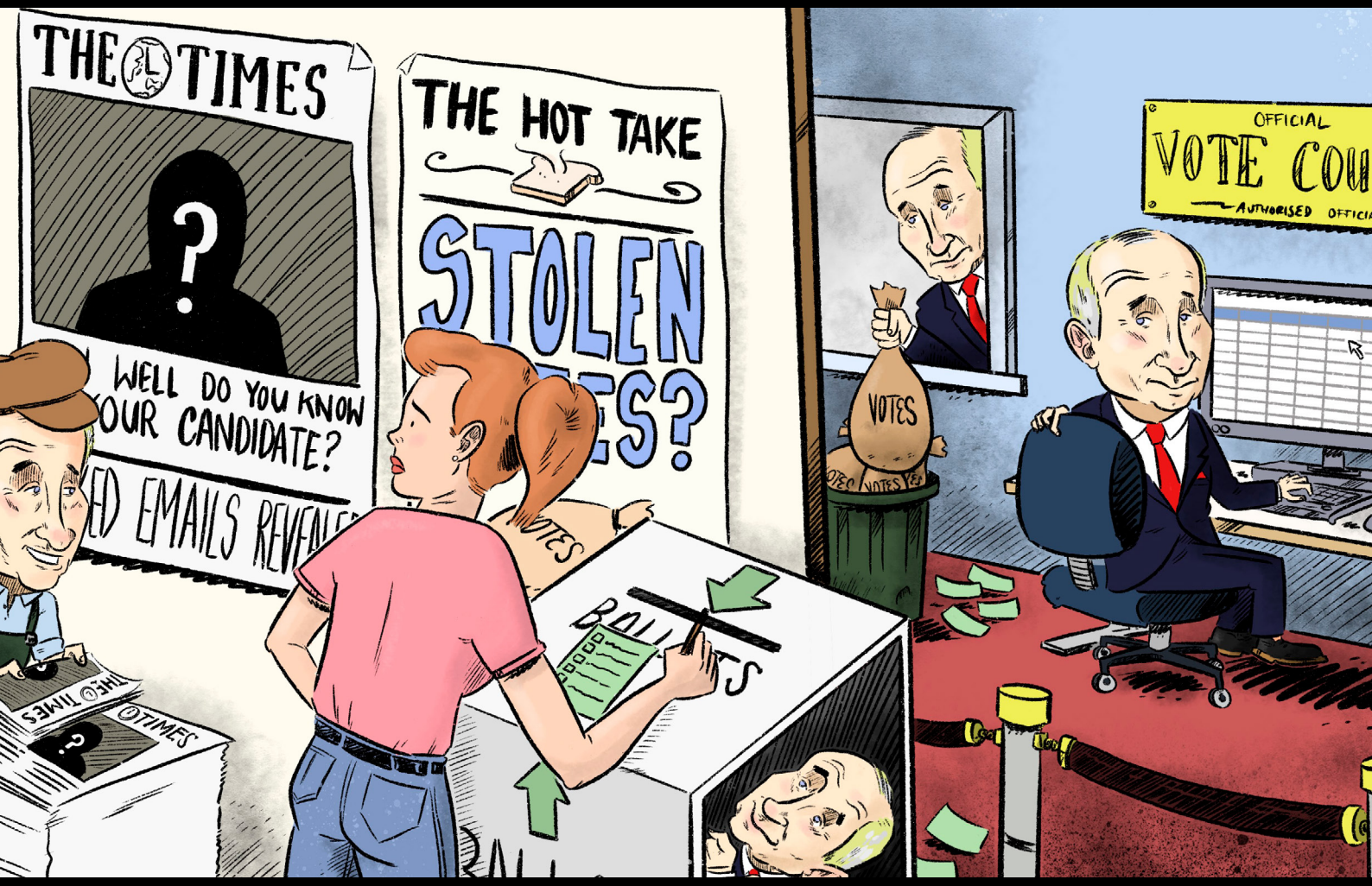
Hacking democracies

Cataloguing cyber-enabled attacks on elections

Fergus Hanson, Sarah O'Connor, Mali Walker and Luke Courtois



ASPI AUSTRALIAN STRATEGIC POLICY INSTITUTE
INTERNATIONAL CYBER POLICY CENTRE
acs

Policy Brief
Report No. 16/2019

About the author

Fergus Hanson is the head of ASPI's International Cyber Policy Centre. He is the author of *Internet wars* and has published widely in Australian and international media on a range of cyber and foreign policy topics. He was a visiting fellow at the Brookings Institution and a Professional Fulbright Scholar based at Georgetown University working on the take-up of new technologies by the US Government. He has worked for the United Nations and as a program director at the Lowy Institute and served as a diplomat at the Australian Embassy in The Hague. He has been a fellow at Cambridge University's Lauterpacht Research Centre for International Law and the Centre for Strategic and International Studies, Pacific Forum.

