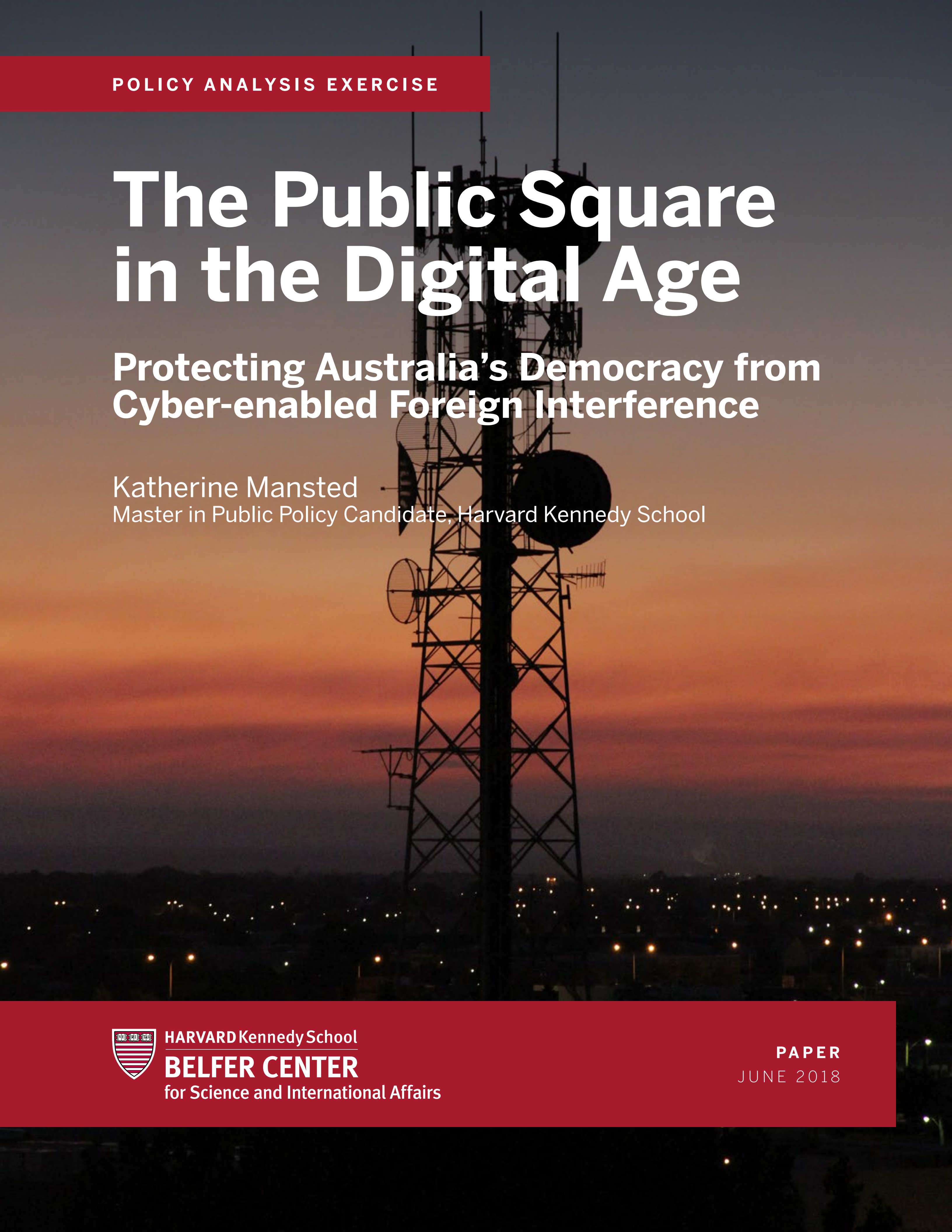
POLICY ANALYSIS EXERCISE



The Public Square in the Digital Age

Protecting Australia's Democracy from Cyber-enabled Foreign Interference

Katherine Mansted
Master in Public Policy Candidate, Harvard Kennedy School

HARVARD Kennedy School
BELFER CENTER
for Science and International Affairs

PAPER
JUNE 2018

Belfer Center for Science and International Affairs
Harvard Kennedy School
79 JFK Street
Cambridge, MA 02138

www.belfercenter.org

Statements and views expressed in this report are solely those of the author and do not imply endorsement by Harvard University, the Harvard Kennedy School, or the Belfer Center for Science and International Affairs.

This paper was completed as a Harvard Kennedy School Policy Analysis Exercise, a yearlong project for second-year Master in Public Policy candidates to work with real-world clients in crafting and presenting timely policy recommendations.

Design & layout by Andrew Facini

Cover photo: A cell tower over Perth, Australia, January 4, 2014. (Flickr User “Shari” / CC BY-NC-ND 2.0)

POLICY ANALYSIS EXERCISE

The Public Square in the Digital Age

Protecting Australia's Democracy from Cyber-enabled Foreign Interference

Katherine Manssted
Master in Public Policy Candidate, Harvard Kennedy School

HARVARD Kennedy School
BELFER CENTER
for Science and International Affairs

PAPER
JUNE 2018

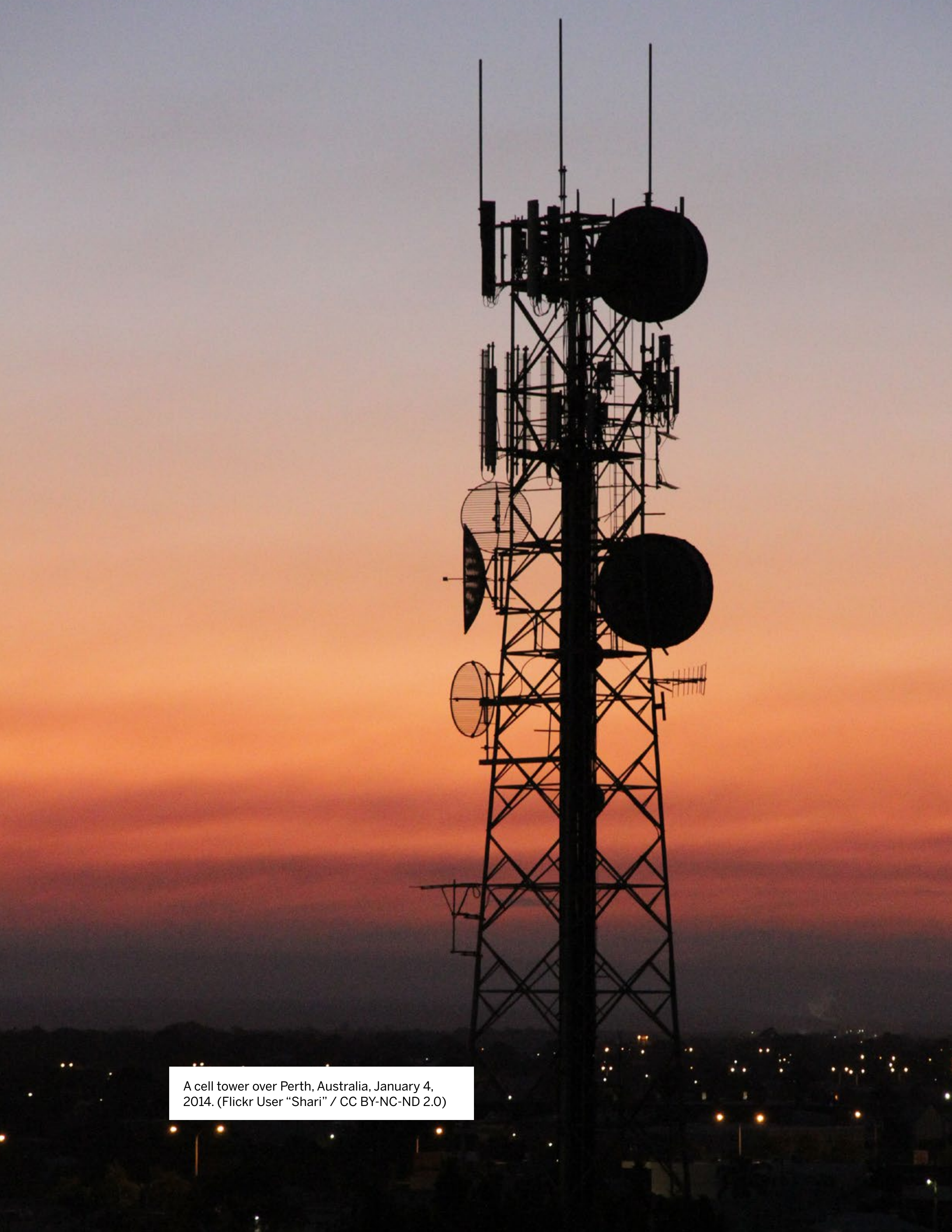
About the Author

Katherine Mansted is a Fellow at the Belfer Center, with a focus on emerging technologies and national security. She recently graduated with a Master in Public Policy from the Harvard Kennedy School. Previously, Katherine practiced as a lawyer in Australia, and has worked as an adviser to an Australian Cabinet Minister.

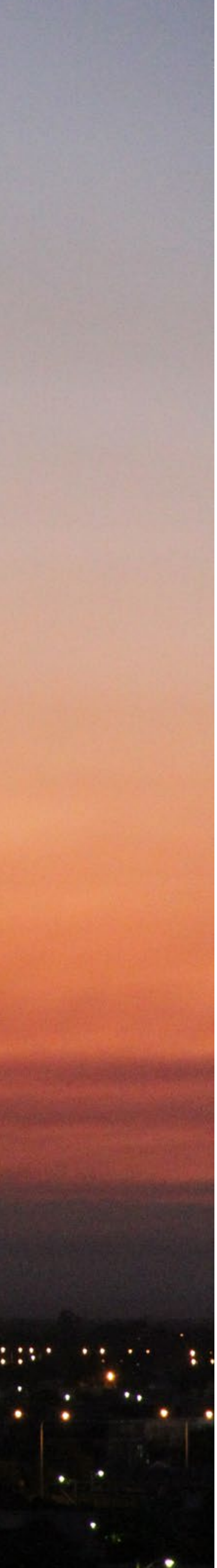
Acknowledgments

The author is deeply grateful to grateful to Eric Rosenbach, Jim Waldo, Michael Sulmeyer, and Matthew Bunn of the Harvard Kennedy School, and Danielle Cave of the Australian Strategic Policy Institute, for their comments and suggestions on earlier drafts. The views in this paper, and any errors, are the author's own.

Table of Contents



A cell tower over Perth, Australia, January 4, 2014. (Flickr User "Shari" / CC BY-NC-ND 2.0)



Executive summary

Australia faces a threat of foreign interference, greater than at any prior point in its history—even during the Cold War. This paper explores one component of this development: the threat of cyber-enabled interference operations. These operations—which this paper dubs CEI-OPS (pronounced *key-ops*)—are clandestine or deceptive in nature, and exploit digital technologies to undermine democratic, social, and market institutions. CEI-OPS are used by foreign powers to advance their national interest or foreign policy at the expense of Australia's sovereignty, and the inherent right of Australian citizens to choose their own future.

This paper addresses the question: how should Australia respond to the rising threat of CEI-OPS? While its focus is Australia, its findings and recommendations are intended to be relevant to a global audience. Australia has already been something of a 'canary in the coal mine' in putting the issue of foreign interference on the global agenda. Its geostrategic position—as a democracy in the middle of the increasingly volatile Indo-Pacific region—is likely to ensure it remains on the leading edge of the CEI-OPS threat.

Part 1 defines CEI-OPS, and distinguishes them from related activities like cyber operations, and military information operations. It also makes the normative case for why CEI-OPS are illegitimate.

Part 2 then provides a survey of the global threat landscape. It examines the technology and commercial trends that are likely to make CEI-OPS even more frequent and potent in the future. It explains why democracies are uniquely vulnerable to CEI-OPS, and why revisionist powers are increasingly willing and able to use "grey zone" capabilities like CEI-OPS. Part 2 then combines these insights to build out a taxonomy of the CEI-OPS tactics available to adversaries.

Part 3 homes in on two specific threat actors: Russia and China. It is only possible to respond to a threat by understanding the motivations and capabilities of potential adversaries. Part 3 concludes that China is most likely to use CEI-OPS against Australia to protect China's vital national interests—and in particular to protect the power and legitimacy of the Chinese Communist Party (CCP). There is also a risk that China could engage in CEI-OPS to reshape regional norms in its favor. China's existing cyber warfare and domestic propaganda capabilities provide it with the means to conduct CEI-OPS, and there is evidence that it is beginning to do so.

Part 4 then examines how Australia has so far responded to the CEI-OPS threat. It concludes that the response is not well-calibrated to the threat as defined in Part 1, and lacks an overarching, coherent strategy. Australia's response is also not responsive to the full breadth of CEI-OPS tactics, or to the motivations and capabilities of CEI-OPS adversaries explored in Parts 2 and 3. In particular, the response fails to address the fact that CEI-OPS affect society as a whole and are just as much a threat to individual rights, as they are to national security. If it continues to treat CEI-OPS as mostly either a counter-espionage, or technical cyber matter, Australia will be unable to sufficiently address the threat.

Part 5 recommends a framework for a better response. The overarching thread running through this Part is that a "whole-of-society" response is required to meet what is a whole-of-society threat. The unprecedented CEI-OPS threat demands that all elements of state power be brought to bear on the problem and—crucially—that civic power be mobilized. The foundation to coordinating Australia's response will be the development of a **National Counter Cyber-Enabled Interference Strategy.** The paper concludes with **15 recommendations grouped under four pillars** to inform this Strategy.

1. **Understand the threat.** Raising awareness of the CEI-OPS threat is a prerequisite for all other elements of the response but must be done without inciting fear about government censorship or racial prejudice. The Government should:

    - develop a CEI-OPS lexicon;

- educate the public about the nature of the threat;
- educate politicians about the nature of the threat;
- increase intelligence-sharing about CEI-OPS threats; and
- focus public discussion on Australia's vulnerabilities not on specific adversaries.

2. **Deter adversaries.** To reduce the incidence of CEI-OPS, Australia needs a deterrence strategy that alters the decision-making calculus of potential adversaries. The Government should:
   - pursue retaliatory counter-measures (but never engage in CEI-OPS);
   - respond to covert influence with overt counter-measures;
   - use cyber operations to disrupt and degrade CEI-OPS; and
   - support norms to constrain cyber attacks that may be precursors to CEI-OPS.
3. **Protect the public square.** To make CEI-OPS tactics less effective, Australia must reduce its attack surface. The Government should:
   - identify "critical public square infrastructure" and develop best practices for its protection;
   - develop a CEI-OPS "early warning" system; and
   - regulate social media companies to make their platforms less susceptible to CEI-OPS.
4. **Prepare the public for CEI-OPS.** Even if CEI-OPS are used against Australia, by building resilience, it can inoculate itself from their effect. The Government should:
   - ensure national media remains well-funded and independent;
   - consider creating a "special media forces"; and
   - introduce certification standards for audio-visual records.

Introduction

This paper addresses the question: how can Australia protect our public square from foreign interference in the digital age? More precisely, how can we protect the public square without undermining the very political principle—a free and open exchange of ideas—on which democracy rests?

Digital technologies have provided hostile actors with unprecedented tools and opportunity to undermine Australia's democratic, social, and market institutions. The cornerstone of all of these institutions is the public square. This is the place where ideas are put forward, debated, and where the best ones—economic, political, and cultural—triumph. It is how citizens inform themselves about policy, and who to trust to run the country.

However, Australia must prepare for its public square to come under unprecedented assault in coming years. The public square in the 21st century has several features, not present in previous eras, which make it particularly vulnerable: it is (i) digital; (ii) democratic; and (iii) central.

Public discourse today is overwhelmingly *digital*. Digital technologies make speech cheaper, and capable of spreading at a pace and scale previously unimaginable. Geography no longer limits participation. Australia's public square is a mouse click away for most citizens, but also from Beijing, Moscow, and Tehran.

The public square itself is increasingly *democratic*. Eighty-eight percent of Australians are active internet users.[1] Most citizens regularly access Wikipedia, blogs, and social media, and can engage in online debate on just about any subject. Public discourse is no longer the purview of an educated "elite." In the internet era, anyone can start a social revolution, go "viral," or otherwise enter the contest of ideas.

The public square is playing an increasingly *central* role in democracies' decisions. Political parties and governments, including in Australia, routinely use opinion polls and plebiscites to inform policy, while the 24/7

[1] "2018 Digital Report-Australia," We Are Social Australia, February 15, 2018, https://wearesocial.com/au/blog/2018/02/2018-digital-report-australia.

news cycle forces politicians and public servants to be hyper-responsive to public opinion. It is likely that this trend may deepen: think tanks, political parties, and technologists are increasingly championing the idea of "participative democracy," whereby citizens, not their representatives, determine policy.[2]

These three trends are coupled with a disturbing geopolitical reality. States—particularly those with authoritarian forms of government—are aggressively acquiring cyber capabilities and honing their abilities to acquire and shape information. They see control over information flows and manipulation of foreign opinion as vital tools of state power.

