Australian National University

National Security College
POLICY **OPTIONS** PAPER
NO 13, DECEMBER 2019

Activating People Power to Counter Foreign Interference and Coercion

Katherine Mansted

Key points

- Citizens are increasingly frontline actors in Australia's security challenges: as targets of malign interference and coercion, victims of collateral damage, and agents of national resilience.
- Advances in information and communications technologies have made Australian society unprecedentedly porous and provided adversaries with potent tools for interference and coercion.
- Counter interference and coercion measures will affect citizens' interests as consumers, business owners and internet users. To ensure law and policy is appropriately calibrated, and accepted by the public as necessary and legitimate, citizens must be included in national security policy debate.
- Intelligence-sharing and public attribution can deter adversaries from malign activities targeting the social realm by piercing the veil of 'plausible deniability' that makes these tactics appealing.

Policy recommendations

- Agencies should boost national security literacy via a more proactive dialogue with information gatekeepers in the media, academia and civil society.
- Agencies should spread awareness of the political warfare 'playbooks' of foreign states to enhance the public's ability to identify and expose malign activities, and to inoculate citizens to their effects.
- Working with like-minded international partners, the Government should develop a publicly available, principles-based framework for attributing malign activities to foreign states.

Australia needs a new national security paradigm that recognises the centrality of the social realm. As strategist Kori Schake reminds us, societies—not militaries—fight wars.[1] The popular will is key to whether a country chooses to contest an adversary, capitulate, or negotiate peace. The social realm is also vital terrain during conditions of strategic competition.

Today, Australia faces a complex and increasingly fraught security environment. Authoritarian governments like Russia and China pursue 'political warfare' strategies that view democratic institutions, public opinion and civilian infrastructure as legitimate targets. Technology change has also made Australia unprecedentedly porous to these tactics.

The social centre of gravity

Since at least the end of WWII, Australians have enjoyed the luxury of being able to draw clear lines between domestic society and the arena of international competition and conflict. We are not unique. Western nations have professionalised the national security apparatus: most now only field all-volunteer armed forces; domestic security agencies remain secretive and distant from society; and policy and doctrine emphasise the distinction between combatants and non-combatants, and between military and civilian infrastructure. These factors prime decision-makers to see the policy and practice of security as separate and distinct from domestic politics and society.

However, the social realm has always been a decisive battleground in interstate conflict and competition. Moreover, throughout history, advances in technology have tended to close the distance between national security matters and citizens—temporally and geographically. For example, industrial technologies made 20th century civilians easier targets of mass propaganda and coercive operations, typified by British and German aerial bombing campaigns during WWII. The North Vietnamese exploited mass broadcast technology: while a tactical victory for America, the Tet Offensive projected graphic imagery across American living rooms and depleted public support for the Vietnam War, setting the conditions for strategic defeat.

The social realm in the digital age

Today, the social realm is unprecedentedly contested, and technology has increased the variety and effectiveness of the tools states use to target citizens. The digitisation of most social and economic activities allows states to interfere and coerce at scale and with immediacy. Of course, the social realm's centrality to security is not just a function of technology. China's United Front work, for example, extensively uses 'analogue' interference activities such as manipulating political and social organisations and targeting diaspora communities. While they do not rely on digital tools, these activities can be enhanced by technology. Four trends merit further discussion.

Access and reach

Previously, adversaries could only reach into the social realm through relatively imprecise and expensive means. 20th century propaganda often relied on centralised mass broadcast infrastructure. However, automated online tools enable adversaries to engage with entire populations, while advances in natural language processing may enable computers to 'autopilot' sophisticated propaganda campaigns.[2] Digital platforms subject to the directions of foreign powers, such as WeChat, act as closed tunnels into Australian society, enabling foreign governments to engage in extraterritorial propaganda and censorship. These platforms can also be plugged into foreign government 'digital incentive' ecosystems, epitomised by China's social credit system, designed to effect behaviour change through surveillance, rewards and punishment.

Targeting

Traditionally, adversaries lacked the technology and evidence to segment populations and customise operations for salient subgroups. However, mass collection of private data by companies and governments, together with advances in machine learning, has created new opportunities for micro-targeted interference and coercion. The Cambridge Analytica scandal is an early example of how data analytics can be used to profile individuals based on personality traits, political preferences and identity characteristics. Machines are also getting better at predicting human behaviour and the outcomes of complex social interactions, enhancing states' ability to operate effectively in the social realm. These advances will not just guide cyber interference and sabotage, but may be used to better target analogue activities like infiltration of political groups and blackmail of decision-makers.

Feedback loops

Previously, adversaries seeking to target the social realm lacked reliable mechanisms to test the effectiveness of their operations and to justify their value to decision-makers. However, machine learning systems, such as those routinely used by advertisers and digital platforms, can create real-time feedback mechanisms to assess the effects of operations and to refine them over time. This reduces the risk and uncertainty associated with operations in the social realm, increasing the likelihood that their incidence will increase.

Obfuscation and plausible deniabilty

Previously, coercive operations targeting the social realm tended to be overt. Populations would know they had suffered a physical attack, or were subject to a siege or blockade, and could identify that a hostile actor was responsible (even if their identity or nationality was not immediately known). As a result, these operations could backfire by calcifying public will against the

attacker. Similarly, while interference efforts such as black or grey propaganda often attempted to obfuscate their origin or purpose, the digital environment makes detecting, understanding, and attributing responsibility for interference significantly more difficult. There is also often a time lag between an operation occurring and its effects materialising.

