseminated disinformation alleging election fraud. These efforts were intended to undermine public trust in the US' election process and democratic institutions.
Misinformation	False, misleading or biased information spread without the intention to cause harm as the person sharing it believes it is true.	Throughout the Israel-Hamas conflict, false claims, unverified reports and misattributed images and videos have flooded social media , often shared out of concern or outrage, leading to widespread confusion.
Mal-information	Information based on reality, but shared with the intent to cause harm or sow discontent. For example, sharing private information in order to discredit someone.	In November 2023, France accused Russian networks of exploiting social divisions and antisemitism by amplifying real images of Star of David graffiti in Paris on social media. This was intended to incite further social tensions and unrest.
Propaganda	Biased or misleading information used to promote a political agenda.	China has a sophisticated and vast propaganda system , which enables its information campaigns. China exploits non-traditional media outlets like search engines and YouTube to share state-sponsored media globally, often heavily biased and omitting facts.
Influence / narrative campaigns	Coordinated strategic communication efforts that may involve mis/dis/mal-information, intended to promote specific narratives, shape perceptions and influence behaviour. Often emphasises certain facts while omitting others.	China's state-sponsored campaign known as ' Spamouflage ' involves the creation of fake social media accounts that spread anti-Western and anti-democratic sentiment, including accounts posing as US citizens ahead of the US election.
Cognitive / information warfare	An invasive weaponisation of information, targeting cognition and exploiting human vulnerabilities. It alters the cognitive functions, perception and decision-making of individuals and populations. Cognitive and information warfare is often conducted to precede or coincide with conventional, hybrid or cold war.	Russia uses cognitive warfare as a non-military warfare tactic in its ongoing invasion of Ukraine. As a result, Russia has created a sense of legitimacy to the war, as demonstrated by declining global public opinion polls for supporting Ukraine, and increasing criticism of Western support of Ukraine from developing countries.

The evolution of disinformation and its use in war

Information warfare has been used since ancient times, and texts as far back as Sun Tzu's "The Art of War" (from the 5th century BCE) talk about the use of deception and psychological warfare.¹ Throughout history, military leaders and governments have employed tactics like disinformation, censorship, propaganda and deception to gain strategic advantages.

The modern concept of information warfare was used extensively in World War I, World War II and the Cold War.² The advancement of digital technologies in the late 20th century marked a significant turning point in the evolution of information warfare. The information age and digital revolution that came with the advent of the internet completely revolutionised war and strategic competition³, with the added benefits of:

- expanded reach,
- real-time dissemination of information and immediate consumption by the intended audience,
- new key battlegrounds on social media, messaging and content sharing platforms, and
- the democratisation of information, meaning the ability to create and spread information has a lower barrier to entry and is accessible to a wider range of actors including non-state entities.

In recent years, technological advancements have made cognitive and information warfare even more sophisticated and multifaceted.

Artificial intelligence and machine learning have enhanced the ability to create and disseminate targeted content at an unprecedented pace and industrial scale. This has also opened up the ability to create deep fakes, produce content in more languages than ever before, and conduct vast big data analysis to measure sentiment and improve the effectiveness of targeted information campaigns.⁴

Russia's tactics against Ukraine: A new frontier

Since Russia's full-scale invasion of Ukraine in February 2022, it has made several significant shifts in its use of disinformation and approach to cognitive warfare.

- **Shift to social media platforms.** After sanctions disrupted state-sponsored media outlets like RT and Sputnik, Russia has ramped up its use of TikTok, Telegram, X, and other platforms to **reach international audiences**. This includes establishing the largest known influence campaign on TikTok to undermine the Ukrainian government's credibility.
- **Expansion of target audiences.** Russia has broadened its disinformation efforts, expanding targeted propaganda campaigns across **Latin America, Africa and the Middle East**. These campaigns are effective, and tailor messaging to cater to regional audiences and exploit existing grievances.
- **Sophisticated data manipulation.** There are reports that Russia has increasingly relied on **manipulating data** to shape narratives, including by distorting statistics on military losses, demographics and refugee issues, and by presenting false data or presenting correct data in misleading ways.
- **Diversification of tactics.** Russia has deployed a variety of **new** and **adapted** tactics including the use of inauthentic networks on social media, increased hacking and document forgery activities, deployment of the "Matryoshka" campaign which targets foreign fact-checkers, and flooding information channels with positive narratives to distract from the realities of the battlefield.
- **AI integration.** There are signals that Russia has **incorporated AI** into its disinformation efforts, including by deploying AI-powered tools to identify dissenting voices, and to produce AI-generated content targeting English-speaking audiences.
- **Domestic information control.** Russia took **swift control** of broadcasting infrastructure in occupied territories, imposed harsh prison sentences for dissent on social media, and has commissioned influencers to reach and appeal to new audiences.

Supporters of Ukraine are responding to Russia's use of disinformation with a variety of countermeasures, including:

- The European Union **banned Russian media outlets** across member states to lessen the spread of propaganda.
- Some **digital platforms** have suspended advertising in Russia and Ukraine to prevent the monetisation of disinformation, and/or blocked Russian state media networks from their platforms entirely.
- Media outlets and non-profits have launched **fact-checking** initiatives to debunk false narratives and correct the record.
- Institutions like NATO have launched public awareness campaigns and published materials to **correct the record**.
- International bodies like the **German Marshall Fund, International Federation of Journalists**, and the **Global Forum for Media Development** have provided support to independent Ukrainian media outlets.
- Governments have taken legal action and imposed **sanctions** on individuals and organisations involved in the spread of disinformation.