A tipping point in our awareness of how digital technologies have revolutionized foreign interference occurred in 2016. Russia's cyber-enabled interference in the American presidential election catapulted the vulnerabilities of the public square to the front-page of newspapers and the front-of-mind of national security practitioners the world over. The world's most powerful state was unable to prevent a foreign power from spreading disinformation to tens of millions of its citizens, manipulating public and media narratives, and exacerbating partisan fault-lines. Russia turned the United States' democratic political system, open public square, and technological superiority against itself, with deep—and as of yet, unquantified—impact. Russia's actions in 2016 are still, as of time of writing in June 2018, fueling political in-fighting, government dysfunction, and public uncertainty in the United States. This is a stark warning sign for Australia.

[2] See, for example, The Australian Greens, "Democracy," Policy Platform, accessed March 26, 2018, https://greens.org.au/policies/democracy; Samantha Grassle, "Digital Tools for Participatory Democracy," *The Governance Lab @ NYU* (blog), March 5, 2015, http://thegovlab.org/digital-tools-for-participatory-democracy/.

1. The threat

> *"The Government is concerned about growing attempts by foreign governments or their proxies to exert inappropriate influence on and to undermine Australia's sovereign institutions and decision-making. Such attempts at foreign interference are part of a wider global trend that has affected other democracies."*
>
> *— Australian Foreign Policy White Paper 2017*[3]

Democracies today face an unprecedented threat of foreign interference. This has been publicly recognized by governments in the United States[4] and in Australia.[5] Australia's domestic security agency, the Australian Security and Intelligence Organisation (ASIO) assesses that the scale and complexity of foreign interference activity outstrips even that experienced during the Cold War.[6] Both the United States and Australia have announced their intention to deter, or otherwise reduce, foreign interference in their domestic affairs. New laws, as well as changes to regulations, bureaucratic organization, and military doctrine are underway. However, to date, Australia's response has been slow, and fragmented. We are in good company. The United States' 2017 National Security Strategy lamented that "efforts to counter the exploitation of information by rivals have been tepid and fragmented" and hampered by a lack of "sustained focus" and "properly trained professionals."[7]

Concern about foreign interference is new to Australia's post-Cold War national security agenda. ASIO first publicly aired concerns about the rise

[3] "2017 Foreign Policy White Paper" (Canberra: Australian Government, Department of Foreign Affairs and Trade, November 23, 2017), 75, https://www.fpwhitepaper.gov.au/home.

[4] Jim Mattis, "Summary of the 2018 National Defense Strategy of the United States of America" (United States Department of Defense, January 19, 2018), 3, https://www.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf; "National Security Strategy of the United States of America" (Washington, D.C.: The White House, December 2017), 2–3, https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf.

[5] "ASIO Annual Report: 2016-17" (Canberra: Australian Government, Australian Security Intelligence Organisation, October 3, 2017), 45, https://www.asio.gov.au/asio-report-parliament.html. ("the scale of the [espionage and foreign interference] threat to Australia and its interests is unprecedented").

[6] Michael McGowan, "ASIO Says Threat to Australia Greater Now than in Cold War," *The Guardian*, January 31, 2018, http://www.theguardian.com/australia-news/2018/jan/31/asio-says-threat-to-australia-greater-now-than-in-cold-war.

[7] "National Security Strategy of the United States of America," 35.

of foreign interference in 2014.[8] From 2007 ASIO had been reporting a gradual rise in foreign espionage and interference activity, and reprioritization of its capability and resourcing towards this threat, in its annual reports.[9] The 2014-15 reporting year seemed to be a turning point: ASIO warned of a rise in scale and sophistication of hostile cyber activity against government and civilian systems.[10] Regardless, its priority focus—and public and political attention—remained on counter-terrorism efforts. Moreover, both public and government discussions about foreign interference tended to focus on use of cyber tools for espionage, or disruption of service, as well as more 'traditional' activities, such as coercion, intimidation, or bribery of specific targets, and insider threats.

Concern about foreign manipulation of public opinion is a more recent addition to the national security agenda. This concern has been elevated by twin catalysts. First, there was significant attention by the Australian media throughout 2017 on allegations that China has interfered in Australian politics, media organizations, and certain segments of the Australian population.[11] Second, Russia's interference in the 2016 US presidential election drew attention to the risk that adversaries might engage in cyber-enabled interference, and that elections are an attractive target. The October 2017 Australian International Cyber Strategy, for example, referred to the risk of "cyber-enabled influence operations during elections."[12]

However, Australia needs to widen its conversation about cyber-enabled foreign interference. While cyber-enabled interference operations timed

[8] AustralianPolitics.com, "ASIO Director-General David Irvine Addresses National Press Club," August 27, 2014, http://australianpolitics.com/2014/08/27/asio-director-general-david-irvine-addresses-the-national-press-club.html. See also "ASIO Annual Report: 2014-15" (Canberra: Australian Government, Australian Security Intelligence Organisation, October 15, 2015), 8, https://www.asio.gov.au/previous-reports-parliament.html. ("Foreign interference in Australia by foreign powers is pervasive. It spans community groups, business and social associations and is directed against all levels of Australian Government and the community.")

[9] In the 2006-7 reporting year, ASIO created a separate division for counter-espionage and foreign interference. It first referred to foreign interference as a "pervasive threat" to Australia in its 2011 report to Parliament. See "Previous Reports to Parliament," Australian Government, Australian Security Intelligence Organisation, 2017, https://www.asio.gov.au/previous-reports-parliament.html.

[10] "ASIO Annual Report: 2014-15" (Canberra: Australian Government, Australian Security Intelligence Organisation, October 15, 2015), 9, https://www.asio.gov.au/previous-reports-parliament.html.

[11] Christopher Knaus and Tom Phillips, "Turnbull Says Australia Will 'stand up' to China as Foreign Influence Row Heats Up," *The Guardian*, December 9, 2017, http://www.theguardian.com/australia-news/2017/dec/09/china-says-turnbulls-remarks-have-poisoned-the-atmosphere-of-relations.

[12] "Australia's International Cyber Engagement Strategy" (Canberra: Australian Government, Department of Foreign Affairs and Trade, October 2017), 5, 46, 65, http://dfat.gov.au/international-relations/themes/cyber-affairs/aices/index.html.

to coincide with national elections are particularly egregious, democratic decision-making processes, the integrity of our institutions, our economic competitiveness, and social cohesion can be subverted at any time in the political cycle. It was perhaps this broader scope of foreign cyber-enabled interference that Australia's inaugural Homeland Affairs Secretary was thinking about, when he referred in an October 2017 speech to the risk that foreign-sponsored "fake news" and "information subversion" could harm community cohesion, or fracture public discourse.[13] There are, however, few other instances when public officials have spoken about this risk, or how they think Australia might address it.

[13] Michael Koziol, "'Home Is Not What It Used to Be': Michael Pezzullo Justifies New Security Super-Ministry in Colourful Speech," *The Sydney Morning Herald*, October 17, 2017, https://www.smh.com.au/politics/federal/home-is-not-what-it-used-to-be-michael-pezzullo-justifies-new-security-superministry-in-colourful-speech-20171017-gz29hx.html.

1.1 Strategy and objectives of CEI-OPS

This paper addresses a specific sub-set of foreign interference activity—which I define as cyber-enabled interference operations (or CEI-OPS, pronounced *key-ops*). For the purposes of this paper, CEI-OPS are a sequence of clandestine or deceptive tactical actions that use digital technologies, and share a common purpose of changing, shaping, or constraining the actions of decision-makers.[14] Figure 1A defines each of these three purposes, and provides examples. For reasons explained in Part 2, CEI-OPS are largely used by states with centralized, authoritarian governments, against adversaries which are free market democracies. While many actors—both state and non-state—can make use of the tactics of CEI-OPS, this paper addresses use of CEI-OPS by states only.

Figure 1A. Strategic objectives of CEI-OPS

Objective	Example
Change. An operation that causes a state to change its policy to align with the political interests of the adversary.	Actor A influences large segments of the voting population in Actor B to believe that A is no longer their adversary, resulting in an official change to Actor B's foreign policy.
Shape. An operation that changes public perception, or shapes public narrative in a way that makes it more likely that decisions will be made in the adversary's interest.	Actor A influences segments of the under-18 population to believe that a version of history, favorable to Actor A's interests, is true, making these groups more receptive to Actor A's future advocacy efforts.
Constrain. An operation that does not intend to create any specific change in the target's policy, but causes confusion or delay in decision-making.	Actor A influences specific target groups in Actor B to believe that democracy is futile, or that the target state's institutions have no democratic legitimacy, which destabilizes Actor B's government.

CEI-OPS target public opinion (either of society-at-large, or particular groups such as minorities, key influencers, or political elites). This is because decisions in a free market, liberal democracy like Australia are informed by, and in some cases, directly reflect, public opinion. By influencing the public square, an

[14] This definition builds off the definition of an "operation" in Australian and US military doctrine, discussion of "foreign interference" in the 2017 Australian Foreign Policy White Paper, and the definition of "foreign interference" in section 4 of the *Australian Security Intelligence Organisation Act 1979* (Commonwealth).

adversary can influence the full spectrum of activities within a state: political decisions; social and cultural forces; and economic activity. Much has been written about the threat of CEI-OPS during elections.[15] However, CEI-OPS can be used to manipulate the public square at any point in the political lifecycle. A robust public square does not just allow citizens to inform themselves so that they can cast a rational vote in public elections. It is also fundamental to maintaining the rule of law—since public figures and officials can be held to account via public scrutiny and judgment. The public square also facilitates progress via debate and refinement of social and economic ideas.

In support of their overall strategic objective—that is, in order to successfully change, shape, or constrain their target's decision-making—adversaries using CEI-OPS will have at least one or more operational objectives. These objectives might be to:

- build, or undermine public support for certain values, causes, or people;[16]
- cause, or exacerbate domestic infighting and social disharmony; [17]
- generate mistrust in the target state's institutions, or in certain facts;
- damage the target's international reputation, or diplomatic or trade relations;[18]
- manipulate source documents or datasets from which history will be written, or policy made;[19]
- conceal information relevant to political or economic decisions that affect the adversary's interests.

[15] See, for example, Defending Digital Democracy Project, "The State and Local Election Cybersecurity Playbook" (Cambridge, Mass.: Belfer Center for Science and International Affairs, February 2018), https://www.belfercenter.org/publication/state-and-local-election-cybersecurity-playbook.

[16] "National Security Strategy of the United States of America" (Washington, D.C.: The White House, December 2017), 3, https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf ("Rival actors use propaganda and other means to try to discredit democracy [and to] advance anti-Western views.").

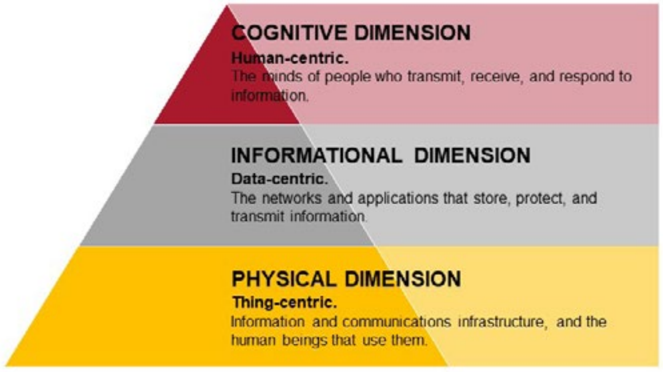
[17] "National Security Strategy of the United States of America," 3 ("[Rival actors] spread false information to create divisions among ourselves, our allies, and our partners.").

[18] "ASIO Annual Report: 2016-17" (Canberra: Australian Government, Australian Security Intelligence Organisation, October 3, 2017), 24, https://www.asio.gov.au/asio-report-parliament.html.

[19] "Statement of Glenn Tiffert, Visiting Fellow, Hoover Institution, The Long Arm of China: Exporting Authoritarianism with Chinese Characteristics" (2017), https://www.cecc.gov/events/hearings/the-long-arm-of-china-exporting-authoritarianism-with-chinese-characteristics.

In carrying out these operational objectives, CEI-OPS rely on digital systems and platforms, like the internet and social media. This enables the adversary to reach a mass audience with speed, scale and effect not possible with "analog" forms of interference, such as clandestine funding of political groups, or co-opting print media. CEI-OPS occur in what is referred to in military doctrine as the "information environment." This consists of three dimensions, as shown in Figure 1B. CEI-OPS target the third dimension—the cognitive dimension—or what Stanford Professor Herb Lin calls a state's "brain-space" (as distinct from cyberspace or physical space). An adversary can of course seek to interfere in national decisions by bribing, blackmailing, or even assassinating officials, without needing to change the target's actual opinions. CEI-OPS cuts out the friction between the adversary's intent and the target's decision, by causing targets to *change* their very beliefs, not just behaviors.

Figure 1B. Three dimensions of the information environment[1]


COGNITIVE DIMENSION
Human-centric.
The minds of people who transmit, receive, and respond to information.
INFORMATIONAL DIMENSION
Data-centric.
The networks and applications that store, protect, and transmit information.
PHYSICAL DIMENSION
Thing-centric.
Information and communications infrastructure, and the human beings that use them.

[1] Adapted from Chairman of the Joint Chiefs of Staff, *Joint Publication 3-13: Information Operations*, Updated 20 November 2014 (United States Military, 2012), I–3.

1.2 The need for a new term, 'CEI-OPS'

This paper is proposing a new term—CEI-OPS—because the terms currently used in policy and academic discussion about cyber-enabled interference are inconsistent and overly broad. Terms including information warfare; cyber warfare; information attacks; information operations; and psychological operations are interchangeably used to include activity I would label as CEI-OPS.[20] This impedes development of responses which are appropriate and adapted to the specific CEI-OPS threat. None of these terms make the cyber-enabled nature of CEI-OPS explicit, while some extend to acts which are overt, and legitimate. Herb Lin and Jackie Kerr, pioneering researchers in this area use the umbrella term "cyber-enabled information/influence warfare and manipulation" to include the actions I call CEI-OPS.[21] However, their concept includes a much broader array of activities—including overt acts, and actions targeted towards any of the three dimensions of the information environment. While these types of actions can be used in conjunction with CEI-OPS by a hostile actor, the CEI-OPS threat is sufficiently serious, and unique, to warrant its own category. Additionally, using the word 'interference,' rather than 'influence,' better captures the problem with CEI-OPS. All states agree that foreign interference is internationally wrongful (even if they do not agree on the definition of "interference").[22] Finally, the term CEI-OPS avoids the word 'warfare,' which implies equivalence to kinetic actions, and can therefore encourage inaction if applied to activities like CEI-OPS which are non-violent.

[20] See, for example, Susan Landau, "Cybersecurity: Time for a New Definition," *Lawfare*, January 12, 2018, https://www.lawfareblog.com/cybersecurity-time-new-definition; Jen Weedon, William Nuland, and Alex Stamos, "Information Operations and Facebook" (Facebook Security, April 27, 2017), 5, https://newsroom.fb.com/InfoOps (Information operations are "Actions taken by governments or organized non-state actors to distort domestic or foreign political sentiment, most frequently to achieve a strategic and/or geopolitical outcome.").

[21] Herbert Lin and Jaclyn Kerr, "On Cyber-Enabled Information/Influence Warfare and Manipulation" August 13, 2017, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3015680.

[22] Peter Mattis, "What We Talk About When We Talk About Chinese Communist Party Interference in the Public Square," *War on the Rocks*, March 7, 2018, https://warontherocks.com/2018/03/talk-talk-chinese-communist-party-interference-public-square/.

CEI-OPS are distinct from cyber operations

It is worth distinguishing cyber-*enabled* interference operations from cyber operations. There are four main differences: (i) target; (ii) objective; (iii) means; and (iv) quantifiability.

Target. Cyber operations exploit vulnerabilities in technology, whereas cyber-enabled information operations use technology to exploit people. Cyber operations target code, largely to achieve "real world" effects—like stealing data, disrupting machines, or destroying infrastructure. By contrast, CEI-OPS target something more inchoate: people's beliefs, and perceptions. In other words, CEI-OPS target the cognitive dimension of the information environment (see Figure 1B, above). They might exploit vulnerabilities in any of the three dimensions as means to this end, however it is in the cognitive dimension that their effects are achieved. By contrast, cyber operations primarily target the availability, integrity or confidentiality of systems and data within the informational dimension. Cyber operations can also target the physical dimension—consider, for example, North Korea's use of a cyber attack to destroy up to 75% of the servers of Sony Pictures Entertainment.[23] Cyber operations can also be used to achieve effects *outside* the information environment. For example, the United States and Israel allegedly used the Stuxnet cyber attack to target Iran's nuclear infrastructure.[24]

Objective. Cyber operations also tend to have a specific, limited objective. For example: theft of data from a particular network; disruption of a particular service; or destruction of a particular object. However, CEI-OPS can be continually deployed against an adversary, in order to progressively shape the adversary's information environment over time.