This 'unseen' nature of cyberspace makes covert and plausibly deniable activities the norm, rather than the exception. Cyber-enabled interference and coercive attacks appeal to adversaries because they can be used to destabilise society, sow dissent, or paralyse political processes.[3] By hiding behind a veil of plausible deniability or engaging in deceptive 'false flag' attacks, adversaries maximise confusion and mistrust caused by their actions.

Imagine a destructive cyber-attack against an Australian electricity network. At first, it might not even be clear whether the incident is an accident or an attack. The attacker might plausibly deny involvement, exacerbating public confusion and disorder. Instead of becoming mobilised against an external threat actor, Australians might blame government or the infrastructure provider. This could undermine support for and participation in government recovery efforts, and deplete government resources and attention for responding to other security threats.

Building resilience in the social realm

An increasingly targeted citizenry will be more resilient to interference and coercion if it is informed. Resilience does not just let Australians bounce back from attack; it can affect adversaries' decision-making by reducing the benefits they expect to receive by targeting Australian people and institutions.

An inclusive national security conversation

National security has traditionally been an 'elite' and cloistered domain; but citizens need to be engaged as key stakeholders. Security policy increasingly affects citizens' choices as consumers, their assessment of business and personal risk, and how they use online platforms. Citizens must be a far greater part of the national security conversation to ensure they support decisions and feel the policy process is legitimate and justified. This is especially so in cases where citizens' short-term interests will be impacted to safeguard against unseen risks that, while real and high magnitude, might never materialise. One way to broaden the conversation is for agencies to proactively brief information gatekeepers such as opposition and backbench politicians, academics and journalists.

Boost national security literacy

If there is to be an inclusive national conversation, it must be an informed one. Agencies should build public awareness of foreign states' political warfare 'playbooks' and educate the public about the features and security implications of critical technologies like 5G and AI. This can activate one of democracy's key advantages: its ability to mobilise a whole-of-society approach to managing security risk, and to responding to interference and coercion.

The US interagency Active Measures Working Group, which operated during the Cold War, is one model. Considered to have been effective at blunting the impact of disinformation, the AMWG published unclassified reports cataloguing Soviet malign activity and conducted national and overseas roadshows to educate officials, journalists and academics about Soviet tools and tactics. The European Centre of Excellence for Countering Hybrid Threats, an intergovernmental think tank, is another model. While member states supply funding and governance, the Centre publishes a range of academic and practitioner perspectives on political warfare trends and the activities of Russia and China.

Ensure agencies remain trusted and credible sources of infomation

Much national security risk in the digital age is contingent and may never materialise. For example, the decision to exclude certain vendors from 5G infrastructure was not based on a 'smoking gun' but on future risk: that access to the network could enable interference or coercion. Further, the facts about disinformation, cyber-sabotage and other operations in the social realm will be contested: agencies must act now to bolster their credibility. In particular, while Australia has robust procedures for crisis communications, agencies must develop more proactive ways to publicly explain and motivate risk assessments *before* an incident occurs. If they are to be trusted, communications from government should be consistent and personalised. One positive step in this regard is the increased public presence of Australia's spy chiefs.

To further build trust, the Office of National Intelligence should consider ways in which the intelligence community can publicly share key assessments and associated confidence levels, without compromising sources or methods. One example of this approach is the Office of the US Director of National Intelligence's guidance on the

processes involved in making 'attribution' assessments for state cyber-attacks. Significantly, when providing advice to Ministers on whether and when to make information public, agencies should not limit their evaluation of the trade-offs involved to operational considerations such as the intelligence gain/loss trade-off. They must also weigh the longer-term impacts of secrecy on public trust and resilience.

Consistent, principles-based attribution

Working with like-minded partners, Australia should act to pierce the veil of plausible deniability that adversaries hide behind when engaging in interference, coercion and precursor activities. More frequent, principles-based attribution of responsibility for these activities can blunt their impact. It can position the Government as an 'honest broker' and minimise the confusion and mistrust engendered by future cyber-attacks and disinformation campaigns. Multilateral attribution statements can mitigate the risk that named states will retaliate with diplomatic or economic punishment, but are not always possible. Australia should accelerate efforts to develop common, public frameworks among like-mindeds for identifying and attributing malign activities. These can act as external benchmarks which support the legitimacy of attribution statements.

Society-centred deterrence

In the interwar period, airpower strategists theorised that a decisive airstrike on a target's civilian infrastructure would cause political paralysis and social chaos, leading "stricken civilians" to quickly demand that their government capitulate.[4] These theories were not evidence-based and reflected classist assumptions about the emotional susceptibility of the body politic. Although misguided, they inspired mass bombings of cities and untold human suffering.

Today, there is a need to ensure we do not give our adversaries the impression that people are Australia's soft underbelly. Showing that the Government trusts the public to engage in nuanced debate about the threat environment and response options is one way to do this. Similarly, establishing and signalling that we have processes for trusted government messaging about interference and coercion can reduce the perceived benefits to adversaries of targeting the social realm. This, in turn, can have a deterrence-by-denial effect, reducing the appeal of these tactics to adversaries.

Notes

1 *Civilians win wars, too,* August 2017, Hoover Institution.

2 E. Rosenbach & K. Mansted, *Can democracy survive in the information age?*, October 2018, Belfer Center for Science and International Affairs, Harvard Kennedy School.

3 J. Nye, *Is cyber the perfect weapon?*, July 2018, Project Syndicate.

4 L. Freedman, *The future of war: A history*, 2018.

About the author

Katherine Mansted is senior adviser for public policy at the National Security College, and a non-resident fellow at the Harvard Kennedy School's Belfer Center for Science and International Affairs.

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