Sarah O'Connor is a researcher working with ASPI's International Cyber Policy Centre. Sarah holds a Bachelor of International Relations (Hons.) and Graduate Certificate in Law from the Australian National University (ANU), and is currently undertaking a Masters of International Law at ANU. Her research interests include international law, cybersecurity, and the future of warfare and technology.

Mali Walker is an ASPI research intern.

Luke Courtois is an ASPI research intern.

What is ASPI?

The Australian Strategic Policy Institute was formed in 2001 as an independent, non-partisan think tank. Its core aim is to provide the Australian Government with fresh ideas on Australia's defence, security and strategic policy choices. ASPI is responsible for informing the public on a range of strategic issues, generating new thinking for government and harnessing strategic thinking internationally.

ASPI International Cyber Policy Centre

The ASPI International Cyber Policy Centre's mission is to shape debate, policy and understanding on cyber issues, informed by original research and close consultation with government, business and civil society.

It seeks to improve debate, policy and understanding on cyber issues by:

1. conducting applied, original empirical research
2. linking government, business and civil society
3. leading debates and influencing policy in Australia and the Asia–Pacific.

The work of ICPC would be impossible without the financial support of our partners and sponsors across government, industry and civil society. This research was made possible thanks to the generous support of the Australian Computer Society (ACS).

Important disclaimer

ASPI

Tel +61 2 6270 5100
Fax + 61 2 6273 9566
Email enquiries@aspi.org.au
www.aspi.org.au
www.aspistrategist.org.au
www.aspi.org.au/icpc/home
facebook.com/ASPI.org
@ASPI_ICPC

First published May 2019

ASPI AUSTRALIAN STRATEGIC POLICY INSTITUTE
INTERNATIONAL CYBER POLICY CENTRE
acs

Hacking democracies

Cataloguing cyber-enabled attacks on elections

Fergus Hanson, Sarah O'Connor, Mali Walker and Luke Courtois

Policy Brief
Report No. 16/2019

Contents

Foreword

One of the great hopes for the internet was that it would herald a new era in the democratisation of information. To a large extent, it's been successful. So successful, in fact, that global platforms, technology diffusion and mobility have brought some unintended consequences by enabling the rapid dissemination of disinformation and fake news.

We live in a time when trust in our democratic and other key institutions has declined, and this is compounded by new capabilities of adversaries seeking to interfere in our elections and to undermine people's trust in those institutions.

In this policy brief, the writers explore areas where interference has been detected across the world and consider key learnings from those examples in order to develop policy responses for countering each type of interference.

Technology has the power to transform lives by reducing barriers to entry and creating greater equity so that all our citizens can participate in education and the economy. We want to live in a world where friction is removed and technology enhances our experience, where all citizens have access to the internet, and where we can vote electronically in elections. However, our interconnection needs to be safe and trusted, protecting and enhancing our democracies.

This brief starts an important national conversation, generating awareness of the approaches commonly taken by adversaries to spread disinformation, misinformation and fake news. It lays out a series of measures for managing risk, and serves as an educational resource for our citizens on what to keep an eye out for, and how to better distinguish reputable information from disinformation in real time.

Yohan Ramasundara
President, Australian Computer Society

What's the problem?

Analysis of publicly known examples of cyber-enabled foreign interference in elections reveals key challenges. First, while perceptions of interference are widespread, the actors are few—Russia and China—and the effort is highly targeted. Russia is targeting the US and Europe (with a few forays into South America), while China targets its region (having, for the moment, reached as far as Australia). Second, the methods used can be hard to pick up and democracies seem poorly equipped to detect intrusions, being traditionally focused on external intelligence collection. Adversaries are able to enter public debates, infiltrate legitimate activist networks and even enter the mainstream media as trusted commentators. Significant activity may be being missed. Finally, while opinion polling shows concerning levels of dissatisfaction with democracy and weakening trust in public institutions, it's very difficult to assess the impact of election interference on those phenomena. It's likely to have some impact but be outweighed by larger societal factors.