Means. The means used by cyber operations and CEI-OPS overlap but differ in important ways. Cyber operations exploit a technological vulnerability or error in code to compromise the integrity, availability, or

[23] Michael Cieply and Brooks Barnes, "Sony Cyberattack, First a Nuisance, Swiftly Grew Into a Firestorm," *The New York Times*, December 30, 2014, https://www.nytimes.com/2014/12/31/business/media/sony-attack-first-a-nuisance-swiftly-grew-into-a-firestorm-.html.

[24] Jack Goldsmith, "Richard Clarke Says Stuxnet Was a U.S. Operation," *Lawfare*, March 29, 2012, https://www.lawfareblog.com/richard-clarke-says-stuxnet-was-us-operation.

confidentiality of a system, or its data. CEI-OPS have a greater range of available means. As Figure 1C summarizes, they can use cyber attacks to achieve their operational objectives, but just as powerfully can also use technology in full compliance with what its code allows. That is, CEI-OPS can 'game' systems, rather than hacking them. While this may seem like an arcane distinction, it is important to devising responses which reduce the means, and opportunities, available to adversaries to conduct CEI-OPS.

Quantifiability. The nature and quantum of damage from CEI-OPS is very difficult to quantify—even more so than for cyber operations. For example, imagine that before an election, a voter registration roll is hacked, and entries altered, as part of a cyber operation. Through forensic analysis, cybersecurity experts will likely be able to determine which records were affected. Even if this is not possible, the damage will be bounded to the network that was penetrated. However, a CEI-OPS campaign which distributed false election-related 'memes' on social media is much harder to quantify. There is no way to measure the effects of words and images on people's brains.[25] Moreover, the number and identity of people affected is difficult to map.[26] Finally, CEI-OPS are often pursued with the long-game in mind. As ASIO notes in its 2017 report, foreign interference "is an insidious threat—activities that may appear relatively harmless today can have significant future consequences."[27]

[25] Informed by author's conversation with Professor Herb Lin on 19 December 2017.

[26] Idea informed by Jacqueline Van De Velde, "The Law of Cyber Interference in Elections," SSRN Scholarly Paper (Rochester, NY: Social Science Research Network, May 15, 2017), https://papers.ssrn.com/abstract=3043828.

[27] "ASIO Annual Report: 2016-17," 4.

Figure 1C. Three ways CEI-OPS may exploit digital technologies

Method	Example
Cyber attack. An actor exploits an error in code or takes advantage of a vulnerability in how a network is configured.	Actor X hacks into a politician's email account, and steals embarrassing, but private, correspondence, which they then leak online.
Misuse of digital technology. An actor 'games' code to produce an outcome that violates the use policy of a system or application.	Actor X creates a fake Facebook account that purports to belong to a politician. There is no cyber attack—Facebook is designed to allow people to create profiles. However, X has violated Facebook's use policy, which bans impersonation.
Gaming of digital technology. An actor 'games' code to produce an outcome that is not banned by the use policy of the system or application.	Actor X uses a network of Twitter 'bots' (automated accounts) to retweet a certain message. There is no cyber attack—Twitter is set up to allow users to retweet whatever they please. Additionally, Twitter's use policy does not does not ban the use of bots.

CEI-OPS are distinct from military information operations

A distinction must also be drawn between CEI-OPS and "information operations" (IO). Australian (and US) military doctrine permits IO to be used during authorized military operations,[28] in concert with other lines of operation. IO is a term that includes a very broad array of activities—including information assurance to safeguard Australia's own decision-making capacity, military deception to deliberately mislead adversary decision-makers, or disrupting an adversary's access to the physical or informational dimensions of the information environment.[29] IO can also include psychological operations (PSYOPS), which target the cognitive domain of a foreign target audience.[30] However, unlike CEI-OPS, PSYOPS will not always be covert. For example, Australia and the United States used PSYOPS to "win hearts and minds" of local populations in Afghanistan and Iraq, including by providing

[28] Note that "military operations" is not synonymous with wartime activities. There is a full range of military operations, extending from defense support of civil authorities through to large-scale combat operations.

[29] Chairman of the Joint Chiefs of Staff, *Joint Publication 3-13: Information Operations*, Updated 20 November 2014 (United States Military, 2012), II.3-II.13. Note, the author could not obtain an unclassified version of Australia's equivalent Defence Doctrine Publication (ADFP 3.13.1—*Information Operation Procedures*).

[30] "Australian Defence Doctrine Publication (ADDP) 3.13-Information Activities (Released under FOI 330/13/14)" (Australian Government, Department of Defence, November 6, 2013), 1–13, http://www.defence.gov.au/FOI/Docs/Disclosures/330_1314_Document.pdf.

aid to potentially hostile villages, and by dropping leaflets and broadcasting radio messages urging civilians to stay away from fighting.[31] Australia has also used cyber-enabled IO to counter ISIS propaganda and recruitment in the Philippines,[32] Iraq and Syria.[33] Again, however, this use of cyber tactics is clearly connected to an extant military operation, authorized under Australian domestic law and otherwise conducted in accordance with the laws of war.

1.3 **CEI-OPS are illegitimate**

It may seem intuitive that CEI-OPS are illegitimate, however it is worth identifying the implicit reasoning behind this assumption. This will help clarify why, and how, a democracy like Australia should counter CEI-OPS. CEI-OPS are illegitimate—at least from a normative perspective—and thus distinguishable from public diplomacy, information operations during wartime, or even espionage in peacetime. This is because CEI-OPS violate: (i) the universal right to self-determination; (ii) state sovereignty; and (iii) principles of necessity and distinction.

Universal rights. CEI-OPS violate the right of all peoples to self-determination—which is a foundational principle of international law, enshrined in Article 1 of the United Nations Charter.[34] Under the principle, the Australian people have an ongoing right to decide their system of government and future destiny, including the policies of law, culture, and economics by which they are governed.[35] CEI-OPS are inherently manipulative; and in this sense deprive people of autonomy to make these choices, and to self-determine.[36]

[31] "Australian Defence Doctrine Publication (ADDP) 3.13-Information Activities (Released under FOI 330/13/14)," 4–4.

[32] Charles Miranda, "Australian Defence Force Troops Deployed to Philippines to Fight Islamic State," *News.Com.Au*, October 24, 2017, http://www.news.com.au/national/australian-defence-force-troops-to-be-deployed-to-philippines-for-isis-fight/news-story/40efb7727938b842ee328a393ef8df68.

[33] Laura Tingle, "Australia Launches Cyber War against Islamic State," *Financial Review*, November 22, 2016, http://www.afr.com/news/politics/australia-launches-cyber-war-against-islamic-state-20161122-gsv4lg.

[34] United Nations, "Charter of the United Nations," 1 UNTS XVI (1945), art. 1.2.

[35] Antonio Cassese, *Self-Determination of Peoples: A Legal Reappraisal* (Cambridge University Press, 1995).

[36] A similar argument has been advanced by Jens David Ohlin, "Did Russian Cyber Interference in the 2016 Election Violate International Law," *Tex. L. Rev.* 95 (2017): 1579.

They are manipulative because they are undertaken covertly, to obscure the involvement of foreign governments, and aim to make people change their beliefs or perceptions in ways inconsistent with their baseline beliefs or perceptions.[37] This distinguishes CEI-OPS from legitimate, overt tools of influence, such as public diplomacy and private advocacy.[38] It is also why there is no moral equivalency between CEI-OPS and state-funded media—like Voice of America or China's Global Television Network, which are transparent about who they are acting on behalf of.[39] There is also no moral equivalency between CEI-OPS and democracy promotion programs, or even covert activities that support opposition groups inside authoritarian regimes. These lines of effort *advance* the right of self-determination, by promoting a system in which citizens will be free to make their own choices.[40]

Interference with a state's sovereign choices. There is a longstanding principle of international law that states should not intervene in the domestic affairs of other states. The International Court of Justice (ICJ) has opined that a state has the sovereign prerogative to choose its own political, economic, social, and cultural system, and to formulate its own foreign policy.[41] From a legal perspective, it is unlikely that anything but the most egregious instances of CEI-OPS could constitute an unlawful "intervention," as

[37] Anne Barnhill, "You're Too Smart to Be Manipulated by This Paper," in *Manipulation*, 2012, https://www.bgsu.edu/content/dam/BGSU/college-of-arts-and-sciences/philosophy/documents/conferences/2012/what-manipulation.pdf.

[38] "2017 Foreign Policy White Paper" (Canberra: Australian Government, Department of Foreign Affairs and Trade, November 23, 2017), 76, https://www.fpwhitepaper.gov.au/home.

[39] Mattis, "What We Talk About When We Talk About Chinese Communist Party Interference in the Public Square."

[40] It is sometimes argued that democracies do not have 'clean hands' when it comes to covert influence, and therefore should be circumspect about asserting that CEI-OPS are illegitimate. Particularly during the Cold War, the United States did use covert action to destabilize democratic regimes. However, evidence of historical illegitimate conduct is no justification for states today to act illegitimately. (For examples of US covert interference, see Ishaan Tharoor, "The Long History of the U.S. Interfering with Elections Elsewhere," *Washington Post*, October 13, 2016.)

[41] Case Concerning Military and Paramilitary Activities In and Against Nicaragua (Nicaragua v. United States of America), 1986 ICJ Reports 14 (International Court of Justice 1986), ¶205.

defined by the ICJ.[42] However, even if they do not meet the legal threshold for interference, CEI-OPS subvert a state's ability to make its own decisions, and in this sense are illegitimate from a normative perspective.

Lack of necessity and distinction. Unlike most other hostile activities, CEI-OPS are not limited to specific targets. This should be contrasted with actions that the Australian military takes within the information environment, which as discussed above are always in support of defined military objectives. Australia's partner militaries have conducted covert cyber operations not connected to any extant military conflict, such as the allegedly Israeli / US Stuxnet malware used to disrupt Iran's nuclear program. However, even Stuxnet was very limited in objective (it targeted Iran's Natanz nuclear facility) and impact (the code contained a 'self-destruct' timer) and damaged what would in wartime be considered a legitimate target (a nuclear enrichment plant is 'dual-use' infrastructure that could serve civilian or military purposes[43]). Stuxnet's code appeared to have been "governed by a team of Washington lawyers,"[44] with the laws of war in mind. CEI-OPS exhibit none of this restraint: they deliberately target citizens, and civilian institutions, and their impact is not limited, but inchoate and unquantifiable.

[42] The most frequently cited case on the non-intervention principle is the 1986 judgment in *Nicaragua v United States* 1986 ICJ Reports 14. There, the ICJ opined that for an intervention to be illegal, it must be accompanied by an element of "coercion." Some legal scholars have interpreted this element to mean that the intervention would need to involve a threat of an unlawful act, should the target state not behave in a particular way. CEI-OPS are not coercive in this sense; they merely seek to influence or persuade. Other scholars, most notably the authors of the *Tallinn Manual*, are of the view that in order to be coercive, an act need only "have the potential for compelling the target state to engage in an action that it would otherwise not take (or refrain from taking an action that it would otherwise take)." Even if this lower standard ultimately prevails, there would be significant evidentiary issues to overcome. Given the impact of CEI-OPS is inherently unquantifiable, and the near impossibility of establishing counterfactuals (i.e. what the target state would have done, absent the interference) proving that an operation succeeded in making the target state change its behavior seems a near-impossible task. See Jens David Ohlin, "Did Russian Cyber Interference in the 2016 Election Violate International Law," *Tex. L. Rev. 95* (2017): 1589; Michael N. Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 2nd ed. (Cambridge: Cambridge University Press, 2017), 319.

[43] International Committee of the Red Cross, "Customary IHL - Rule 8. Definition of Military Objectives," accessed March 16, 2018, https://ihl-databases.icrc.org/customary-ihl/eng/docs/v1_rul_rule8#Fn_2751A90D_00019.

[44] Jack Goldsmith, "Richard Clarke Says Stuxnet Was a U.S. Operation," *Lawfare*, March 29, 2012, https://www.lawfareblog.com/richard-clarke-says-stuxnet-was-us-operation.

2. The threat landscape

"We increasingly live in a digital 'glass house' that must be much better protected."

—Eric Rosenbach, former US Department of Defense "Cyber Czar"[45]

As technology advances and the public square becomes more digitally connected, the risk of CEI-OPS grows. Additionally, democracies' open and transparent information environments make them uniquely vulnerable to CEI-OPS. At the same time, authoritarian states are increasingly able and willing to use CEI-OPS since they provide a powerful asymmetric capability.

2.1 Technology is making CEI-OPS easier

Propaganda has been used as a tool of political influence for centuries, to shape public perception at home, and weaken enemy morale. Technological developments, including mass media and the capacity to deliver airborne leaflets, saw states deploy 'mass propaganda' during the 20th century's two world wars. During the Cold War, influence became increasingly covert, and psychological operations directed towards civilian targets became increasingly popular. Both the United States and the Soviet Union used clandestine support for subversives and insurgents, and other types of covert psychological operations, to influence public opinion and political outcomes.[46] The Cold War was, after all, as much a contest of ideologies as it was of world powers. The possibility for covert influence tactics to be coupled with exploitation of cyber technologies was flagged as early as 1995. In a landmark paper, Cyberwar and Netwar, two RAND Corporation analysts identified the prospect for a new "grand strategy level" conflict between states based on information. Netwar would "disrupt or damage"

[45] Eric Rosenbach, "Defending Digital Democracy: The Four Corners of Election Security," United States Senate Intelligence Committee, Hearing on Russian Interference in the 2016 US Elections (21 March 2018).

[46] Niall Ferguson, *Kissinger: The Idealist*, vol. 1 (New York: Penguin Books, 2016), 263–64.

what a target "knows or thinks it knows about itself and the world around it" by influencing public opinion. It would use a combination of:[47]

> diplomacy, propaganda and psychological campaigns, political and cultural subversion, deception of or interference with local media, infiltration of computer networks and databases, and efforts to promote dissident or opposition movements across computer networks.

CEI-OPS is a subset of what RAND Corporation imagined "netwar" would be—a new, technology-enabled manifestation of an ancient form of state competition.

CEI-OPS are helped by the design principles of computing and the internet

Figure 2A sets out seven technological forces which enable CEI-OPS. These seven forces stem from the design principles of computing and the internet—that is, how the technology *is,* rather than how it is *used* by people. How the internet is used today, for example by major internet companies, can also enable or constrain CEI-OPS. However, unlike the very design principles of technology, these patterns of use are less likely to persist into the future and are more susceptible of regulatory intervention. Think of it this way: it is easier to use regulation to influence the business model of a company (even if it is Facebook, or Google) than it is to re-design the internet from first principles. This distinction will become relevant when formulating a response to CEI-OPS. The forces outlined in Figure 2A are not mutually exclusive. It is in fact the interaction between them all that creates such a ripe environment for CEI-OPS.

[47] John Arquilla and David Ronfeldt, "Cyberwar and Netwar: New Modes, Old Concepts, of Conflict," RAND Review (RAND Corporation, Fall 1995), https://perma.cc/NNT3-C6U3.

Figure 2A. Seven technological forces enabling CEI-OPS

1 **Information abundance**

People, businesses and governments continue to migrate operations to the digital sphere. This increased connectivity leaves an indelible trail of 'digital breadcrumbs,' that it is more expensive to delete than to store indefinitely. Adversaries now have access to information that previously never would have existed in recorded form. They can access vast troves of information about target audiences to better target their campaigns.[1]

2 **Cyber insecurity**

No computer is perfectly secure, and insecurity is exacerbated by complexity. As work and life become more digitized, networks become more complex, and harder to secure. Additionally, as technologist Bruce Schneier has explained, cyber attack is generally easier than defense, since adversaries can choose the time and method of attack, whereas defenders must secure an ever-expanding attack surface against every type of attack.[2] This means that adversaries are not limited to using public domain information; they can use cyber attacks to access sensitive and confidential information that results from the information abundance described above.

3 **Decentralization**

The internet is a distributed, disintermediated network. The ability to broadcast is therefore also no longer limited to those with control of centralized, expensive broadcasting infrastructure (such as a state). The barriers to produce and consume information—including CEI-OPS material—are low, and influence is limited only "by one's ability to garner and distribute attention."[3] Information can also spread peer-to-peer; it does not need to pass through a gatekeeper who will assure its veracity.[4] These properties make CEI-OPS cheap, and hard to obstruct.

4 **Network effects**

The distributed nature of the internet lends itself to 'network effects,' whereby people engage in activity that maximizes the number of links they have to others. They congregate on social media platforms and in other online communities. These communities then act as 'watering holes' for adversaries seeking to distribute CEI-OPS material quickly, and widely.

5 **Identity non-verification**

The internet protocols that are baked into the architecture of the internet do not require users to authenticate who or where they are before they access or transmit data. Therefore, *users* of the internet cannot always verify the identity of who they are interacting with. While cybersecurity experts have become good at attributing online activity, this attribution usually occurs ex post facto, or by nation-states with sophisticated espionage capabilities. Given the speed at which content on the internet moves, CEI-OPS material could have already achieved its intended effect among users before an expert is able to expose it.