The significance for Australia and the Indo-Pacific region

The geopolitical dynamics in the Indo-Pacific are complex due to its political, ideological, racial and geographic diversity, and as China seeks to exert regional dominance. Lessons from Russia show us that the Indo-Pacific is vulnerable to disinformation and cognitive warfare for two main reasons, both exacerbated by the rapid evolution of technology:

1. There is a new warfare playbook. Technological innovation and its applications evolve faster than governments can prepare for, leaving gaps in readiness.
2. The use of cognitive warfare, no matter where in the world, transcends borders and has global implications.

Russia's actions in Ukraine demonstrate how information operations can be used to legitimise unlawful and unprovoked acts of war, undermine a nation's sovereignty, and erode public trust in institutions.

Cognitive warfare can serve as a precursor or component to broader military or geopolitical strategies, and democracies are particularly vulnerable due to their open information environments and commitment to upholding the right to free speech. As regional tensions grow, and contestation in the South China Sea and South Pacific intensify, the Indo-Pacific region must adapt to an escalation in the use and sophistication of cognitive warfare tactics.

Russia's use of disinformation and cognitive warfare has also impacted Ukrainian diaspora communities in Australia and the Indo-Pacific. By spreading narratives that erode Ukrainian identity and undermine the legitimacy of Ukraine's sovereignty, Russia's campaigns can isolate and create disunity within diaspora communities.

Alliances and security partnerships, in particular AUKUS, the Quad and the Australia-United States alliance, may also be targeted by campaigns aimed at undermining trust and cohesion. For example, Chinese-backed media has been consistently critical of the AUKUS arrangement, with biased and misleading messaging that it undermines regional peace and security amplified across Southeast Asia.⁵ Such campaigns are designed to exploit regional sensitivities and undermine coordinated security efforts.

How Australia is responding to disinformation and cognitive warfare

The Australian government is taking a multipronged approach to address the geostrategic, social and democratic impacts of disinformation and cognitive warfare, through both domestic initiatives and international collaborations.

SOME OF THESE INITIATIVES INCLUDE:

- ▶ Legislative actions, such as the recently introduced *Communications Legislation Amendment (Combatting Misinformation and Disinformation) Bill 2024*.
- ▶ Regulatory oversight, such as the Australian Communications and Media Authority's oversight of the *Australian Code of Practice for Disinformation and Misinformation*.
- ▶ Public awareness and education, including the government's parliamentary *inquiry into civics education, engagement, and participation in Australia*.
- ▶ Strengthening democratic resilience through the establishment of the '*Strengthening Democracy Taskforce*', within the Department of Home Affairs.
- ▶ Alliances and partnerships, including by joining international partners to *publicly attribute malicious disinformation campaigns*.
- ▶ Research and development, including significant research investment through the *Defence Science and Technology Group*.
- ▶ Global statements and commitments, such as its commitment to the *Global declaration on information integrity online*.

Endnotes

- 1 Sun Tzu (2010), *The Art of War*, Capstone Classics, Chichester, England: Capstone Publishing
- 2 E.A. Kotelenets and V.V. Barabash (2019), 'Propaganda and Information Warfare in Contemporary World: Definition Problems, Instruments and Historical Context', *Proceedings of the International Conference on Man-Power-Law-Governance: Interdisciplinary Approaches*
- 3 Paulo Fernando Viegas Nunes (1999), 'The Impact of New Technologies in the Military Arena: Information Warfare', Air University, <https://www.airuniversity.af.edu/Portals/10/ASPJ/journals/Chronicles/nunes.pdf>
- 4 Annamaria Sarbu and Gavrilas Anca (2023), 'Using Artificial Intelligence Tools for Obtaining Cognitive Warfare Advantages', *The Defence Horizon Journal*, <https://tdhj.org/blog/post/artificial-intelligence-cognitive-warfare-twitter/>
- 5 Euan Graham, et. al. (2024), 'Joining the battle for the narrative: the case for AUKUS public diplomacy', Australian Strategic Policy Institute, <https://www.aspistrategist.org.au/joining-the-battle-for-the-narrative-the-case-for-aukus-public-diplomacy/>

About the Perth USAsia Centre

The Perth USAsia Centre is a leading think tank focused on Indo-Pacific strategy. Through our research and educational activities, we strengthen relationships and strategic thinking between Australia, the Indo-Pacific, and the United States. Based at the University of Western Australia, we are a non-partisan and not-for profit institution. We engage thought leaders across government, business, and academia to address challenges and opportunities in the Indo-Pacific region. Since the Centre's inception in 2013, we have informed a broad and diverse community of over 30,000 at more than 800 events across 25 cities in 10 countries.

For more information, contact us via perthusasiacentre@uwa.edu.au

Disclaimer

This publication is designed to provide accurate and authoritative information in relation to the subject matter covered. It is provided on the understanding that the publisher is not engaged in rendering any form of professional or other advice or services. No person should rely on the contents of this publication without first obtaining advice from a qualified professional individual or agency.

© Perth USAsia Centre 2025

This publication is subject to copyright. Except as permitted under the Copyright Act 1968, no part of it may in any form or by any means (electronic, mechanical, microcopying, photocopying, recording or otherwise) be reproduced, stored in a retrieval system or transmitted without prior written permission. Enquiries should be addressed to the publisher. Notwithstanding the above, educational Institutions (including schools, independent colleges, universities, and TAFEs) are granted permission to make copies of copyrighted works strictly for educational purposes without explicit permission from the Perth USAsia Centre and free of charge.



perthusasia.edu.au



M265, 3rd Floor, Old Economics Building, The University of Western Australia, 35 Stirling Highway, Crawley WA 6009, Australia



@ perthusasiacentre@uwa.edu.au
X @PerthUSAsia
f PerthUSAsia
in linkedin.com/company/perth-usasia-centre
perthusasia.edu.au
@perthusasiacentre