What's the solution?

First, the response from democracies should be calibrated to the likely risk and adversary. The US and European states are clear targets of Russia; Indo-Pacific nations are targets of the Chinese Communist Party (CCP). Second, more effort is needed to detect foreign interference, including offline and non-state efforts. Because democracies have a natural aversion to government surveillance, a better answer than simply stepped-up government monitoring may be supporting non-profit, non-government initiatives and independent media. Third, effort is needed to develop better ways to measure the impact of foreign interference to allow for a more informed decision on resourcing efforts to counter it. Notwithstanding the lack of current empirical data on impact, opinion polling points to a perception that foreign interference will occur and, in places such as the US, a view by many that the 2016 presidential election was swayed by it (a credible view, given the narrowness of the outcome). Research is needed to measure the effectiveness of different education and awareness efforts to address these concerns. Fourth, public funding may be needed to better secure political parties and politicians from cyber intrusions. Finally, democracies need to impose costs on the two primary state actors: they should consider joint or regional action to make future or continued interference sufficiently costly to those states that they will no longer pursue it. Legislation may also be needed to make it more difficult for foreign adversaries to operate (being mindful of the differing objectives of the two main actors); this may be a second best for countries that find it too difficult to call out adversaries.

Introduction

In 2016, Russia comprehensively and innovatively interfered in the US presidential election, offering a template for how democracies around the world could be manipulated.[1] Since then there have been 194 national-level elections in 124 countries and an additional 31 referendums.[2] This report seeks to catalogue examples of foreign interference in those polls and group them into three 'buckets':

- interference targeting voting infrastructure and voter turnout
- interference in the information environment (to make the scope manageable, we have focused on interference surrounding elections, but it's apparent that such efforts continue outside election periods as part of longer term efforts to manipulate societies)
- longer term efforts to erode public trust in governments, political leadership and public institutions.

This research focused on cyber-enabled interference (including, for example, information operations that harness social media and breaches of email and data storage systems), but excluded offline methods (for example, the financing of political parties and the suborning of prominent individuals). The yardstick for counting an activity as interference was that proposed by former Prime Minister Malcolm Turnbull, who put it this way when introducing counter-foreign-interference laws in Australia in 2017: 'we will not tolerate foreign influence activities that are in any way covert, coercive or corrupt. That's the line that separates legitimate influence from unacceptable interference.'[3]

A major issue has become the public perception that results may have been swayed, with consequences for the direction of these states' policies and actions, together with a loss of public trust in democratic institutions and processes.

Multi-country Pew Research Center polling shows that there's an increasing expectation among global publics that elections will suffer interference: majorities (including 65% of Australians) in 23 of 26 countries surveyed in 2018 said it was very or somewhat likely that a cyberattack would result in their elections being tampered with.[4]

In some cases, such as the 2016 US presidential election, polling shows that a large proportion of people (39% of US adults) feel that Russian meddling swung the election,[5] which is probably the most valuable outcome Russia could have hoped for, given that it's seeking to undermine confidence in US global leadership and the US public's faith in the nation's democratic process.[6]

Since that election, reports of foreign interference in democratic elections have continued to surface. This suggests a belief among adversary states that interference is serving their interests and that the costs of action are not sufficiently high to deter this behaviour.

Of course, foreign governments interfering in elections is nothing new.[7] While the objectives might be similar to those of Cold War style efforts, the means are different. Today, a state such a Russia is able to reach more than a hundred million Americans through a single platform such as Facebook without sending a single operative into US territory.[8] Or, as nearly happened in Ukraine, the official election results can be remotely altered to show a candidate who received just 1% of the vote as winning.[9]

And, significantly, a little effort goes a long way: in 2016, Russian operatives were able to organise two opposing groups to engage in a protest in front of the Islamic Da'wah Centre of Houston for 'the bargain price of $200'.[10] Having a big impact is now much easier, cheaper and less risky.