6 **Autonomous algorithms**

Autonomous algorithms exacerbate the problems of identity non-verification. These algorithms can be used to create 'bots,' programs which impersonate human users, and can deliver CEI-OPS messages rapidly and at unprecedented scale. Bots are cheap to program and run, and enable a single adversary to have outsize influence in the public domain. In effect, they provide adversaries with a virtual 'rent-a-crowd.'

7 **Artificial intelligence**

Advances in artificial intelligence (AI) over the next five years are likely to exacerbate the problems caused by cyber insecurity and autonomous algorithms.[5] First, machine learning (a subset of AI) enables adversaries to find trends and insights in the information-abundant online environment. They can use these insights to tailor messages to particular groups or even individuals to maximize the effectiveness of CEI-OPS campaigns.[6] Second, with AI-enabled advances in natural language processing, machines will become able to themselves create messages specifically targeted at those most susceptible to them. Adversaries will thus be able to take humans out of the loop, to produce even more cost effective, large-scale CEI-OPS campaigns. Third, AI is making forgeries of video and image content increasingly realistic and cheap.[7]

[1] "National Security Strategy of the United States of America" (Washington, D.C.: The White House, December 2017), 34, https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf.

[2] Bruce Schneier, "Click Here to Kill Everyone," Schneier on Security (blog), January 27, 2017, https://www.schneier.com/essays/archives/2017/01/click_here_to_kill_e.html.

[3] Zeynep Tufeki, "It's the (Democracy-Poisoning) Golden Age of Free Speech," Wired, January 16, 2018, https://www.wired.com/story/free-speech-issue-tech-turmoil-new-censorship/amp?__twitter_impression=true.

[4] "Australia's International Cyber Engagement Strategy" (Canberra: Australian Government, Department of Foreign Affairs and Trade, October 2017), 65, http://dfat.gov.au/international-relations/themes/cyber-affairs/aices/index.html ("the decentralized and largely unregulated nature of online conversations leaves democratic processes vulnerable to malicious interference.").

[5] Future of Humanity Institute et al., "The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation," February 2018, https://maliciousaireport.com/.

[6] "National Security Strategy of the United States of America," 34 ("[America's competitors] exploit marketing techniques to target individuals based upon their activities, interests, opinions, and values.").

[7] Future of Humanity Institute et al., "The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation."

CEI-OPS are also enabled by the business models of major internet companies

The business models of the powerful commercial entities that mediate much of the activity on the internet also enable CEI-OPS. Platforms like Twitter, Facebook, and YouTube follow a business model that: (i) derives profit from paid advertisements; and (ii) uses algorithms to maximize user attention, and thus profit. Their algorithms are optimized for engagement. That is, they are programmed to serve the content they predict will grab each user's attention most.[48] Researchers have found that these algorithms prioritize and promote controversial information, a property that can be exploited in CEI-OPS campaigns.[49] Algorithms that are optimized for engagement also produce social media "filter bubbles" and "echo chambers," which may exacerbate partisan divides, since users are only served with content that confirms their pre-existing views.[50] This feature can be exploited to maximize the effect of a CEI-OPS campaign. However, the way in which internet platforms choose to configure their algorithms are business decisions, and therefore may change in time. First, business strategy may change in response to public pressure, commercial forces, or government intervention. Second, there is nothing inevitable about today's most dominant platforms maintaining their prominence in the public square. Today's Facebook could be tomorrow's MySpace (the world's most popular social network until 2008, which had all but disappeared by 2011). [51] Indeed, Facebook's membership, and influence, may already have peaked.[52] The distinction between core features of technology, which underpin the forces in Figure 2A, and how businesses today choose to utilize those features is important when it comes to projecting which tools and tactics will be available to adversaries to conduct future CEI-OPS campaigns.

[48] Roger McNamee, "How to Fix Facebook—before It Fixes Us," *Washington Monthly*, March 2018, https://washingtonmonthly.com/magazine/january-february-march-2018/how-to-fix-facebook-before-it-fixes-us/.

[49] David Lazer et al., "The Science of Fake News" (Belfer Center for Science and International Affairs, March 8, 2018), https://www.belfercenter.org/publication/science-fake-news.

[50] Cass R. Sunstein, *#Republic: Divided Democracy in the Age of Social Media* (Princeton: Princeton University Press, 2017).

[51] Amy Lee, "Myspace Collapse: How the Social Network Fell Apart," *Huffington Post*, June 30, 2011, sec. Tech, https://www.huffingtonpost.com/2011/06/30/how-myspace-fell-apart_n_887853.html.

[52] Kurt Wagner and Rani Molla, "Facebook Lost Daily Active Users for the First Time Ever in the U.S. and Canada," *Recode*, January 31, 2018, https://www.recode.net/2018/1/31/16957122/facebook-daily-active-user-decline-us-canda-q4-earnings-2018.

2.2 **Democracies are uniquely vulnerable to CEI-OPS**

CEI-OPS turn the characteristics of democracy against itself. Three characteristics of a democracy's information environment render it significantly more vulnerable to CEI-OPS than an authoritarian state: (i) openness; (ii) rule-of-law decision-making; and (iii) pluralism.

Openness. Democracies are premised on the idea that information should be decentralized; information is primarily a tool for citizens to keep the government in check, rather than a tool for the state to control citizens. As a result, barriers to enter the digital public square in democracies are low. By contrast, authoritarian states tend to see information as a tool of the state and have long used censorship and propaganda to influence the discourse and beliefs of their own citizens. Democracies also guarantee to some extent—by law or political convention—free speech by citizens, and the operation of a free media. These protections, however, provide foreign actors with almost unfettered access to the modern democracy's public square. In the digital age, where communication is no longer geographically-constrained, authoritarian states are now able to incorporate tools they have long used domestically into their foreign policy.

Rule of law decision-making. Democracies are premised on the belief that making determinations between what is 'good' and 'bad' speech or determining what is 'truth' is not the role of the state, but rather should be adjudicated in the public square. At most, democracies will have some rules which proscribe extreme speech acts (like incitement to violence). However, CEI-OPS operate in the 'space between' lawful and unlawful activity. Therefore, unlike authoritarian states, democracies have few mechanisms to (a) identify; and (b) censor foreign interference material once it has entered the public square. Even if some laws existed which empowered the government to regulate foreign interference material, a democratic bureaucracy is ill-equipped to make a call about which content is impermissible. For example, a narrative promoted as part of a CEI-OPS campaign might not even have a foreign source or be untruthful. The narrative's falsity might come from the fact it is being "up-voted," despite being only a fringe view. By contrast, an authoritarian government can make one-off decisions based on arbitrary factors to more nimbly suppress CEI-OPS content.

Pluralism. The multi-party system within a democracy inevitably leads to political disagreements, polarization, and partisanship. CEI-OPS can amplify or otherwise exploit the divisions that naturally and inevitably surface in the public square, to achieve their operational objectives. The 24/7 news cycle also forces democratic politicians and public servants to be hyper-responsive to public opinion; a factor that increases the impact a CEI-OPS campaign can have. By contrast, decision-makers in authoritarian governments are less influenced by public opinion. Finally, a multi-party system can complicate exposing CEI-OPS: if a CEI-OPS campaign is exposed by actors connected to a particular party or movement, other actors may dispute the characterization, particularly if it is politically expedient to do so.

2.3 Adversaries are increasingly willing and able to conduct CEI-OPS

Authoritarian powers are developing grey zone capabilities

The rising use of CEI-OPS reflects a broader trend of states using 'grey zone' actions to advance their foreign policy.[53] Grey zone challenges sit in the 'space between' wartime and peacetime. Revisionist powers like China and Russia, and smaller states like Iran and North Korea, have embraced grey zone tactics because it gives them an asymmetric advantage over the United States and its security partners—which maintain conventional military superiority. The Soviet Union heavily used grey zone tactics during the Cold War. However, the world is now experiencing a second flourishing of grey zone tactics; they are being used with renewed intensity and by a

[53] A related but distinct concept is "hybrid warfare," which combines grey zone tactics with conventional military action. See Zack Cooper and Andrew Shearer, "Thinking Clearly about China's Layered Indo-Pacific Strategy," *Bulletin of the Atomic Scientists* 73, no. 5 (September 3, 2017): 305–311, https://doi.org/10.1080/00963402.2017.1364005.

greater number of actors.[54] Grey zone actions, including CEI-OPS, share four characteristics that make them difficult for democracies to respond to. They are: (i) sub-escalatory; (ii) deniable; (iii) integrated; and (iv) gradual.

Sub-escalatory. Grey zone actions occur below escalatory thresholds that would justify a kinetic response. In democracies, military doctrine, government policy, and public opinion largely view the world in binary terms: states are either at peace, or at war.[55] Grey zone actions defy binary characterization. Accordingly, the available strategic options for responding to them tend to be either too militarized or too constrained, leading decision-makers to either choose an ineffective response, or fail to act. [56]

Deniable. Grey zone actions are meant to make definitive attribution of the responsible actor difficult. This is because they often involve non-state mercenaries, or covert components. While intelligence agencies may be able to identify the responsible state, they can struggle to make a public case for attribution without revealing sensitive sources and methods. This quality helps grey zone actions to elude traditional deterrence theory—because attribution is uncertain, there is no guarantee that the action will be met with retaliation.[57]

Integrated. Grey zone actions tend to use multiple instruments of power simultaneously to achieve their objective, including economic, informational, intelligence, and legal aspects of power. This means they are far easier for authoritarian states to execute and defend against.[58] Authoritarian states have more unified control of the levers of state power. By contrast, democracies are generally more decentralized, and outsource more activities. Responses to grey zone challenges by democratic governments therefore require coordination across multiple agencies, several levels of government, and often with private sector actors.

[54] "National Security Strategy of the United States of America" (Washington, D.C.: The White House, December 2017), 3, https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf ("many actors have become skilled at operating below the threshold of military conflict—challenging the United States, our allies, and our partners with hostile actions cloaked in deniability.").

[55] "National Security Strategy of the United States of America," 28.

[56] "Shades of Grey: Neither War nor Peace," *The Economist*, January 27, 2018.

[57] Cooper and Shearer, "Thinking Clearly about China's Layered Indo-Pacific Strategy."

[58] "Shades of Grey: Neither War nor Peace."

Gradual. Grey zone actions edge towards their strategic objective over time. They aim to change the status quo gradually through a series of small tactical wins rather than making an "all-out grab."[59] In this sense, they achieve their objectives through 'a thousand cuts,' rather than a single sword thrust. This quality means that traditional deterrence theories may be inappropriate: by the time the target realizes that certain grey zone actions are adverse to its interests, it can no longer *deter*, but must *compel* the actor to stop. Compellence is harder than deterrence, in part because the target of compellence must change course (often visibly and embarrassingly), whereas the target of deterrence does not have to do anything.[60] The gradual nature of grey zone actions also makes it difficult for short-term-focused democratic governments to define and assess the threat, let alone build political will to respond to it.

States are seeking to acquire information power

The rise of CEI-OPS parallels the emergence of information power as a key form of national power, and increasingly contested domain of great power competition. In 2017, *The Economist* declared that data is the "new oil": the world's most significant geostrategic commodity.[61] Information power is the ability to use data, and the systems that transmit, process and store it, to influence the behavior or interests of other actors.[62] The 2017 US National Security Strategy devotes an entire chapter to "Information Statecraft," and labels Russia and China as being "determined" to control data to expand their influence.[63] China's President, Xi Jinping recently characterized the rivalry among major powers as "not just one for technology, but rivalry for ideology, for the power of discourse."[64] The growing strategic importance of data contributes to states' interest in using CEI-OPS to build information power to advance their interests.

[59] Michael J. Mazarr, "Struggle in the Gray Zone and World Order," *War on the Rocks*, December 22, 2015, https://warontherocks.com/2015/12/struggle-in-the-gray-zone-and-world-order/.

[60] Joshua Rovner, "Could Obama Have Stopped the Election Hack?," *War on the Rocks*, February 6, 2018, https://warontherocks.com/2018/02/obama-stopped-election-hack/.

[61] "The World's Most Valuable Resource," *The Economist*, May 6, 2017.

[62] Adapted from Joe Nye's famous definition of "power." See Joseph S. Nye, *The Future of Power*, 1st ed. (New York: PublicAffairs, 2011), 10.

[63] "National Security Strategy of the United States of America," 2.

[64] Quoted in Fergus Ryan, "Money Talks in China's Cloistered Internet," *The Strategist* (blog), December 15, 2017, https://www.aspistrategist.org.au/money-talks-in-chinas-cloistered-internet/.

States are increasingly prepared to engage in covert activities

In its 2017 annual report, ASIO revealed that it has identified “a number” of state and non-state actors conducting foreign interference activities against Australia.[65] ASIO’s Director for Counter-Espionage and Interference subsequently testified to a Parliamentary Committee that the diversity of foreign interference actors today makes responding more complex than during the Cold War period, when “adversaries were fairly readily identifiable.”[66] This general increase in covert activity may translate to an increase in CEI-OPS activity since, as a result of the drivers in Figure 2A above, CEI-OPS are cheap and have an outsized return on investment. Additionally, more and more states are developing capabilities to conduct cyber attacks.[67] This may also be the precursor to wider adoption of CEI-OPS tactics, since cyber capabilities can be repurposed to carry out many of the CEI-OPS tactics catalogued in Figure 2B, below.

[65] “ASIO Annual Report: 2016-17” (Canberra: Australian Government, Australian Security Intelligence Organisation, October 3, 2017), 4, https://www.asio.gov.au/asio-report-parliament.html.

[66] Michael McGowan, “ASIO Says Threat to Australia Greater Now than in Cold War,” *The Guardian*, January 31, 2018, http://www.theguardian.com/australia-news/2018/jan/31/asio-says-threat-to-australia-greater-now-than-in-cold-war.

[67] Dan Coates, “Worldwide Threat Assessment of the US Intelligence Community” (Office of the Director of National Intelligence, February 13, 2018), 5, https://www.dni.gov/index.php/newsroom/congressional-testimonies/item/1851-statement-for-the-record-worldwide-threat-assessment-of-the-us-intelligence-community.

2.4 **Taxonomy of CEI-OPS tactics**

Figure 2B catalogues the types of CEI-OPS tactics that states might employ. They are drawn from real examples of CEI-OPS tactics, and the preceding analysis of the technological and political trends that enable CEI-OPS and motivate adversaries to use them.

Figure 2B. CEI-OPS tactics

Category 1. Suppress authentic facts or opinion	
1A	**Explicit censorship** The adversary silences authentic facts or opinion by blocking content or users. Methods could include: deleting specific content, 'blacklisting' keywords or users, or taking down machines or entire networks via cyber attacks. For example, Russian hackers used a denial-of-service attack in 2007 to take down the presidential campaign website of Garry Kasparov and in 2011 did the same to opposition media outlets.[1]
1B	**Self-censorship** The adversary causes the target to silence themselves or to alter their views by imposing an "unbearable and disproportionate cost" on the act of speaking out.[2] Methods include: coordinating online harassment campaigns, or orchestrating "viral outrage" against the target.[3]
1C	**Reverse censorship** The adversary generates noise to 'drown out' authentic facts or opinion, either by concealing them entirely, or by diminishing their perceived popularity.[4] For example, during the 2012 Syrian Civil War, bots were used to amplify #Syria tweets about content that was Syria-related, like Syrian films, but irrelevant to the civil war.[5] This tactic is also called 'smoke-screening' or 'flooding.'
1D	**Decoy information** The adversary seeds decoy content into the information environment to distract from authentic facts or opinion. Decoy information is calculated to direct viewers away from certain content (as opposed to Reverse Censorship, which limits the reach of that content in the first place). For example, researchers found decoy tweets during the 2012 Syrian Civil War that were labelled with #Syria but linked to news about US Hurricane Sandy or civil unrest in Bahrain.[6]
Category 2. Exploit authentic facts or opinion	
2A	**Leak confidential information** The adversary leaks classified, confidential, or sensitive information about politically significant people or organizations. The adversary may have obtained this information via cyber attacks, inadvertent disclosure by the target, or by purchasing it from criminal actors. This tactic is also called 'doxing.'

2B	**Amplify minority views** The adversary amplifies content created by a legitimate person or organization to give the impression that this view or opinion has more support than it really does. Methods could include: using bots or human operatives to 'up-vote' fringe views, or actually hacking and altering information distribution algorithms so that they amplify this content.
Category 3. Create false or misleading facts or opinion	
3A	**Distribute new content** The adversary creates new false or misleading content and seeds it into the information environment. The adversary may then choose to amplify this content itself, or it simply may be shared by legitimate users. This tactic is also called 'astroturfing.'
3B	**Poison official records or datasets** The adversary uses cyber attacks to access official records or datasets and alter their content. For example, the adversary could change official maps so that officials and academics in the target state are more likely to accept its territorial claims. The adversary could alter official statistics to make certain groups within the target feel more marginalized. Alternatively, the adversary may simply choose to introduce errors into the records to obstruct or confuse decision-making, or to damage public confidence in the government.

