Australian National University

National Security College
POLICY **OPTIONS** PAPER
NO 15, OCTOBER 2020

The Strategic Implications of Manipulative Digital Platforms: A Trust-Driven Approach

Zac Rogers

Key points

- Consumer-facing digital platforms are components of a manipulative regime of technologies, designed to monitor and modify people's behaviours and preferences.
- These platforms are widely exploited by domestic and foreign actors for commercial, political and strategic ends.
- Foreign adversaries also benefit from the social and political vulnerabilities the normal daily use of these technologies exacerbate within democracies. Manipulative technologies can weaken public trust in institutions and deplete the social capital which upholds our convention-based society.
- Trust – as the bedrock of a convention-based society – has become a key battleground between states. It should be understood and protected as a strategic resource.

Policy recommendations

- National security agencies should pay close attention to the security consequences of manipulative technologies, and play a stronger supporting role in policy development led by other portfolios – for example, competition and consumer protection, industrial design, technology standard setting, public education, and media policy.
- Agencies should prioritise, with dedicated resources, strategic engagement across all relevant portfolios on the use and governance of digital technologies, including flow on impacts on trust.

Australia's strategic environment is rapidly changing. The most measurable changes are shifts in the regional balance of power and intensifying competition for influence in the Indo-Pacific. These developments have been complicated and exacerbated by the uncertainty generated by the presidency of Donald Trump, and most recently by unpredictable but not unexpected events such as COVID-19.

Yet in many ways, shifting power balances based on conflicting interests between geopolitical actors – and unpredictable events – are the normal cycles of international politics. Less obvious (but arguably of greater concern) are fundamental technology-driven changes in how power flows among networks of actors and institutions, and how conflicting interests are contested and mediated in a disrupted information environment.

The strategic environment

Four key features of Australia's evolving strategic environment are:[1]

1. a shift from vertical to horizontal networks of power
2. the pervasiveness of manipulation and cognitive uncertainty
3. erosion of trust in social, political, and economic institutions
4. the normalisation of constant and unrestricted political competition.

Shifting power structures

Corporate actors have achieved monopolies of control over flows of information, and have established new networks of horizontal power in which the role of the state is unclear and contested. The activities of corporations with global, profit-making agendas are also often at odds with states' strategic interests.

Technology companies develop products which are intended to monitor and alter consumer behaviour and preferences. Digital platforms predict and manipulate user behaviour in order to offer greater certainty in advertising outcomes. They do this by aggregating and analysing huge amounts of consumer data (both inside and outside of their own platforms) and via algorithmically-driven news feeds which serve users with the content that will affect them most.

The notorious Cambridge Analytica case – where Facebook users' data was used to build psychological profiles for political advertising – is the tip of an expanding iceberg. Data-driven public relations and advertising, for economic and political actors, is a growing business.

Moreover, the ad tech and data broker ecosystems that operate at the back-end of these consumer-facing platforms are a largely unregulated and borderless tangle.[2] As a result, consumer data is effectively frictionless. It can end up anywhere, in any hands.

Importantly, digital technologies are manipulative by design. This is a condition that shapes the information environment and exists *before, during, and after* they are exploited by malign actors for political or geopolitical ends.

For digital platforms subject to the control of foreign governments, such as TikTok, the manipulative architecture provides unique opportunities for censorship and propaganda. However, all platforms, regardless of country of origin, can be 'gamed' for political gain.[3]

Cognitive uncertainty

State and non-state actors alike now exploit and manipulate information for commercial, political, and strategic effect. As a consequence, the ability of the body politic to form knowledge and understanding out of a growing ocean of data and information is increasingly challenged. This has been highlighted recently with the rapid, global spread of dangerous COVID-19-related health disinformation and conspiracy theories.

At the same time, companies and governments increasingly offload cognitive tasks to algorithmic machines for the purported efficiency and accuracy on offer. A growing body of scholarship, however, urges caution.[4] These interventions create disruptions in the very architecture of knowledge itself. They risk undermining the cognitive basis of authority, legitimacy and trust in democratic institutions.