For democratic governments, responding can be extremely difficult. The methods used by adversaries typically exploit treasured democratic principles such as free speech, trust and openness. Detection can be hard both because the methods are difficult to identify and because democracies avoid surveillance of their own domestic populations and debates (outside niche areas such as traditional criminal and terrorist activity). Typically, the bulk of intelligence resources is directed towards external collection, and domestic populations are rightly wary of increased government monitoring.

Democratic governments themselves can be obstacles: if the winning party believes it benefited from the foreign interference or would be delegitimised by admitting its scale, it can even mean the newly elected government will play down or ignore the interference. Tensions in the US in the wake of Russian interference in the 2016 election point to the potential for these sorts of issues to arise.[11]

Measuring levels of interference and adversary's objectives is another challenge. Given the difficulty of detection and the variance in methods employed, it's hard to compare relative levels of interference across elections. Objectives are also not always straightforward. Most efforts to interfere in elections are not about directly altering the vote count. Instead, many appear aimed at disrupting societies or undermining trust in important institutions. There also appear to be different overarching aims depending on the adversary involved.

Project overview and methodology

This research was generously supported by the Australian Computer Society and stemmed from a series of engagements with policymakers on countering election interference. Desk research and interviews focused on developing a database of cyber-enabled foreign interference in democratic elections. It was informed by a full-day workshop in London involving several electoral commissioner equivalents from around the world as well as the President of the Australian Computer Society. A key focus of the workshop was the development of a framework for mapping election interference with a view to improving the policy response.

The start date for the research was the 2016 US presidential election and the end date was April 2019. During that period, this research identified 194 national-level elections in 124 countries and an additional 31 referendums.

Using Freedom House's *Freedom in the world* report,[12] of the 124 states that have held national elections since November 2016, 53 are considered 'free', 45 'partly free' and 26 'not free'. Given the focus of this report on democracies, we limited the research scope to the 97 countries that held elections and that were deemed free or partly free.

As noted above, examples of foreign interference were grouped into three buckets. This built off and expands on a framework in the International Cyber Policy Centre's *Securing democracy in the Digital Age* report.[13]

Categorising incidents was an inexact science. Often there was a lack of publicly available information about the case (many media reports described 'hacks' without elaborating), or it might easily straddle more than one category. Consider the intrusion into Australia's parliament and three political parties reported by Prime Minister Scott Morrison on 18 February 2019,[14] suspected to have been carried out by Chinese state-sponsored actors. The intent behind this incident is still unclear.

Was it solely espionage or an act of foreign interference?[15] The sophisticated state actor has not seemed to use any material obtained to interfere in the current election. That may be because of the discovery of the intrusions, or because the information obtained is being used for a different purpose (as suggested by ASPI's Michael Shoebridge[16]). For the purposes of this report, it was classified as 'long-term erosion of public trust', given that the public reporting highlighted inadequate security among core Australian institutions.

This report captures examples of interference that were executed (for example, Russian online disinformation campaigns that ran on social media during the 2016 US presidential election) and those that were discovered but not executed (such as Russians' accessing of US voter rolls during that election without manipulating or using them).

Findings

Of the 97 national elections in free or partly free countries reviewed for this report during the period from 8 November 2016 to 30 April 2019, a fifth (20 countries) showed clear examples of foreign interference, and several countries had multiple examples (see the appendix to this report).[17] It's worth noting that confidence in attributions to foreign actors varied widely. In ideal circumstances, a government source made the attribution, but often the attribution was more informal. Our intention was not to provide an exhaustive list of every alleged case of foreign interference but instead to capture the spread of states experiencing the phenomenon and illustrative examples of different methods. Details on all examples identified through this research are set out in the appendix.

Country analysis

Of the 97 elections and 31 referendums reviewed, foreign interference was identified in 20 countries: Australia, Brazil, Colombia, the Czech Republic, Finland, France, Germany, Indonesia, Israel, Italy, Malta, Montenegro, the Netherlands, North Macedonia, Norway, Singapore, Spain, Taiwan, Ukraine and the US.

Of those 20 states, 14 were deemed 'free' and 6 'partly free'. Just over half (12 of 20) of the states were in Europe, which is unsurprising given Russia's leading role in this area (Table 1).