[1] Andy Greenberg, "Everything We Know About Russia's Election-Hacking Playbook," *Wired*, June 9, 2017, https://www.wired.com/story/russia-election-hacking-playbook/.

[2] Zeynep Tufeki, "It's the (Democracy-Poisoning) Golden Age of Free Speech," *Wired*, January 16, 2018, https://www.wired.com/story/free-speech-issue-tech-turmoil-new-censorship/amp?__twitter_impression=true.

[3] Tufeki.

[4] Tim Wu, "Is the First Amendment Obsolete?" (Columbia University: Knight First Amendment Institute, 2017), https://knightcolumbia.org/content/tim-wu-first-amendment-obsolete; Tim Wu, "Blind Spot: The Attention Economy and the Law," *Antitrust Law Journal*, Forthcoming, March 26, 2017, https://papers.ssrn.com/abstract=2941094.

[5] Norah Abokhodair, Daisy Yoo, and David W. McDonald, "Dissecting a Social Botnet: Growth, Content and Influence in Twitter," in *Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing* (New York, 2015), 849, http://doi.acm.org/10.1145/2675133.2675208.

[6] Abokhodair, Yoo, and McDonald, 849.

3. Threat actors

> *"[Our] competitors weaponize information to attack the values and institutions that underpin free societies, while shielding themselves from outside information."*
>
> *— National Security Strategy of the United States 2017*[68]

The number of state and non-state actors which are able and willing to use CEI-OPS is likely to grow. This Part focusses on the state actors most able and likely to engage in CEI-OPS in the near term. Russia is currently the most sophisticated and frequent user of CEI-OPS; however, China is Australia's most significant CEI-OPS threat. This assessment is based on China's geostrategic significance to Australia, its historic use of non-cyber interference operations against Australia's interests, and its investment in cyber and other information technologies. This Part first examines Russia's use of CEI-OPS through the lens of a case study of Russia's interference in the 2016 US presidential campaign. It then examines China's interests and capabilities, to analyze which circumstances might prompt China to engage in CEI-OPS against Australia.

3.1 Russia

From at least 2014, Russia has been conducting CEI-OPS across the United States, Europe and the Baltics, and the Middle East. It is alleged to have used CEI-OPS to target elections in Italy, Germany, France, Ukraine, and the United Kingdom's Brexit referendum.[69] Its most significant campaign—unprecedented in variety, scope, and impact—targeted the 2016 US presidential election campaign. The strategic intent, tactics, and consequences of Russia's interference in American politics is essential to understanding how future CEI-OPS may be conducted—by Russia and others. However, as I am not the first to point out,[70] fixation on Russia's 2016 activities can also cloud strategic thinking and public understanding of the CEI-OPS threat. This is for three main reasons.

[68] "National Security Strategy of the United States of America," 34.

[69] Greenberg, "Everything We Know About Russia's Election-Hacking Playbook."

[70] Niall Ferguson, "Silicon Valley and the Threat to Democracy," *Daily Beast*, January 20, 2018, https://www.thedailybeast.com/social-media-shreds-the-social-fabric-one-click-at-a-time.

First, Russia is an adaptive opponent; it will learn from what was easiest, and most impactful in 2016. Second, while Russia's perceived success in influencing narratives about the US election may embolden other states to develop their CEI-OPS capabilities, there is no guarantee they will choose the same tactics as Russia. Third, CEI-OPS can be used to manipulate the public square at any point in the political lifecycle, not just during elections. Accordingly, Russia's use of CEI-OPS in 2016 should not be taken as the 'textbook' CEI-OPS operation; otherwise, any response risks being a 21st century Maginot Line: expensive, but soon obsolete.[71] To avoid this pitfall, after the Case Study below, I attempt to draw generalizable insights from Russia's 2016 campaign. The Case Study does not provide a detailed summary of Russia's activities since many exist elsewhere.[72]

Case Study: Russian CEI-OPS during the 2016 US presidential election	
Overview	Contrary to much media commentary, election systems were not 'hacked.'[1] Instead, Russia hacked people, and hijacked discourse in the public square, to shape, constrain, and possibly change US public perceptions and government decisions. Groundwork for the campaign commenced in 2014, with information gathering and research into social media groups related to US politics and social issues,[2] while actual acts of CEI-OPS began from 2016.[3]
Strategic objectives	Referring to the strategic objectives in Figure 1A, Russia's goal was to constrain US decision-making, by causing political confusion, infighting, and social discord. It also intended to shape US policy, by damaging the credibility of America's political system—both to citizens and foreign onlookers. It is also possible that Russia aimed to change US policy by influencing who was elected. Certainly, its CEI-OPS campaign supported some candidates—specifically Donald Trump and Bernie Sanders—and disparaged others, most notably Hillary Clinton.[4] However, it is unclear whether this bias was intended to result in President Trump's election (or even to reduce Clinton's expected margin of victory), or whether support for more polarizing candidates was intended to maximize political discord. It is also possible that Russia's objectives changed during the operation—and that once it became possible that then-candidate Trump could win, Russia's campaign re-orientated to support that possibility.

[71] Named for France's Minister of War and World War I veteran André Maginot, the Maginot Line along France's eastern land border took ten years to build and was impenetrable to German ground forces. However, in 1940, German forces—aided by improvements in tank technology—blitzed north through Belgium, the Netherlands, and Luxembourg, in an unexpected maneuver that bypassed the Maginot Line, while the Luftwaffe flew over it. France surrendered within two months. Instead of deterring a German attack, the Maginot Line "helped stimulate a new kind of war." (Stanley McChrystal, Tantum Collins, and David Silverman, *Team of Teams* (Penguin Publishing Group, 2015), 52.)

[72] See, for example, Robert S. Mueller, "United States of America v Internet Research Agency & Ors. Indictment by the Grand Jury for the District Court of Columbia." (Case 1:18-cr-00032-DLF, February 16, 2018).

Tactics	The Russian campaign used tactics from each of the categories in the taxonomy in Figure 2C. Tactics included: reverse censorship (tactic 1C); amplifying divisive, minority views (tactic 2B); and distributing false content (tactic 3A). These were primarily carried out by a highly-organized group of several hundred Russian operatives who used false social media pages and groups,[5] and online advertisements.[6] Russian operatives also leaked sensitive information (tactic 2A), obtained by hacking into the Democratic National Committee's networks.
Impact	As discussed in Part 1, the impacts of CEI-OPS are difficult to quantify. However, the campaign succeeded at: *Reaching a mass audience*. Facebook has indicated that up to 126 million Americans were touched by the campaign on its core platform and another 20 million on Instagram.[7] Buzzfeed reported in November 2016 that top "fake election news stories" generated more engagement on Facebook than top election stories from 19 major news outlets combined (although it is not known what proportion of these fake stories were part of Russia's campaign).[8] *Shaping public and political narratives in the public square*. Mainstream television networks and newspapers across the world have run hundreds of stories about interference in the election and in so doing unwittingly helped advance Russia's objectives of creating discord and distrust. There is significant ongoing media and political attention on criminal investigations,[9] and multiple US congressional inquiries,[10] into Russia's actions. US political elites remain bitterly divided over the consequences of Russia's campaign, the appropriateness of the US response, and the question whether there was collusion between the Trump campaign and Russia.[11] *Exacerbating political divides, and social discord*. Before the November 2016 election, Russian fake social media accounts orchestrated political rallies across the United States which supported then-candidate Trump, often by leveraging particular marginalized identity groups, such as Muslim Americans. After the election, fake accounts were used to orchestrate rallies both in support, and in protest, of the election result.[12]

[1] In a small number of US states, voter registration databases were accessed by Russia-affiliated hackers, however there is no evidence that these databases were modified in any way. Additionally, while Russia-affiliated hackers scanned at least 18 states' voting systems for vulnerabilities, there is no evidence that these were in fact successfully penetrated. See "Russian Targeting of Election Infrastructure During the 2016 Election: Summary of Initial Findings and Recommendations" (Washington, D.C.: United States Senate Intelligence Committee, May 8, 2018), https://www.intelligence.senate.gov/publications/russia-inquiry.

[2] Mueller, "United States of America v Internet Research Agency & Ors. Indictment by the Grand Jury for the District Court of Columbia.," para. 29.

[3] Mueller, para. 34.

[4] Mueller, paras. 6,43.

[5] Mueller, para. 4.

[6] Mueller, paras. 6, 10.

[7] Olivia Solon and Sabrina Siddiqui, "Russia-Backed Facebook Posts 'reached 126m Americans' during US Election," *The Guardian*, October 31, 2017, https://www.theguardian.com/technology/2017/oct/30/facebook-russia-fake-accounts-126-million.

[8] Craig Silverman, "This Analysis Shows How Viral Fake Election News Stories Outperformed Real News On Facebook," *BuzzFeed*, n.d., https://www.buzzfeed.com/craigsilverman/viral-fake-election-news-outperformed-real-news-on-facebook.

[9] See, for example, Michael S. Schmidt and Maggie Haberman, "Mueller Subpoenas Trump Organization, Demanding Documents About Russia," *The New York Times*, March 15, 2018, https://www.nytimes.com/2018/03/15/us/politics/trump-organization-subpoena-mueller-russia.html.

[10] CNN Library, "2016 Presidential Election Investigation Fast Facts," *CNN*, February 28, 2018, https://www.cnn.com/2017/10/12/us/2016-presidential-election-investigation-fast-facts/index.html.

[11] See, for example, Nicholas Fandos, "Despite Mueller's Push, House Republicans Declare No Evidence of Collusion," *The New York Times*, March 12, 2018, https://www.nytimes.com/2018/03/12/us/politics/house-intelligence-trump-russia.html; Diana Stancy Correll, "Devin Nunes Defends House Intelligence's Decision to End Russia Probe," *Washington Examiner*, March 16, 2018, https://www.washingtonexaminer.com/news/devin-nunes-defends-house-intelligences-decision-to-end-russia-probe.

[12] Mueller, paras. 51–57.

Generalizable insights from Russia's 2016 CEI-OPS campaign

Tactics will vary based on social and political factors on the ground. Russia's tactics were carefully adapted to the US political system, and cultural context. For example, they exploited partisan fault lines between Republicans and Democrats; polarizing issues including immigration and religion; and disparities between socio-economic and geographic identities.[73] They also exploited American race politics—which has long been a theme of Soviet / Russian propaganda against the United States.[74] To anticipate how states might conduct CEI-OPS against Australia, it will therefore be important to appreciate domestic conditions on the ground. In particular, existing social and political fissures, and perceived economic and social injustices, may provide material for exploitation.

Cheap, low-sophistication tactics can be powerful. Most of the tactics Russia used were enabled by activities that required only low technical sophistication. The hacks used to obtain, and then leak, sensitive documents from the Democratic National Committee were enabled by a mass spear-phishing campaign—a type of cyber attack that relies on human error, not sophisticated cyber tools. Moreover, not many of Russia's tactics even required Russia to find and exploit technology vulnerabilities. Instead, they mostly misused or gamed online platforms (see Figure 1D, above). Russia's tactics were also cheap: technology activists Tristan Harris and Roger McNamee hypothesize that the Russians were able to manipulate tens of millions of American voters for a sum less than it would take to buy an F-35 fighter jet.[75] Therefore, in modelling possible attack vectors for CEI-OPS, Australia should not only consider the impact of major cyber attacks, but should focus on the cumulative effects of low-level cyber incursions, or activity which simply takes advantage of opportunities presented by communications platforms.

[73] Mueller, paras. 33–34.

[74] Writing in the 1950s, race relations historian C. Vann Woodward noted that Russian propaganda has "long used stories of racial discrimination and injustice to discredit American capitalism and democracy." See C. Vann Woodward, *The Strange Career of Jim Crow* (New York: Oxford University Press, 1955), 131.

[75] Roger McNamee, "How to Fix Facebook—before It Fixes Us," *Washington Monthly*, March 2018, https://washingtonmonthly.com/magazine/january-february-march-2018/how-to-fix-facebook-before-it-fixes-us/.

Democratic governments and technology companies have a CEI-OPS blind spot. Prior to 2016, it was clear that the technological capability existed to engage in the actions that Russia did. For example, CEI-OPS tactics including reverse censorship and decoy information had been used by the Syrian Government in the Syrian Civil War in 2012,[76] while Facebook had specifically advertised its platform's ability to be used to alter voter's preferences.[77] Further, in the lead-up to the election, there was much discussion about the vulnerabilities of election systems to cyber attack[78]—demonstrating that there was awareness of Russia's willingness to disrupt political processes in the United States. Despite this, the CEI-OPS threat to the 2016 election was largely unanticipated by the media, government agencies, and technology and social media firms. This points up the difficulties democracies have in understanding and responding to CEI-OPS. We are playing doctrinal 'catch up.'

[76] Norah Abokhodair, Daisy Yoo, and David W. McDonald, "Dissecting a Social Botnet: Growth, Content and Influence in Twitter," in *Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing* (New York, 2015), 849, http://doi.acm.org/10.1145/2675133.2675208.

[77] Ashley Parker, "Facebook Expands in Politics, and Campaigns Find Much to Like," *The New York Times*, July 29, 2015, https://www.nytimes.com/2015/07/30/us/politics/facebook-expands-in-politics-and-campaigns-find-much-to-like.html.

[78] See, for example, Michael Sulmeyer and Ben Buchanan, "Hacking Chads: The Motivations, Threats, and Effects of Electoral Insecurity" (Belfer Center for Science and International Affairs, October 2016), https://www.belfercenter.org/publication/hacking-chads-motivations-threats-and-effects-electoral-insecurity.

3.2 **China**

Unlike Russia, China has not engaged in significant CEI-OPS activity. However, it is alleged to engage in extensive non-cyber-enabled interference activities. These include coercion, intimidation, and bribery of political and economic elites, tacit influence of traditional media companies, and intimidation of civil society and academia.[79] Instances of these 'analog' forms of interference have been documented in Europe, and the United States,[80] but states in the Asia-Pacific including Australia, New Zealand, and Singapore, have been most affected.[81] Therefore, it is reasonable to question whether, and to what extent, China might 'digitize' its foreign interference activities, and engage in CEI-OPS.

To evaluate the threat another state might present, it is necessary to assess two things: intent and capability. China is most likely to be motivated to engage in CEI-OPS when its vital interests are threatened, or perhaps if it perceives an opportunity to use CEI-OPS to advance other important national interests. Figure 3A presents a prioritized list of how China perceives its national interest, based on a review of translated Chinese official documents, and Chinese and Western academic analysis.[82] The rest of this Part then analyzes how these interests might encourage—or constrain—Chinese CEI-OPS.

[79] Thorsten Benner et al., "Authoritarian Advance: Responding to China's Growing Political Influence in Europe" (Berlin: Global Public Policy Institute, February 5, 2018), 11, http://www.gppi.net/publications/rising-powers/article/authoritarian-advance-responding-to-chinas-growing-political-influence-in-europe/.

[80] "The Long Arm of China: Exporting Authoritarianism with Chinese Characteristics" (2017), https://www.cecc.gov/events/hearings/the-long-arm-of-china-exporting-authoritarianism-with-chinese-characteristics.

[81] Benner et al., "Authoritarian Advance."

[82] Wang Jisi, "China's Search for a Grand Strategy: A Rising Power Finds Its Way," *Foreign Affairs*, April 2011; "Full Text of Xi Jinping's Report at 19th CPC National Congress," *China Daily*, November 4, 2017, http://www.chinadaily.com.cn/china/19thcpcnationalcongress/2017-11/04/content_34115212.htm.

Figure 3A. Chinese national interest

Vital interests	• Sustaining rule of the CCP • Maintaining internal economic development • Defending territorial integrity of existing borders (including ultimately regaining control of Taiwan)
Very important interests	• Enforcement of its expansive territorial claims in the East and South China Seas • Establishing preeminence in the Asia-Pacific region (and perhaps becoming a great power globally)

China may use CEI-OPS to defend its vital interests

Preserving the power of the CCP is arguably China's primary interest. Liberal values, including democracy, could delegitimize the CCP's one-party system of rule, while ideologies like selfdetermination could stoke secessionist elements in Tibet and China's Western provinces. Whereas most Western countries can address their security concerns through conventional hard power military and economic means, the CCP sees the "realm of ideas" as a major vector for instability—even existential security threats. When President Xi Jinping first came to power, a memo was distributed to senior party leaders referred to as "Document No.9." It listed seven "perils" to CCP leadership. The first was "Western constitutional democracy." Others included the promotion of "universal values" like human rights, media independence, and civic participation; pro-market "neo-liberalism;" and "nihilist" criticisms of the CCP's past.[83] Internet technologies have exacerbated China's concerns about the threat of ideas. China's 2017 Cybersecurity Strategy, for example, contained this bleak observation: "If our Party cannot traverse the hurdle represented by the internet, it cannot traverse the hurdle of remaining in power for the long term."[84]

[83] Chris Buckley, "China Takes Aim at Western Ideas," *The New York Times*, August 19, 2013, http://www.nytimes.com/2013/08/20/world/asia/chinas-new-leadership-takes-hard-line-in-secret-memo.html.