Erosion of trust

An item of faith for many in the technology sector is that tools optimised for economic efficiency are a net positive for society. However, the needs of people are not exhausted by the efficiency-centric model to which much digital technology has so far been directed. An emerging body of scholarship suggests that ubiquitous digital use has exacerbated negative social trends such as anti-social behaviour, depression, addiction and loneliness.[5]

Moreover, manipulative digital technologies exacerbate declining levels of institutional and social trust in liberal democracies. Australia already faces multiple trust-related headwinds: trust in traditional sectors like banking and finance, the media, religious organisations, politicians and governments is fragile and declining.[6]

Manipulative technologies degrade the *capacity for societal mediation* of distrust by weakening the convention-base on which those mediations rely. Digital manipulation is algorithmically-driven to optimise consumption patterns, putting it at odds with the often messy, inefficient, but necessary work of civil society within a democracy.

This is particularly concerning, since trust is a strategic and economic asset for 'high trust' societies like Australia. When people are able to trust one another at a distance – that is, beyond the bounds of heredity and coercion – society accrues numerous economic and governance efficiencies not available to 'low trust' societies.[7]

Foreign adversaries recognise the importance of trust to liberal democracies and pursue strategies designed to undermine it. For example, Russian disinformation routinely seeks to reduce public trust in democratic institutions, expert information and objective 'truth', as well as trust between democratic governments.

Constant, unrestricted warfare

The breakdown of internationally-recognised norms of state behaviour established after WWII has coincided with the emergence of manipulative digital technologies. Australia's competitors and adversaries embrace below-the-threshold competition, particularly via non-kinetic and non-lethal means. Unrestricted competition is now a constant between and across whole societies.[8]

As a result, we have transitioned to an era in which people and states contend with each other in ways that blur traditional lines of demarcation between, for example, foreign policy and citizens' everyday lives, and between security issues and economic and social policy.

Technology and strategy in open societies

Since at least the Cold War, strategists have assumed that the commercial development of digital technologies would be to the strategic advantage of the United States and its allies. Such technologies would be 'dual-use' – delivering benefits to western militaries and economies.[9] Moreover, it was widely assumed that features such as openness, transparency, a commitment to the rule-of-law, and free market competition would see these advantages uniquely accrue to liberal democracies.

However, at best, the development and subsequent democratisation of dual-use technologies delivered a radical levelling effect,[10] and at worst, a relative advantage to asymmetric competitors. Further, strategic competitors have learnt to leverage the vulnerabilities exposed in open societies by the *normal daily use* of manipulative digital technologies. Using existing digital platforms and tools, malign activities can be commenced in a way that is low cost and low risk, and at the time and place of the adversary's choosing.

New collaborations and horizons for national security agencies

The national security community in Australia and its allies and partners are coming to terms with this reality. For example, awareness of foreign interference activities has grown in Australia. This is a welcome development – but discussions related to espionage, bribery, and malign interference address only part of the challenge for an open society in the digital age. In particular, it leaves out of focus the broader questions raised in this paper: namely, how Australia's orientation to the development and deployment of technologies, which present unanticipated negative strategic consequences, should be reassessed.

Australia has also made steps to address the end-user impacts of technology, for example via the government's response to the 2019 Digital Platforms Inquiry by the Australian Competition and Consumer Commission. However, legislative and regulatory reform must be coordinated with civil society and industry buy-in, and community, family, and individual-level awareness-raising. Domestic policy needs to be aligned with foreign affairs and national security matters, such as Department of Foreign Affairs and Trade led work on standards-setting and regional-capacity building, as well as influence building and soft power.

At the same time, domestic policy related to data and the digital economy, developing for example via AustCyber's 2020 Digital Trust Report,[11] the 2020 Cyber Security Strategy,[12] and the use by government of citizen-facing digital tools (from health data apps, such as COVIDSafe, to welfare and tax-related tools), must incorporate an expanded awareness of the broader techno-social and techno-political environment. Malicious code and malicious actors are rightly at the forefront of Australia's national security response to digital challenges, but these threats do not exhaust matters of strategic concern.

As recognised in the 2019 Independent Review of the Australian Public Service, governments face rising pressure to provide citizens with services comparable in efficiency to the offerings of digital giants such as Apple and Google. Governments will need to carefully manage these expectations, and the temptation to use data and algorithms in ways that are manipulative, deplete trust or provide opportunities for foreign interference.