Table 1: Regional spread (alleged actor)

Europe	Asia–Pacific	Middle East	Americas
Czech Republic (Russia)	Australia (China)	Israel (Iran)	Brazil (Russia)
Finland (Russia)	Indonesia (China/Russia)		Colombia (Russia/Venezuela)
France (Russia)	Singapore (China)		US (Russia)
Germany (Russia)	Taiwan (China)		
Italy (Russia)			
Malta (Russia)			
Montenegro (Russia)			
Netherlands (Russia)			
North Macedonia (UK/Russia)			
Norway (Russia)			
Spain (Russia)			
Ukraine (Russia)			

Table 1 shows the strong geographical link between the target and actor. With the exception of one anomalous case involving the UK (which was alleged to have supported a Yes campaign in a Montenegrin referendum), Russia was the only state interfering in European elections. Similarly, in the Indo-Pacific, China was the only actor (except for Indonesia, where Russia was also involved). Iran's interference in Israel has a clear connection to its adversarial relationship. In the Americas, there's more diversity among the actors, but Russia remains the dominant player.

China's versus Russia's motivations

Russia's and China's interference reflect different national approaches. For Russia, a key objective is to erode public trust in democracies and to undermine the idea that democracy is a superior system.[18] This might be driven by President Putin's personal drive to make the West 'pay' for its destruction of the Soviet bloc and by the desire to mount a case inside Russia that democracies are flawed and therefore not a model that Russians should aspire to. As a consequence, Russian interference is inherently destructive to democratic systems, even at the same time as Moscow may seek to promote a party or a candidate thought to be more sympathetic to its interests.[19]

Chinese interference seems more strategically focused on ensuring that its interests are promoted across all party lines. Unlike the Russian stance, one party's interests don't appear to be favoured at the expense of others (with the exception, perhaps, of Taiwan[20]). Instead, all consequential parties are in its crosshairs with a view to making them more sensitive to core CCP interests. China also seems to pursue a broader front of influencing activities (many of which aren't captured by this report's focus on cyber-enabled methods), which can include financial donations,[21] aligning the policy interests and public comments of party figures to CCP political goals and suborning prominent individuals to advocate for Beijing's interests. China doesn't seem to be as openly intent on doing damage to the credibility of foreign political systems so much as aligning those systems to its strategic objectives.[22]

Methods

A review of the dataset reveals considerable repetition in methods. There are multiple examples of social media platforms being exploited to reach target populations, often used in concert with state-sponsored media outlets. There is, however, considerable variation in the way social media are exploited. This ranges from organising rallies and amplifying the voices of favoured groups to suppressing voter turnout and exacerbating existing divisions.[23] There are also several examples of system breaches, again to pursue different ends, including stealing and leaking emails and accessing voter rolls.

Given the lack of detail in many media reports on foreign interference, it's difficult to provide a list of the most common methods. Frequency of use also does not translate into impact. For example, the breach of one person's email account (such as the account of Hillary Clinton's campaign chair, John Podesta) can have much greater impact than any single social media post or perhaps all of them.

Types of interference

This section examines our three defined buckets of interference.

Targeting of voting infrastructure and voter turnout

Direct tampering with election results is perhaps the most affronting form of foreign interference because it most directly overturns the will of the people.

Ukraine has long been one of the main targets of Russian election interference efforts and has also suffered the most egregious effort to alter the technical results of an election. As Mark Clayton reported back in 2014 (a date outside the scope of the mapping period covered by this report):

> Only 40 minutes before election results were to go live on television at 8 p.m., Sunday, May 25, a team of government cyber experts removed a 'virus' covertly installed on Central Election Commission computers, Ukrainian security officials said later.
>
> If it had not been discovered and removed, the malicious software would have portrayed ultra-nationalist Right Sector party leader Dmytro Yarosh as the winner with 37 percent of the vote (instead of the 1 percent he actually received) and Petro Poroshenko (the actually [*sic*] winner with a majority of the vote) with just 29 percent, Ukraine officials told reporters the next morning.[24]

There are multiple means by which adversary states could interfere with the technical results of elections. Various methods could be used to prevent citizens from being able to vote (for example, by rendering electronic voting booths unusable or corrupting the voter roll so eligible voters are removed and turned away from voting booths[25]) or reducing the turnout of certain voter groups with known dominant voting behaviours (for example, via online campaigns that encourage a boycott[26] or targeted misinformation that has the effect of deterring certain voter groups[27]).