[84] Elsa Kania et al., "China's Strategic Thinking on Building Power in Cyberspace," New America, September 25, 2017, https://www.newamerica.org/cybersecurity-initiative/blog/chinas-strategic-thinking-building-power-cyberspace/.

Significantly, the CCP does not just fear that Chinese citizens will 'pull' destabilizing ideas from the internet but believes these are being actively 'pushed' by countries including the United States and Australia, in order to destabilize CCP rule. For example, former President Hu Jintao articulated his fear of a long-term foreign "strategic plot" of "westernizing and dividing" China.[85] This is not a baseless fear. Western governments have consistently advocated China's inclusion into global systems, on the underlying strategic assumption that 'engagement' will result in China becoming more liberal, and therefore more aligned with the West's interests.[86] Moreover, while Western governments may not see themselves as actively attempting to "westernize" China, this is because they do not need to: commercial and civil society actors play a strong role in disseminating ideas around the world, including in China.[87]

Up to this point, the CCP had predominantly protected itself from destabilizing ideas through a sophisticated domestic censorship apparatus, including the 'Great Firewall' system of blocking and filtering internet content. However, there is at least one known example of China using CEI-OPS tactics against foreign organizations and infrastructure to respond to an incident which threatened its ability to control its information environment. In 2015, Chinese hackers[88] launched a massive distributed denial-of-service attack against GitHub, the world's biggest repository for open source code, headquartered in the United States.[89] The attack, which made GitHub intermittently unresponsive for several days, targeted two GitHub pages which provided technology to subvert Chinese online censorship.[90] The attack indicates that China may no longer confine itself to defensively blocking content

[85] Edward Wong, "China's Leader Pushes Back at Lady Gaga and Western Culture," *The New York Times*, January 3, 2012, https://www.nytimes.com/2012/01/04/world/asia/chinas-president-pushes-back-against-western-culture.html.

[86] In 2017, the US National Security Strategy acknowledged that the US Government had pursued two decades of engagement-based foreign policy, based mostly on a "false" assumption that inclusion into international institutions and global commerce would turn revisionist powers including China into benign actors. ("National Security Strategy of the United States of America" (Washington, D.C.: The White House, December 2017), 3, https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf.)

[87] Weatherhead Center for International Affairs, "Hard Times for Soft Power: A Q&A with Joseph Nye," Harvard University, May 30, 2017, https://epicenter.wcfia.harvard.edu/blog/joseph-nye-qa.

[88] The hackers are widely believed to have been from China's Cyberspace Administration.

[89] Lorenzo Franceschi-Bicchierai, "China Is Behind DDoS Attack on GitHub, Activists Say," *Motherboard*, March 30, 2015, https://motherboard.vice.com/en_us/article/8qx7wz/china-is-behind-ddos-attack-on-github-activists-say.

[90] Bill Marczak et al., "China's Great Cannon" (Munk School of Global Affairs, University of Toronto: The Citizen Lab, April 10, 2015), https://citizenlab.ca/2015/04/chinas-great-cannon/.

within China; if it believes the content is damaging enough, it may use CEI-OPS to proactively suppress it at its overseas source.

It is also possible that if China's threat perception of the risk posed by the seven "perils" intensifies, the CCP could become more active in seeking to shape, or discredit, these ideas at their source. CEI-OPS would provide a vehicle to achieve this objective. Changes in threat perception could occur as a result of a general increase in strategic competition between states, external political movements (like an international human rights campaign), or by events within China (such as a domestic political or economic event that foments social unrest). Technological developments, such as of mechanisms that allow more Chinese citizens to bypass the Great Firewall, could also prompt a change in China's strategy.

It is also possible that, as China's power grows, it may become more willing to use CEI-OPS to proactively shape or discredit the seven "perils." China's efforts to bolster its hard power—economic, and military—are well-known. China has recently intensified its non-cyber methods of interference to discredit western liberal values, including by allegedly coercing and intimidating academics and publishing houses in Australia.[91] It is not unreasonable to expect that as its investment in hard power grows, so too will its investment in, and use of, CEI-OPS to provide an ideological vanguard to secure its political system.

However, China's likelihood to use CEI-OPS is also constrained by the CCP's focus on political security. For example, China will only engage in CEI-OPS to the extent that it believes the gains outweigh the risks of reprisals which could compromise its control over domestic propaganda and censorship. China is also a strong advocate of "cyber sovereignty"—the principle that states should enjoy exclusive jurisdiction and control over their information environment—as a global norm of internet governance.[92] China is therefore unlikely to engage in CEI-OPS if it perceives that doing so would undermine its ability to continue to build international support

[91] John Garnaut, "Our Universities Are a Frontline in China's Ideological Wars," *Australian Financial Review*, August 30, 2017, http://www.afr.com/opinion/columnists/our-universities-are-a-frontline-in-chinas-ideological-wars-20170830-gy74br.

[92] Jun Mai, "Xi Jinping Renews 'Cyber Sovereignty' Call at China's Top Meeting of Internet Minds," *South China Morning Post*, December 3, 2017, http://www.scmp.com/news/china/policies-politics/article/2122683/xi-jinping-renews-cyber-sovereignty-call-chinas-top.

for cyber sovereignty. China is therefore unlikely to engage in the type of widespread campaigns we see from Russia, which have broadly defined and possibly evolving strategic objectives and do not always conceal Russian involvement. It can be expected that if China engages in CEI-OPS it will be in support of clear objectives linked to China's national interest, and China will attempt to conceal its involvement.

China may use CEI-OPS to advance its regional influence

China's important interests may also motivate it to use CEI-OPS, including to: (i) support territorial expansionism; (ii) reshape regional norms; and (iii) increase China's power of attraction.

Territorial expansionism. China has already successfully used grey zone tactics to substantially progress its political and territorial agenda in East Asia without triggering a forceful international response.[93] Its territorial expansionism has also been accompanied by cyber intimidation. For example, in 2012, 19 Japanese websites were temporarily blocked or defaced with a Chinese flag, as tensions flared over the disputed Senkaku (Diaoyu) Islands.[94] In 2016, Chinese hackers allegedly took down Philippines government websites by denial-of-service attacks after a ruling by the United Nations Permanent Court of Arbitration on the South China Sea.[95] The Vietnam Airlines website was also taken down, and data on 400,000 of its passengers was leaked online.[96] This paper does not consider these actions to be true examples of CEI-OPS—since it is not clear they had as an objective to alter public opinion. They are more analogous to hard power intimidation tactics like 'buzzing' an airplane, used to signal a preparedness to respond with more force. Nonetheless, these incidents demonstrate

[93] Zack Cooper and Andrew Shearer, "Thinking Clearly about China's Layered Indo-Pacific Strategy," *Bulletin of the Atomic Scientists* 73, no. 5 (September 3, 2017): 305–311, https://doi.org/10.1080/00963402.2017.1364005.

[94] Bill Gertz, "U.S. Officials Say China behind Cyber Attacks on Japan," *Washington Free Beacon* (blog), September 25, 2012, http://freebeacon.com/politics/cyber-blitz/.

[95] Janvic Mateo, "68 Gov't Websites Attacked," *The Philippine Star*, July 16, 2016, https://www.philstar.com/headlines/2016/07/16/1603250/68-govt-websites-attacked.

[96] Charlie Osborne, "Chinese Hackers Take down Vietnam Airport Systems," ZDNet, August 1, 2016, http://www.zdnet.com/article/chinese-hackers-take-down-vietnam-airport-systems/.

that China is prepared to use cyber tools to advance its expansionist agenda.

Reshape norms. To become a regional superpower, China will need to reshape many of the rules of the international system, expand its influence in existing multilateral institutions, and create and advance its own regional institutions.[97] However, China does not wish to trigger a conventional military conflict while it is not the world's preeminent power. This makes grey zone actions, such as CEI-OPS, appealing to China as a means to progressively reshape regional norms and public perceptions, as well as existing alliance structures. In particular, it has been argued elsewhere that China seeks to weaken Australia's alliance with the United States,[98] and to curtail Australia's military access to and foreign relations with other Pacific powers.[99]

Power of attraction. The 19th Chinese Communist Party Congress report, China's most important public strategy document, states that by mid-century, China wants to be "a global leader" in "international influence."[100] However, despite increased spending on soft power over the last decade (averaging around US$10 billion per year—more than the budgetary allocations for soft power by the governments of the United States, United Kingdom, France, Germany, and Japan combined) China's soft power still languishes far behind that of its Western rivals.[101] China ranked 28th out of 30 in Portland's 2016 report on soft power.[102] Frustrated that investment in legitimate tools of soft power is not paying off, China is increasingly moving to embrace "sharp power" which, unlike soft power, centers on

[97] Eswar Prasad, "How China Aims to Limit the West's Global Influence," *The New York Times*, September 1, 2017, https://www.nytimes.com/2017/09/01/opinion/china-west-democracy.html.

[98] China's long-term goal is to urge a rethink of Australia's alliance with the United States.] http://www.abc.net.au/news/2016-09-01/asio-chief-sounded-alarm-about-donor-links-with-china-last-year/7804856.

[99] Dean Cheng, "Winning Without Fighting: Chinese Public Opinion Warfare and the Need for a Robust American Response" (The Heritage Foundation, November 26, 2012), https://www.heritage.org/asia/report/winning-without-fighting-chinese-public-opinion-warfare-and-the-need-robust-american.

[100] "Full Text of Xi Jinping's Report at 19th CPC National Congress," *China Daily*, November 4, 2017, http://www.chinadaily.com.cn/china/19thcpcnationalcongress/2017-11/04/content_34115212.htm.

[101] Martin Davidson, "China's Soft Power: A Comparative Failure or Secret Success," USC Center on Public Diplomacy, August 25, 2017, https://uscpublicdiplomacy.org/blog/chinas-soft-power-comparative-failure-or-secret-success.

[102] Davidson.

using information for the purposes of distraction, manipulation, and intimidation.[103]

However, China's willingness to engage in CEI-OPS to pursue these objectives could be constrained by public responses in the target population, and other countries' reactions. In 2017, a series of revelations of Chinese interference in Australia's domestic politics attracted significant negative media attention, and caused a dip in public support for China.[104] It also prompted a reversal in the Australian Government's rhetoric on China—previously focused on the importance of close economic ties with China, the Government became one of the most outspoken critics of China's foreign policy.[105] This response, or similar responses in other countries, may lead China to conclude that its interests are best served by using legitimate soft power tools to acquire influence.

China has the capability to engage in CEI-OPS

China's investment in controlling its own information environment, building its cyber capabilities and developing its own technological base provides it with the means to conduct CEI-OPS. Should China develop an intent to engage more widely in CEI-OPS, China has: (i) technical; and (ii) organizational capabilities that would allow it to do so.

Technical capabilities. China is one of the most sophisticated, and active state cyber actors.[106] China is responsible for a significant number of cyber attacks against Australian government and private sector entities, which have resulted in theft of data.[107] While currently China's focus is on using

[103] Christopher Walker and Jessica Ludwig, "The Meaning of Sharp Power: How Authoritarian States Project Influence," *Foreign Affairs*, November 16, 2017, https://www.foreignaffairs.com/articles/china/2017-11-16/meaning-sharp-power.

[104] Nick Bisley, "Mistrust of Australia Is Growing in China," *ABC News*, December 6, 2017, http://www.abc.net.au/news/2017-12-06/mistrust-of-australia-is-growing-in-china/9228664.

[105] Bisley.

[106] Dan Coates, "Worldwide Threat Assessment of the US Intelligence Community" (Office of the Director of National Intelligence, February 13, 2018), 5, https://www.dni.gov/index.php/newsroom/congressional-testimonies/item/1851-statement-for-the-record-worldwide-threat-assessment-of-the-us-intelligence-community.

[107] Matt Siegel, "China behind 'massive' Cyber-Attack on Australian Government: ABC," *Reuters*, December 2, 2015, https://www.reuters.com/article/us-australia-cybersecurity/china-behind-massive-cyber-attack-on-australian-government-abc-idUSKBN0TL08M20151202.

its cyber capabilities for espionage purposes, it could easily change its objectives, and redeploy national cyber capabilities to serve CEI-OPS campaigns. Moreover, China's espionage architecture, and the information it has already collected, could be repurposed for use in CEI-OPS campaigns. For example, it could choose to leak sensitive information it already has, use intelligence it has to better target a CEI-OPS campaign, or use access to systems to plant false information. China is also now the world's biggest investor in artificial intelligence[108] which, as Part 2 described, is one of the technological trends that could make CEI-OPS even more potent and prevalent. China's Great Firewall also enables China to execute CEI-OPS with a degree of impunity, since its control over its information environment means that China itself is not particularly vulnerable to CEI-OPS. The Great Firewall, a passive defensive system, can also be converted into what researchers have called the "Great Cannon," an offensive tool that can launch massive cyber attacks to shut down websites overseas[109], or inject new content.[110]

Organizational capabilities. In China, information is primarily viewed as a tool for state power. All of its main news organizations are state-run, and it is increasing its influence over domestic internet and technology firms.[111] Close ties and existing channels of communication between the CCP and media and communications organizations would assist China to coordinate a CEI-OPS campaign. China reportedly uses "content farms" to flood domestic channels of communication with pro-government material and to drown out negative stories; as use of Chinese social media platforms like WeChat increases outside China, especially among Mandarin-speaking populations, this will provide the CCP with a powerful vehicle for CEI-OPS.[112] Moreover, while much of China's government policy and military doctrine is not publicly available, its involvement in foreign interference

[108] Cade Metz, "As China Marches Forward on A.I., the White House Is Silent," *The New York Times*, February 12, 2018, https://www.nytimes.com/2018/02/12/technology/china-trump-artificial-intelligence.html.

[109] The "Great Cannon" was used to conduct the denial-of-service attack against GitHub, discussed above.

[110] Bill Marczak et al., "China's Great Cannon" (Munk School of Global Affairs, University of Toronto: The Citizen Lab, April 10, 2015), https://citizenlab.ca/2015/04/chinas-great-cannon/.

[111] Li Yuan, "Beijing Pushes for a Direct Hand in China's Big Tech Firms," *The Wall Street Journal*, October 11, 2017, https://www.wsj.com/articles/beijing-pushes-for-a-direct-hand-in-chinas-big-tech-firms-1507758314.

[112] Ying Yu Lin, "China's Hybrid Warfare and Taiwan," The Diplomat, January 13, 2018, https://thediplomat.com/2018/01/chinas-hybrid-warfare-and-taiwan/.

in Australia and elsewhere demonstrates that its officials have at least some level of training and experience to engage in covert influence. Unlike democracies, where covert influence is treated as an "exceptional" activity that needs special authorization and oversight, the CCP "approach[es] influence operations and active measures as a normal way of doing business."[113] This would provide it with a strategic advantage, should it decide to engage more widely in CEI-OPS.

[113] Peter Mattis, "Contrasting China's and Russia's Influence Operations," *War on the Rocks*, January 16, 2018, https://warontherocks.com/2018/01/contrasting-chinas-russias-influence-operations/.

4. Current response

Australia's current response to the CEI-OPS threat is inadequate. The main weakness in counter-CEI-OPS policy is that CEI-OPS are treated primarily as a domestic security issue, or technical cybersecurity issue. This ignores the fact that CEI-OPS is a whole-of-society threat that requires a whole-of-society response—including actions by multiple government departments, civil society, media, technology companies, and the public at large. Australia's current response does not clearly explain how Australia will coordinate diverse actors to successfully meet the CEI-OPS threat.

In assessing Australia's current response and formulating recommendations, I was guided by assumptions about Australia's national interest and core political principles, summarized in Figure 4A. Importantly, any response needs to address the fact that CEI-OPS is not just a security or foreign policy issue—it is also an issue of domestic rights. This follows from the analysis in Part 1, which concluded that the illegitimacy of CEI-OPS is based not just on the fact they violate sovereignty, but that they infringe an individual's right to determine their political future. Australia's CEI-OPS response must not just prevent CEI-OPS; it must also preserve free speech, free media, and other values essential to Australia's democracy.