Deepening whole-of-society engagement

One way to better align often disparate lines of effort across government would be to create specialist strategic engagement roles. These positions would be charged with building relationships and collaborations across portfolios responsible for policy issues related to digital platforms. They would be resourced to liaise across portfolios on an ongoing basis – not only during consultation processes on specific policy issues.

Given the role of citizens as the primary users of manipulative digital technologies, strategic engagement specialists could also seek to foster engagement from the bottom-up, expanding the sense of stakeholdership in national security. They could cultivate networks across civil society, academia, industry, communities, and individuals through strategic outreach.

Prioritising trust-building

Trust – between governments and citizens, and among economic and social actors – is a vital strategic and economic advantage for liberal democracies such as Australia.[13] The essential ingredient of these conventions is relational trust – the type of socially-based trust people afford each other and institutions voluntarily, and which is often referred to as 'social capital'.

Regulating digital platforms to ensure that trust is maintained should be a priority for government. Similarly, government policies related to the digital economy and the government's own use of platforms and data must assiduously defend trust. This must go beyond a narrow conception of 'trust' as relating to the need for tools to be reliable and efficient – in effect, operational confidence.

Trust needs to be considered from a multi-dimensional perspective: ensuring that people are treated as more than the sum of their digital parts; minimising privacy intrusions and surveillance; maximising accountability and transparency related to data use and algorithmic performance.

All of these things can help mitigate the dark side of today's pervasively manipulative digital ecosystem, and help move towards a better one in the long term. Critically, it will also help close off opportunities for foreign adversaries to exploit, manipulate or subvert commercial and government data and digital platforms.

Notes

1. E. Bienvenue & Z. Rogers, "Strategic Army: Developing Trust in the Shifting Strategic Landscape," *Joint Force Quarterly* 95 (2019).
2. S. Wodinsky, "It Doesn't Matter Who Owns TikTok," Gizmodo Australia, August 6, 2020.
3. Explored as a fictional vignette by J. Wilhelm, "Autopsy of a Future War," Modern War Institute, November 2019.
4. J. Packer & J. Reeves, *Killer Apps: War, Media, Machine* (2020); P. Mirowski & E.M. Nik-Khah, The Knowledge We Have Lost in Information: *The History of Information in Modern Economics* (2017).
5. D.T. Courtwright, *The Age of Addiction: How Bad Habits Became Big Business* (2019).
6. https://www.edelman.com/research?f%5B0%5D=research_listing_tag%3ATrust%20Barometer.
7. F. Fukuyama, *Trust: The Social Virtues and the Creation of Prosperity* (1996).
8. M.J. Mazarr et al., "The Emerging Risk of Virtual Societal Warfare: Social Manipulation in a Changing Information Environment" (RAND Corporation, 2019).
9. L. Weiss, *America Inc.?: Innovation and Enterprise in the National Security State* (2014).
10. J. Giordano, J. Defranco & L.R. Bremseth, "Radical Leveling and Emerging Technologies as Tools of Non-Kinetic Mass Disruption," Strategic Multilayer Assessment (NSI Inc, 2020).
11. https://www.austcyber.com/resource/digitaltrustreport2020.
12. https://www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-strategy-2020.pdf.
13. E. Bienvenue, Z. Rogers & S. Troath, "Trust as a Strategic Resource for the Defence of Australia," *The Cove* (blog), October 2018.

About the author

Dr Zac Rogers is Research Lead at the Jeff Bleich Centre for the US Alliance in Digital Technology, Security, and Governance at Flinders University of South Australia.

Series editor

Katherine Mansted is senior adviser for public policy at the National Security College.

About this publication

Policy Options Papers offer short, evidence-based and forward-looking insights and recommendations for policymakers on topical national security issues facing Australia. Every paper in the series is informed by consultation, and reviewed by practitioner and academic experts.

About the National Security College

The National Security College is a joint initiative of The Australian National University and Commonwealth Government. The NSC offers specialist graduate studies, professional and executive education, futures analysis, and a national platform for trusted and independent policy dialogue.

T +61 2 6125 1219
E national.security.college@anu.edu.au
W nsc.anu.edu.au
@NSC_ANU
National Security College
CRICOS Provider #00120C