The result itself could be altered via various means. Electronic voting booths could be maliciously programmed to record a vote for Candidate A as a vote for Candidate B instead, the transmission of votes tallied at individual voting booths could be intercepted and altered, affecting the final tally, votes in the central tally room or system could be altered remotely or, as was attempted in Ukraine, the release of the vote outcome could be tampered with (a tactic unlikely to go unnoticed, but likely to cast doubt among some about the integrity of the poll and of the national electoral system).

Research for this report identified six countries that had experienced interference targeted at voting infrastructure and voter turnout: Colombia, Finland, Indonesia, North Macedonia, Ukraine and the US (Table 2).

Table 2: Targeting of voting infrastructure and voter turnout

Target	Actor
Colombia	Russia/Venezuela
Finland	Russia
Indonesia	Russia/China
North Macedonia	Russia
Ukraine	Russia
US	Russia

Examples included the targeting of voter registration rolls in Colombia,[28] Indonesia[29] and 21 US states,[30] a denial of service (DoS) attack on a Finnish web service used to publish vote tallies,[31] a distributed denial of service (DDoS) attack on Ukraine's Central Election Commission,[32] and the use of social media to suppress voter turnout in North Macedonia[33] and in the US.[34] In the US, an Oxford University report noted that Russian operatives tried to suppress the vote of African-Americans by pushing the narrative that 'the best way to advance the cause of the African American community was to boycott the election and focus on other issues instead'.[35] While it's difficult to determine the effect of the disinformation campaign by Russia's Internet Research Agency, the Pew Research Centre reported that the voter turnout of African-Americans fell in 2016 (see appendix, page 19).[36]

The attackers identified in public reports (sometimes speculatively) were Russia (in one instance, combined with Venezuela) and China. Russia was by far the dominant actor.

Interference in the information environment around elections

It's difficult to detect foreign interference during elections with high confidence in a timely manner. Consider this example from Bret Schafer, which fooled multiple media outlets:

> Have you met Luisa Haynes? She was a prolific force in the #BlackLivesMatter community on Twitter. In just over a year, she amassed more than 50,000 followers; and her outspoken, viral takes on everything from Beyoncé to police brutality earned her hundreds of thousands of retweets and media coverage in more than two dozen prominent news outlets.
>
> She was, on the surface, a symbol of a new generation of Black activists: young, female, and digitally savvy—except—she was fake.[37]

At the International Cyber Policy Centre, journalists periodically approach us about websites and social media accounts they suspect are run by foreign agents or trolls. Mostly, investigations lead to dead ends, or to apparently real people who are hard to definitively classify as foreign trolls rather than colourful citizens.

Now that the traditional media have lost their old gatekeeper role and control over the information environment, it's far easier for foreign adversaries to inject themselves into national debates and much harder to trust what you're reading and seeing. When Australians were asked in 2018 'Do you feel like the news you read or watch gives you balanced and neutral information?', 54% said 'never' or 'rarely'. There were similar results in democracies around the world[38] (in historical terms, in the US the proportion of people reporting 'a great deal' and 'quite a lot' of confidence in newspapers has dropped from a high of 39% in 1990 to 23% in 2018[39]).

While avenues for altering the technical results of elections are limited, opportunities to manipulate the information environment are limited only by creativity. Methods might include amplifying a party's existing narrative using social media accounts that have assiduously built up followers over lengthy periods,[40] or creating and spreading disinformation to undermine a candidate (for example, the state-owned Russian news agency *Sputnik* calling French presidential candidate Emmanuel Macron an agent of 'the big American banking system').[41] It might involve infiltrating genuine activist groups and attempting to increase polarisation,[42] or it could involve the creation of fake personas who provide

inflammatory commentary on divisive issues, as with Luisa Haynes. Often such campaigns seek to prey on and exacerbate existing social cleavages with a view to exploiting them to manipulate the information environment in the desired direction.

While the impact of this manipulation isn't as direct as interfering with key election infrastructure, its ease and cheapness, combined with the difficulty of timely detection, make it a preferred method.

Foreign interference in the information environment was identified in 10 states: France, Israel, Italy, Malta, the Netherlands, North Macedonia, Spain, Taiwan, Ukraine and the US (Table 3).