Figure 4A. Criteria for assessing policy options

Security interests	• Reduces the frequency or severity of foreign cyber-enabled interference • Avoids provoking conflict escalation in the cyber and other domains • Avoids violating principles of international law, including sovereignty • Maintains productive diplomatic and trade relations with other states
Civic interests	• Protects Australians' right to determine their own political, economic, and cultural future • Upholds democratic values including free speech, a free media, freedom from discrimination, and due process • Avoids damaging the social fabric of Australia, for example by exacerbating social cleavages or political partisanship
Feasibility	• Technologically possible • Politically feasible, given the likely interests of major stakeholders • Operationally feasible, given the resources and capabilities reasonably available to the Government

4.1 **Absence of a coordinated information strategy**

Australia, like other democracies, remains unprepared for conflict and interstate competition in the Information Age, as a result of two decades of fragmented cyber and information strategy. As discussed in Part 2.1, RAND Corporation analysts flagged that cyber-enabled interference may become an increasingly potent form of interstate competition as early as 1995. Despite this, democracies have tended to focus on the national security implications of the physical and informational dimensions of the information environment, and have failed to consider ways in which the cognitive dimension may be threatened, or weaponized, as technology advances. In 1999, the same RAND analysts provided an assessment of the United States' "information strategy," which is applicable to the landscape in Australia at that time. They warned that national security practitioners were too focused on the "technological dimension" of cyberspace—that is, how to defend information infrastructures from attack, and how to use cyberspace for counteroffensive attacks.[114] But they were ignoring the "socio-political dimension"—that is, how information and ideas shape people's views. According to RAND, this second dimension had, however, garnered attention from political scientists, who saw digital technologies as an opportunity to promote democracy and constrain authoritarian regimes overseas.[115] Yet these political scientists remained blind to the strategic risk that adversaries might also exploit technology to advance their interests.[116] In words remarkably prescient of Russia's recent CEI-OPS campaigns, RAND cautioned that: [117]

> *While there has been much discussion about hackers taking down the Net, it is also the case that US perceptions may be 'hacked' by adversaries and manipulators who want the Net up, so they can air their pronouncements.*

[114] John Arquilla and David Ronfeldt, "The Emergence of Noopolitik" (RAND Corporation, 1999), 3, https://www.rand.org/pubs/monograph_reports/MR1033.html.

[115] Arquilla and Ronfeldt, 2.

[116] Arquilla and Ronfeldt, 4.

[117] Arquilla and Ronfeldt, 17.

The RAND study lamented that experts associated with each of the two dimensions remained "disparate, insular communities."[118] A unifying strategy was needed to bridge the two.

Unfortunately neither the United States nor Australia ever produced a unifying information strategy. Since 1999, the two dimensions have only diverged further. The national security community has focused on defending and securing systems, data, and infrastructure, and on using technical cyber tools for espionage, and to attack enemy systems and infrastructure. It has, however, maintained a blind spot about the risks of CEI-OPS. This is why—despite Russia testing many of the tools it used against the United States years earlier against Ukraine, and actors like the Syrian Government using CEI-OPS tools as early as 2012—pundits and officials were caught off guard by Russia's intervention in the US 2016 presidential election.

At the same time, the foreign policy community has continued to advance policies that in some cases *exacerbate* the CEI-OPS risk. One example of the divergence between the national security and foreign policy communities is Australia's foreign policy commitment to advancing an "open and free" internet, most recently reaffirmed in the 2017 Foreign Policy White Paper.[119] This policy seems to be based on the assumption that promoting internet freedoms overseas advances Australia's national interest. However, it is unclear whether this assumption has been properly tested. From a national security perspective, the policy could exacerbate the CEI-OPS risk—since, on the one hand, we ask adversaries not to interfere in our information environment, yet on the other hand we are actively supporting a policy which they would interpret as undermining their control over their information environment. Indeed, the tension between the security and foreign policy communities is increasingly evident. Australia's counter-terrorism and domestic security agencies are seeking 'backdoors' to break into encrypted communications. Although understandable, this position is logically inconsistent with the idea of a fully "free" internet. This paper does not attempt to answer whether the "open and free" policy

[118] Arquilla and Ronfeldt, 3–4.

[119] "2017 Foreign Policy White Paper" (Canberra: Australian Government, Department of Foreign Affairs and Trade, November 23, 2017), 74, https://www.fpwhitepaper.gov.au/home; This also continues to be the US national position—see, for example, "National Security Strategy of the United States of America" (Washington, D.C.: The White House, December 2017), 41, https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf.

is appropriate, it merely uses it as an example of the disconnect between some national security and foreign policy interests. These interests will need to be reconciled if Australia is to successfully address the CEI-OPS threat.

4.2 **Unclear lines of power and authority**

It is unclear which government agency has the lead for responding to the CEI-OPS threat. CEI-OPS cross multiple lines of responsibility—which, as discussed in Part 2, is one reason why authoritarian states, which have more centralized decision-making, have a comparative advantage in executing CEI-OPS. Protection of Australian citizens from "acts of foreign interference" is part of ASIO's security mandate.[120] CEI-OPS that affect military operations would appear to be the purview of the newly-formed Information Warfare Division within the Department of Defence, while foreign policy responses to CEI-OPS would appear to be the domain of the Cyber Ambassador's office, within the Department of Foreign Affairs and Trade. Countering CEI-OPS also requires familiarity with the motivations and tradecraft of state adversaries—something Australia's external spy agencies are best placed to lead on. To the extent offensive cyber countermeasures are justified, this would be the purview of the Australian Signals Directorate (an intelligence agency within the Department of Defence). Early reactions in Australia to Russian CEI-OPS against the United States indicate that the Government also views CEI-OPS as a cyber issue.[121] Yet only some (and likely not the majority of) CEI-OPS tactics utilize cyber attacks to achieve their goals (recall Figure 1C, above).

One option to coordinate Australia's CEI-OPS response is the new Department of Home Affairs, established in December 2017. Home Affairs is a domestic security and intelligence 'superministry,' with responsibility for cybersecurity, border security and immigration, counter-terrorism, and federal law enforcement. It will also oversee ASIO. In April 2018, a senior

[120] *Australian Security Intelligence Organisation Act* 1979 (Commonwealth).

[121] For example, the Department of Foreign Affairs and Trade's International Cyber Engagement Strategy classifies "operations to influence elections" as an example of "cyber affairs." ("Australia's International Cyber Engagement Strategy" (Canberra: Australian Government, Department of Foreign Affairs and Trade, October 2017), 5, http://dfat.gov.au/international-relations/themes/cyber-affairs/aices/index.html.)

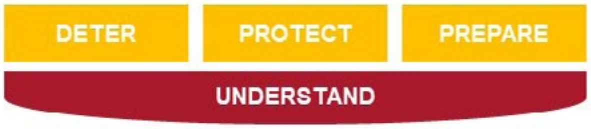
ASIO official was transferred to Home Affairs to act as the inaugural "National Counter Foreign Interference Coordinator." According to the Department, the new Coordinator will facilitate coordination between relevant Home Affairs portfolios, and external agencies including Defence and Foreign Affairs, to address foreign interference, but ASIO will continue to lead on operational matters.[122] Recognizing the need for better coordination is a good first step. However, there remains risks. First, it is unclear whether Home Affairs will have the convening power needed to coordinate the domestic security agencies, let alone Defence and Foreign Policy interests, which remain outside of its lines of authority. Second, there is a real risk that if the National Counter Foreign Interference Coordinator takes ownership of countering the CEI-OPS threat, that Australia's response is reduced to a domestic counter-espionage and / or technical cybersecurity issue. The 'integrated' nature of CEI-OPS campaigns, discussed in Part 2.3 above, means that the response to the threat will require interlinkages with non-security departments, including communications, social, and economic portfolios. Because CEI-OPS target the public and civic institutions, there is also a need to elevate it from a 'closed doors' counter-espionage issue to one which prioritizes public engagement. Finally, a Home Affairs-led response may fail to recognize that Australia's adversaries have interests and motivations we can influence too, inhibiting the development of a national-level CEI-OPS deterrence strategy.

[122] Simon Benson, "Crack Unit to Ward off Spy Attacks," *The Australian*, April 24, 2018, https://www.theaustralian.com.au/national-affairs/national-security/crack-unit-to-ward-off-threats-from-espionage/news-story/8409b24c8595bee1bc27e9927f05fbd5.

5. Recommendations

Australia needs a more holistic response to the CEI-OPS threat that better coordinates and deconflicts domestic and foreign policy, and that reconciles both the technical and cognitive dimensions of the information environment. Such a response should be coordinated via a **National Counter Cyber-Enabled Interference Strategy, the development and implementation of which should be overseen by the Department of Prime Minister & Cabinet (PM&C).** A PM&C-led response would avoid the problems associated with a Home Affairs-led response discussed in Part 4.2. As the central government agency, PM&C is best placed to craft a strategy that mobilizes all of society to address the threat. This Part sets out recommendations that should be considered in formulating the Strategy, grouped under four pillars shown in Figure 5A.

Figure 5A. Elements of a National Counter CEI-OPS Strategy



5.1 Understand the threat

The most urgent part of the response should be to increase understanding of the nature of the CEI-OPS threat. Understanding is a prerequisite for each of the other pillars to succeed. Additionally, part of the reason that CEI-OPS are successful is because democracies have a 'doctrinal gap' in anticipating and responding to them. Simply by raising awareness of the threat, we can make CEI-OPS tactics less effective. In particular, the Government should:

1. **Develop a CEI-OPS lexicon**. The next edition of the Australian Cyber Security Lexicon should include a definition of CEI-OPS, and each of the tactics outlined in Figure 2B. As Australia's Special

Adviser to the Prime Minister on Cyber Security has emphasized in relation to cybersecurity terminology, being able to better define and explain terms will allow decision-makers, and the broader public, "to be involved in a debate that is really necessary for all of society to be part of."[123] A CEI-OPS lexicon will help the Government to better allocate responsibilities to different agencies, update doctrine and policy to take account of the CEI-OPS threat, and develop clear public communication strategies and incident response plans for when CEI-OPS inevitably occur. It could also stimulate further academic research, and development of technical tools to defend against CEI-OPS tactics.

2. **Educate the public about the nature of the threat.** As Part 2 explained, authoritarian states have a strategic advantage over democracies in that they can more easily coordinate all elements of power to conduct grey zone actions like CEI-OPS. Democracies, however, have an underutilized comparative advantage over authoritarian countries—the decentralized nature of public discourse, as well as cultural and economic activity. Their best defense against centralized, grey zone actions is in fact to mobilize a decentralized, whole-of-society response. A prerequisite for this is to first spread awareness of the threat and motivate the urgency of addressing it. The Government could leverage its existing efforts to raise awareness of cybersecurity threats and best practice. In particular, these existing programs could be expanded to emphasize that protecting information from corruption or misuse is just as important as protecting systems from malware and disruption. If businesses are aware that they may be targeted by CEI-OPS activity, they might also design their systems and products in ways which are less likely to be 'gamed' for the purposes of foreign interference.

3. **Educate politicians about the nature of the threat.** Australian political parties have a strong record of bipartisanship on national security issues. Educating politicians about the threat, before Australia faces a major CEI-OPS campaign, can help ensure that politicians maintain their bipartisan approach to CEI-OPS.

[123] Stilgherrian, "Australia to Try Taming Unruly Cyber Words," ZDNet, August 14, 2017, http://www.zdnet.com/article/australia-to-try-taming-unruly-cyber-words/.

CEI-OPS awareness should be incorporated into existing cybersecurity awareness training and briefings delivered to politicians by the Australian Cyber Security Centre. In particular, politicians should be educated about the fact that CEI-OPS often attempt to divide and conquer by exploiting real political divides. Educating politicians about the threat may also help the Government to better prioritize resources. Reprioritization may be needed—for example in its 2017 annual report, ASIO noted that "[t]he heightened terrorist threat this past decade…has limited our scope to redirect resources towards counter-espionage and foreign interference."[124]

4. **Increase intelligence-sharing about CEI-OPS threats.** In its 2017 annual report, ASIO noted that, in contrast with its counter-terrorism efforts, "stakeholders know little about our work [on counter-espionage and foreign interference]."[125] Stakeholders across, and outside of, government will need to be provided with more information about the nature of the CEI-OPS threat, so that they can become helpful partners in responding to it. This will require a proactive approach by ASIO, Home Affairs, and other agencies to declassifying information, and to establishing trusted channels to share threat intelligence. Recent efforts to increase information-sharing on cybersecurity and counter-terrorism issues could provide a model.

5. **Focus public discussion on Australia's vulnerabilities, not on specific adversaries.** It is imperative that the threat of CEI-OPS is not overstated or allowed to fuel xenophobic fears. In particular, when speaking about actual or potential covert interference by China, the Government should make clear that its concern is with the actions of the CCP, not the Chinese people, or Chinese-Australians.[126] First, this upholds individual rights, and prevents social discord. Rhetoric that is, or is perceived as, racist undermines individual rights and

[124] "ASIO Annual Report: 2016-17" (Canberra: Australian Government, Australian Security Intelligence Organisation, October 3, 2017), 141, https://www.asio.gov.au/asio-report-parliament.html. See also page 30 of the same report, where ASIO notes that some stakeholders were of the view that "more resources" should be devoted to foreign interference issues "especially when compared with resources currently devoted to countering the terrorist threat."

[125] "ASIO Annual Report: 2016-17," 58.

[126] Peter Mattis, "What We Talk About When We Talk About Chinese Communist Party Interference in the Public Square," *War on the Rocks*, March 7, 2018, https://warontherocks.com/2018/03/talk-talk-chinese-communist-party-interference-public-square/.

the broader social fabric—without a foreign power even needing to conduct CEI-OPS to achieve this. Moreover, China often denies reports that it is engaging in covert influence by dismissing them as "typical anti-China hysteria" and "racial prejudice."[127] Deniability is one of the factors that makes grey zone activities like CEI-OPS difficult to respond to. Ensuring that discussion is even-handed will help ensure that the public perceives reports of CEI-OPS as credible, not motivated by xenophobic politics.

5.2 Deter adversaries

Australia must act to alter the decision-making calculus of potential adversaries to reduce the likelihood they will engage in CEI-OPS. A state has four primary instruments of power that it can leverage to establish a deterrence strategy: diplomatic, informational, military, and economic. The threat of a diplomatic response alone is unlikely to be an effective deterrent since, as Part 3 concluded, China is only likely to use CEI-OPS where it feels a core national interest is at stake. Economic power is also a poor option. Unlike the US economy, which is significant enough that it can engage in acts of economic warfare like targeted sanctions, this is not a viable option for a middle power like Australia. Additionally, economic sanctions against China—Australia's largest trading partner—would cause Australia more economic harm than China. Military options are also ill-suited to the threat, since CEI-OPS usually do not trigger thresholds for military action and changing these thresholds could trigger conflict escalation. A deterrence strategy based on informational power is the best course of action. This strategy could be supported by diplomatic efforts to gradually shape norms, so as to reduce the appeal of CEI-OPS tactics in the long term. In particular, the Government should:

1. **Pursue retaliatory counter-measures (but never engage in CEI-OPS).** Australia should signal that it is prepared to retaliate to CEI-OPS with a range of measures; but it should never itself authorize a CEI-OPS campaign. Covert manipulation of information by the Australian Government risks infringing on domestic

[127] "Remarks of Spokesperson of Chinese Embassy in Australia," Embassy of the People's Republic of China in Australia, December 6, 2017, http://au.china-embassy.org/eng/gdxw/t1516965.htm.

rights. Cyberspace is borderless, making it impossible to effectively cordon off the domestic audience from the international audience. CEI-OPS campaigns intended to affect an adversary are likely to bleed back into the domestic sphere. Moreover, by engaging in CEI-OPS, a democracy enters a contest that it is likely to lose. As Parts 2 and 3 demonstrate, authoritarian governments are both better able to conduct and defend themselves from CEI-OPS. Finally, covert actions including CEI-OPS generally have a limited deterrent effect. As former Deputy Director of the US Central Intelligence Agency Michael Morell has explained, responses to covert influence must "be seen" to maximize their deterrent effect.[128]

2. **Respond to covert influence with overt counter-measures.** Australia should engage in overt actions in the information environment to respond to CEI-OPS. One type of overt response is to strengthen strategic communications and public diplomacy efforts to counteract adversary narratives.[129] This would need to be managed carefully: a key potential motivator of CEI-OPS by China, discussed in Part 3 above, is fear that China's competitors are trying to "westernize" it to destabilize CCP leadership. To avoid provoking escalation, public diplomacy efforts would need to be carefully targeted to make clear they were not designed to foment political unrest inside China. Another overt response is to 'dox the doxer'[130]—that is, to use offensive cyber tools to determine the identity of adversary CEI-OPS operatives, and then make this information public. This option should only be pursued in response to serious instances of CEI-OPS—since revealing information obtained via cyber means can compromise sources and methods, constraining the future ability to collect intelligence on adversary operatives. Additionally, to control escalation, a 'dox the doxer' response should be targeted at tactical-level operatives, not the strategic-level authorizers of a campaign. Former US Cyber Command Director Admiral Michael Rogers reportedly suggested a 'dox the

[128] Quoted in Eric Lipton, David E. Sanger, and Scott Shane, "The Perfect Weapon: How Russian Cyberpower Invaded the U.S.," *The New York Times*, December 13, 2016, https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html.

[129] See, for example, "National Security Strategy of the United States of America," 35 ("The United States must empower a true public diplomacy capability to compete effectively in this arena.").