Table 3: Interference in the information environment

Target	Actor
France	Russia
Israel	Iran
Italy	Russia
Malta	Russia
Netherlands	Russia
North Macedonia	Russia / UK
Spain	Russia/Venezuela
Taiwan	China
Ukraine	Russia
US	Russia

Examples included information disruption campaigns targeting French presidential candidate Emmanuel Macron (such as the theft and release of 21,000 emails just before the final vote in the election—a technique likely to be of enduring utility for adversaries)[43] and the spreading of disinformation by Russian media outlets *Russia Today* (*RT*) and *Sputnik* in Catalonia[44] and Italy with headlines like 'Migrant chaos, the beginning of a social war'[45] or claiming in the Macedonian referendum that, depending on who won, Google would remove Macedonian from its list of recognised languages.[46] Chinese-backed disinformation campaigns targeting Taiwan were reported as using zombie accounts and China's so-called '50 Cent Army' of online trolls and commentators to amplify the dissemination of disinformation.[47] In Ukraine, Russia sought to buy or rent Ukrainian Facebook accounts to disseminate disinformation.[48] There was also an unusual case of the UK's Foreign and Commonwealth Office being accused of funding British PR agency Stratagem International to help the Macedonian Government with its 'Yes' campaign on the changing of the country's name, thereby opening up the opportunity for Macedonia to join the EU and NATO.[49]

Research identified four alleged actors: Russia (the most dominant by far), China, Iran and the UK.

Long-term erosion of public trust in public institutions

Perhaps the most pernicious aspect of foreign interference is the longer term corrosion of public trust in the institutions that underpin democracy.

For example, the Center for Strategic and International Studies' Defending Democratic Institutions Project has looked at Russian efforts to weaken trust in the rule of law as administered by the justice systems in both the US and Europe.[50] In Australia, China is alleged to have attacked the Australian

Parliament in 2011 and 2019, as well as three political parties in 2019.[51] And in several countries attacks on electoral commissions responsible for impartially conducting elections have been reported.[52] If foreign adversaries can destroy trust in these pillar institutions and related organs of democracy, democracy quickly unwinds.

Making this phenomenon even harder to confront, it's often not immediately clear whether a campaign is being run by a nation-state or by conspiracy-oriented individuals. During the Brexit vote in the UK, what appeared to be a conspiracy theory (that had first surfaced during the 2014 Scottish referendum) spread online, urging voters to use pens, not pencils, to complete their ballot papers.[53] The not-so-subtle inference was that government officials were rubbing out ballots completed in pencil and changing people's votes (figures 1 and 2).

Figure 1: 'I voted in pencil'

Source: Professor Brian Cox, *Twitter*, 23 June 2016, online.

Figure 2: 'Use pens plea'

Source: *BBC News*, 22 June 2016, online.

It's difficult to know how damaging these sorts of campaigns are for public trust in critical democratic institutions or whether they're state-backed. What's apparent is that polling has picked up distrust in key electoral institutions. The *Australian voter experience* report revealed that just 42% of Australians have a great deal of confidence in the Australian Electoral Commission's ability to conduct an election, while a further 43% have 'some' confidence.[54] In the UK, just 21% reported that they were 'very confident' and 48% said they were 'fairly confident' that the 2015 election was well run.[55] While electoral commissions are generally off voters' radars, trust in democracy collapses if people lose trust in those organisations' ability to conduct elections impartially.

More significantly, there's also been a dramatic drop in levels of satisfaction with democracy in Australia. Although once again it's hard to track a causal relationship, it seems likely that democracies experiencing rising dissatisfaction with democracy would be more vulnerable to interference. The *Australian voter experience* report noted that just 55% of Australians "are satisfied with the way democracy works in their country nowadays. This places Australia on the lower end of established democracies, which typically have rates of satisfaction that exceed two-thirds. Historical data indicates that there's been a dramatic fall in satisfaction. Data from the Australian Election Study in 2007 indicated that 86% reported being satisfied with democracy, falling to 72% in 2013".[56] Surveys such as the Lowy Institute Poll have tracked this dissatisfaction with democracy and speculated about its causes, but with no definitive answers.[57]