[130] The author acknowledges Tom Uren of the Australian Strategic Policy Institute, who drew attention to this option.

doxer' strategy of leaking compromising information about the financial affairs of Russian President Vladimir Putin as retaliation for Russian CEI-OPS against the United States.[131] However, actions which directly undermine an adversary's senior political leaders are highly escalatory and likely to be of limited—if not negative—effectiveness in reducing the CEI-OPS threat, since the adversary will deny and discredit the information. They could even point to the doxing to justify future hostile acts. Targeting tactical-level operatives who are more directly linked with CEI-OPS activities ameliorates these risks. It will also have an effect. The risk of doxing could reduce operatives' willingness to serve their government, while revealing their actions could prompt criticisms or concern from the adversary's citizens. This could disrupt the adversary's operational preparedness to engage in CEI-OPS.

3. **Use cyber operations to disrupt and degrade CEI-OPS.** Authoritarian countries have a strategic advantage in manipulating discourse in the public square. However, many democracies, including Australia, maintain significant cyber warfare capabilities. Australia should make it clear that if faced with a significant CEI-OPS campaign, it would use its cyber capabilities or work with partners to disrupt and degrade organizations involved in carrying out the campaign. This could involve targeted attacks on the availability, confidentiality, or integrity of the data and networks of adversary organizations involved in CEI-OPS. Australia could also respond to CEI-OPS with cyber attacks against the adversary's domestic control on information.[132] Such a response could be particularly effective against China since, as Part 3 explains, China views control of its information environment as a vital national interest, linked to CCP survivability. However, for the same reason, this response could provoke escalation, and therefore should only be used in the most egregious cases of CEI-OPS. Of note, this option does not manipulate content, but instead uses technical

[131] Lipton, Sanger, and Shane, "The Perfect Weapon."

[132] A similar strategy, to "punch holes" in Russia's internet controls to allow dissidents to speak out, was reportedly suggested by former US Cyber Command Commander Admiral Rogers as an option to respond to Russia's interference in the 2016 presidential election. It was rejected by the Department of Defense. (Eric Lipton, David E. Sanger, and Scott Shane, "The Perfect Weapon: How Russian Cyberpower Invaded the U.S.," *The New York Times*, December 13, 2016, https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html.)

means (cyber attacks) to disrupt censorship. In this sense, because it would permit legitimate voices to be heard and does not erode individual rights, it does not share the illegitimacy ascribed to CEI-OPS in Part 1.

4. **Support norms to constrain cyber attacks that may be precursors to CEI-OPS.** There is no one body of international law that address cyber-related activities or foreign interference. In the absence of clearly-defined boundaries, it is possible to shape new norms through consensus-building or by behavior. However, there are two important constraints on Australia's ability to push for norms which might help reduce CEI-OPS activity. First, a norm against cyber-enabled interference could backfire. An Australian embassy or government department that uses social media to promote free and fair elections or human rights could be considered in violation of such a norm.[133] Second, enforcing a norm against CEI-OPS would be almost impossible. As Part 1 explains, influence campaigns are by nature deniable, and hard to quantify. An adversary might be spreading information to deceive or coerce, but it could argue it is merely attempting to educate. There are also strong normative arguments against an international body or court becoming the arbiter of what is, and is not, CEI-OPS activity—since this may require subjective determinations about what is, and is not, 'truth.'[134] Norms may be more effective if they focus on constraining cyber attacks that can support subsequent CEI-OPS campaigns, such as massive thefts of data about members of the public, or government. At least for the foreseeable future, such a norm is unlikely to be supported by the United States, let alone potential adversaries like China and Russia. These states are not prepared to reduce their cyber espionage activities, even if the upside would be to reduce the

[133] Jacqueline Van De Velde, "The Law of Cyber Interference in Elections," SSRN Scholarly Paper (Rochester, NY: Social Science Research Network, May 15, 2017), 34, https://papers.ssrn.com/abstract=3043828.

[134] Van De Velde, 31.

CEI-OPS threat.[135] Therefore, Australia could focus on building a consensus among peers in the Indo-Pacific, or among other middle powers, about what activities in the information environment will be accepted, and the appropriate responses when boundaries are crossed. A gradual consensus-building approach may be the most effective way to achieve meaningful agreement in the long term. In the short term, it could also help limit the number of new state actors which choose to develop CEI-OPS capabilities.

5.3 Protect the public square

Australia must act to protect the public square from illegitimate interference. This will involve improving the ability to detect CEI-OPS campaigns and developing capabilities to disrupt and degrade them. Steps should also be taken to make CEI-OPS tactics less effective—including by reducing the attack surface available to adversaries. To protect the public square, the Government should:

1. **Identify "critical public square infrastructure" and develop best practices for its protection.** Many countries have lists of nationally-protected critical infrastructure—which include things like their transport, communications, and energy systems.[136] Given the risk CEI-OPS can pose to democracy, the Government should consider developing a list of actors and organizations which are critical to the proper functioning of the public square. Australia's "critical public square infrastructure" includes elections-related systems, as well as political campaigns, federal and state politicians, media outlets, and academic institutions. Publishing this list would itself be an important signal, encouraging these actors to be more aware

[135] After the 2015 hack of the US Office of Personnel Management (OPM), the United States decided not to respond. Then Director of National Intelligence Jim Clapper said: "you have to kind of salute the Chinese for what they did... If we had the opportunity to do that, I don't think we'd hesitate for a minute." The United States viewed the hack as cyber espionage—something that the US National Security Agency also extensively engages in. However, the OPM hack gave China a trove of documents—including over 20 million records of the personal information of every holder of a US security clearance—which could be used to develop a highly-targeted future CEI-OPS campaign. (Matthew Ferraro, "On the OPM Hack, Don't Let China Off the Hook," *The Diplomat*, July 14, 2015, https://thediplomat.com/2015/07/on-the-opm-hack-dont-let-china-off-the-hook/.)

[136] See, for example, "Critical Infrastructure Sectors," Department of Homeland Security, July 11, 2017, https://www.dhs.gov/critical-infrastructure-sectors.

of, and prepared for, CEI-OPS threats. The Government should also develop and share "best practices" specifically tailored to each of them. These would include recommendations for how they can mitigate their cyber and CEI-OPS risk, engage in incident response planning, and access available government resources.[137]

2. **Develop a CEI-OPS "early warning" system.** The intelligence community should develop mechanisms to detect CEI-OPS campaigns, and precursor activities. As the Case Study in Part 3 showed, groundwork for CEI-OPS campaigns can be laid years before specific tactics are used, or an effect is achieved. Developing an early-warning system will require collaboration between domestic intelligence and counter foreign interference expertise housed in ASIO, and the foreign signals intelligence and cyber skills housed in the Australian Signals Directorate. It will also require collaboration and information-sharing with private sector entities—for example, Internet Service Providers, and social media companies.[138] The Department of Home Affairs would be well-placed to lead this effort, given its experience in coordinating diverse stakeholders to address other security issues.

3. **Regulate social media companies to make their platforms less susceptible to CEI-OPS.** Many of the underlying forces that enable CEI-OPS, set out in Figure 2A, are almost impossible for a national government to affect—since they arise from a complex interaction of technological and social forces, and are global in nature. It is more feasible to use government regulation to affect the business decisions of social media companies. Regulators have previously shied away from imposing rules on 'big tech,' since Australia is only a small portion of their global business.[139] However, while Australia has less leverage over big tech than, for example, the United States, it can regulate companies with a business presence in

[137] See, for example, Defending Digital Democracy Project, "The State and Local Election Cybersecurity Playbook" (Cambridge, Mass.: Belfer Center for Science and International Affairs, February 2018), https://www.belfercenter.org/publication/state-and-local-election-cybersecurity-playbook.

[138] Eric Rosenbach, "Defending Digital Democracy: The Four Corners of Election Security," United States Senate Intelligence Committee, Hearing on Russian Interference in the 2016 US Elections (March 21, 2018).

[139] Deborah Snow and James Manning, "Modern-Day Droogs Are Free to Roam," *The Sydney Morning Herald*, September 14, 2012, https://www.smh.com.au/technology/modernday-droogs-are-free-to-roam-20120914-25xhf.html.

Australia—which includes Facebook, Twitter, and Google. Moreover, while big tech has been historically resistant to regulation, the recent public "techlash"[140] is likely to have made it more willing to engage with governments.[141] Many CEI-OPS tactics exploit the data and algorithms used by social media platforms. To ensure that social media platforms provide less opportunity to CEI-OPS operatives, the Government should consider regulation that requires:

- *Transparency*. Social media companies could be required to publicly disclose if they are aware that their platform is being manipulated by government operatives, and to flag content they identify as foreign interference material. Public companies have an obligation to tell the investing public if they become aware that someone is manipulating their share price; similar transparency should be required of key actors in the public square.[142]
- *Detection and labelling of social bots*. A bot is "software designed to automate a task in a computing system."[143] They are often used on social media platforms, including by legitimate actors, to spread or up-vote content quickly and at scale. However, as former Facebook investor Roger McNamee has explained, bots can "distort the public square in a way that was never possible in history".[144] Researchers have found that bots play a disproportionate role in spreading and repeating misinformation, and that people often repost content distributed by bots without realizing they

[140] A term coined in 2017 to describe mounting public criticism of the tech sector due to its perceived failure to pay sufficient corporate taxes, concern about personal privacy and fair data use, and the social consequences of their products.

[141] "The Pendulum of Power Swings Back towards the State," *The Economist*, November 7, 2017.

[142] Idea adapted from a US government official who presented at a Director's Lunch at the Belfer Center for Science and International Affairs held under Chatham House Rule in Cambridge Massachusetts in 2017.

[143] Norah Abokhodair, Daisy Yoo, and David W. McDonald, "Dissecting a Social Botnet: Growth, Content and Influence in Twitter," in *Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing* (New York, 2015), 840, http://doi.acm.org/10.1145/2675133.2675208.

[144] Roger McNamee, "How to Fix Facebook—before It Fixes Us," *Washington Monthly*, March 2018, https://washingtonmonthly.com/magazine/january-february-march-2018/how-to-fix-facebook-before-it-fixes-us/.

are interacting with a bot.[145] Some have proposed a "ban on bots" to curtail CEI-OPS tactics which rely on spreading or amplifying content. However, a "ban on bots" is unfeasible; Australia is unlikely to be able to enforce such a major rule change on its own, and it would also harm legitimate users' interests. Instead, a law requiring that platforms identify and label bots (and even provide users with the option to block them) would be more politically feasible. It is also likely to be technically possible:[146] researchers have already developed tools which screen for and identify bots.[147]

- *Public interest standards for social media algorithms*. Social media algorithms prioritize and promote controversial content—a feature that is easily gamed for the purposes of CEI-OPS. To address this, the Australian Communications and Media Authority (ACMA) could promulgate public interest standards for social media algorithms, which require them to take factors other than popularity into account when serving content to users. Currently however, ACMA lacks the expertise and personnel to monitor whether a standard like this has been complied with. As an interim step, the Government could pass laws which require social media companies to provide a level of 'algorithmic explainability' to the public.[148] Platforms would be required to clearly disclose what parameters their algorithms are optimized for, and the factors that cause content to be up- or down-voted. Laws could also be introduced to make it easier for social media platforms to share information

[145] Chengcheng Shao et al., "The Spread of Misinformation by Social Bots," *Cornell University Library*, July 24, 2017, http://arxiv.org/abs/1707.07592.

[146] Zi Chu et al., "Who Is Tweeting on Twitter: Human, Bot, or Cyborg?" (Proceedings of the 26th Annual Computer Security Applications Conference, 2010), https://dl.acm.org/citation.cfm?id=1920265.

[147] It should be noted that these tools largely work because bots exhibit 'bot-like' behaviors. In future, adversaries are likely to adapt to make their bots harder to detect. A good regulatory response would recognize that bot detection may never be perfect, but would require social media platforms to make their best efforts to do it.

[148] Any law should stop short of mandating full 'algorithmic transparency' since: (a) a platform's precise algorithmic formula is sensitive commercial information; and (b) social media algorithms are so complex and quick to self-learn, that they are increasingly not readily understandable to their creators, let alone the public. Therefore, requiring the algorithmic formula to be disclosed would be disproportionately damaging to firms, and may not provide much relevant information to the public.

with researchers who are studying the impacts of their algorithms. Together, these interim steps could increase pressure on social media firms to agree to industry public interest standards for their own algorithms, without need for further government intervention.

5.4 Prepare the public for CEI-OPS

Australia will not be able to deter or prevent all instances of CEI-OPS. However, it can minimize their impact. By making people and institutions less susceptible to CEI-OPS, the Government can frustrate the strategic objectives behind CEI-OPS campaigns. In particular, the Government should:

1. **Ensure national media remains well-funded and independent.** Transparency and exposure are the antithesis of covert intervention.[149] Moreover, given the way in which CEI-OPS campaigns attempt to manipulate perception and belief, attempts to attribute and discredit them must be highly credible. When it comes to attributing CEI-OPS campaigns to foreign adversaries, the Government may not have sufficient credibility to make a 'trust us' call to the public. Researchers and journalists are likely to be viewed more favorably. [150] To date, these actors have played a very important role in unveiling foreign interference and, especially with regard to China, "countering false CCP narratives."[151] They are likely to continue to play an important role in identifying and countering CEI-OPS. Accordingly, the Government must ensure that the CEI-OPS threat informs national media and higher-education policy. It should recognize that maintaining a well-funded public broadcaster and robust traditional media sector is not just necessary for a well-functioning democracy, but also has national security implications. A strong traditional media sector also prevents people reverting to social media for news—a positive, since the existing

[149] Kelsey Munro, "A Free Press Is a Magic Weapon against China's Influence Peddling," The Lowy Institute, *The Interpreter* (blog), December 18, 2017, https://www.lowyinstitute.org/the-interpreter/free-press-magic-weapon-against-china-influence-peddling.

[150] Munro.

[151] Sarah Cook, "How to Respond to Beijing's Growing Influence Abroad," *The Diplomat*, February 27, 2018, https://thediplomat.com/2018/02/how-to-respond-to-beijings-growing-influence-abroad/.

business models of these platforms favor CEI-OPS. The Government should also consider providing grant funding to journalists and researchers who are developing digital tools, like fact-checking websites, that can help to expose CEI-OPS. These tools often rely on artificial intelligence and can therefore be expensive, underscoring the need for Government subsidies. The Government should also pass more stringent foreign media ownership laws and require journalists and researchers to disclose links to foreign organizations, in order to safeguard their independence.

2. **Consider the creation of a "special media forces."** As Part 3 discussed, China may be more likely to engage in CEI-OPS if tensions over a particular territorial dispute intensify. In these circumstances, generating trusted facts about the situation on the ground will be imperative, but private journalism might be impeded by the high-tension environment. One option is to consider developing deployable and mobile "counter-CEI-OPS" units. Like military special forces units, these would be small and readily deployable, but they would not engage in combat activities. Instead, they would be "armed with weapons of information…discovery and dissemination."[152] This option is similar to ideas discussed by analysts in the 1990s for how states, which lacked the will to militarily intervene in humanitarian disasters, could at least use information warfare tactics to expose hate speech and propaganda in conflict zones.[153]

3. **Introduce certification standards for audio-visual records.** Currently, "the existence of high-quality recorded video or audio evidence is usually enough to settle a debate about what happened in a given dispute."[154] However, as Figure 2A showed, advances in artificial intelligence are enabling increasingly realistic forgeries of audio-visual materials. Forged information can be used as part of a CEI-OPS campaign. To reduce this risk, the Government should consider introducing standards for official "certification" of audio and video, in circumstances where documentary evidence

[152] John Arquilla and David Ronfeldt, "The Emergence of Noopolitik" (RAND Corporation, 1999), 50–51, https://www.rand.org/pubs/monograph_reports/MR1033.html.

[153] Jamie F. Metzl, "Information Intervention: When Switching Channels Isn't Enough," *Foreign Affairs*, November 1, 1997, 16.

[154] Future of Humanity Institute et al., "The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation," February 2018, 46, https://maliciousaireport.com/.

would ordinarily need to be officially certified. Certification of these media is increasingly technologically feasible. The Australian Federal Police should also ensure it is investing in technology that will permit it to screen for and detect audio-visual forgeries.

Conclusion

The Information Age has brought significant economic and social benefits to Australia. However, advances in information and communications technology have also exposed Australia's public square to an unprecedented threat of distortion and manipulation. The public square is the lifeblood of democracy; ensuring it is protected should be a matter of national urgency. However, the threat that Australia faces from CEI-OPS has been significantly underappreciated. This is despite the fact that Russia's CEI-OPS campaigns against the United States should have served as a warning signal to democracies the world over. Australia lacks the vocabulary to even discuss the CEI-OPS threat, and a coherent strategy to protect itself from it. It is therefore recommended that PM&C develop a coordinated National Counter Cyber-Enabled Interference Strategy that addresses at least four elements: (i) understanding the threat and lifting the quality of public and political debate about it; (ii) deterring potential state adversaries including but not limited to China; (iii) protecting the public square by reducing the means and opportunity for adversaries to conduct CEI-OPS; and (iv) preparing the public for CEI-OPS to inoculate the country from their effect.

Belfer Center for Science and International Affairs
Harvard Kennedy School
79 John F. Kennedy Street
Cambridge, MA 02138

www.belfercenter.org

Printed in the United States of America