The Democracy Perceptions Index 2018 provides hints to the growing levels of public distrust in democracies around the world. It found that 64% of the public in 'free' countries (as defined by Freedom House) said their government 'never' or 'rarely' acts in their interest, compared to 41% in 'not free' countries. In Australia, a third of Australian adults say the government 'mostly', 'often' or 'sometimes' acts in their interest (67% say it does so 'never' or 'rarely').[58] While this is a large proportion of the population, it hasn't yet resulted in French-style yellow vest protestors.[59]

In Australia and elsewhere, it's highly unlikely that this dissatisfaction is driven entirely by foreign interference. Anxiety about large economic and social changes brought about by globalisation and technological development could all be in play.[60] Longitudinal Gallup surveys have also picked up a long downwards trend in average trust in public institutions (Figure 3).[61]

Figure 3: Americans' average confidence in public institutions over time

Quantifying examples of the long-term erosion of public trust is perhaps the trickiest of tasks, as in many cases more immediate efforts to shape public opinion (such as spreading disinformation) also have the longer term impact of eroding public trust in the media and other institutions. Efforts to erode public trust also typically exploit existing societal cleavages,[62] making detection difficult and any additional impact from interference on pre-existing divisions hard to measure. However, for the purposes of this research, 10 states were identified as having experienced efforts to create long-term erosion of public trust: Australia, Brazil, the Czech Republic, Germany, Montenegro, Norway, the Netherlands, Singapore, Ukraine and the US (Table 4).

Table 4: Long-term erosion of public trust

Target	Actor
Australia	China
Brazil	Russia
Czech Republic	Russia
Germany	Russia
Montenegro	Russia
Norway	Russia
Netherlands	Russia
Singapore	China
Ukraine	Russia
US	Russia

Examples have included the use of social media bots in Brazil to question the democratic model,[63] amplification by Russia using Twitter bots of far-right Alternative für Deutschland's warnings about election fraud,[64] and systematic efforts by Russia to weaken 'faith in the rule of law as administrated by the justice system' in the US through the use of disinformation and the exploitation of 'legitimate criticisms of the justice system'.[65]

The two identified actors in this category were Russia and China.

Limitations

There are several notable limitations to this research.

First, we focused on states and therefore missed private actors that are distorting democratic debates in similar ways. For example, there have been several cases of the commercialisation of Russian-like disinformation campaigns. Consider the group in the Balkans that built up popular Facebook pages with titles such as 'Australians against Sharia' and 'Aussie infidels' that targeted Australians to generate ad revenue.[66] Future research could usefully explore the impact that these groups are having and how to counter them.

Second, our focus was on public cases, which perhaps tends to favour the identification of Russian efforts, given Moscow's more overt and detectable methods and the media's growing familiarity with its approach. Parallel research on CCP methods that the International Cyber Policy Centre is preparing suggests that Beijing often uses techniques that are harder to detect and longer term and so may be underreported. A broader methodology is probably needed to capture difficult-to-spot influence

activities such as subverting policy positions and decision-making as well as long-term campaigns to cultivate supportive political figures and voices and silence, pressure or sideline critics.[67]

Third, the focus on foreign state actors has, of course, excluded domestic efforts to harness these same techniques, for example by political parties and local activists that may also be contributing to voter dissatisfaction with democracy and trust in institutions.

Fourth, there has been a tendency to favour English-language sources.

Finally, the increasing ability to micro-target voters and the difficulty of detecting many of the types of interference reported here mean that many examples could be being missed in the online information arena. Consider the case of a Russian-operated fake Black Lives Matter Facebook page that was only reported as suspicious because it used the phrase 'Don't shoot'—an expression that genuine activists had stopped using.[68] The shift by major platforms such as Facebook to move from public broadcasting to private messaging will only accentuate this challenge.[69]

Findings and recommendations

The motivation behind this research is that, by better understanding the methods being used and the targets of high-activity adversary states, democracies will be able to better assess their existing response and mitigation capabilities and adjust as necessary.

We make the following recommendations.

1. Targets are limited: respond accordingly

Despite the enormous amount of media coverage that's been devoted to state-backed election interference, the phenomenon isn't universal. From public accounts, there are two primary actors and they focus judiciously on states that matter to them. Democracies should calibrate their policy responses to the likely risk, methods and adversary. The US and European states are clear targets of the Russian Government; Indo-Pacific nations are targets of the CCP.

2. Build up detection capabilities

More effort is needed to detect foreign interference, including offline and non-state efforts (such as by for-profit groups that misuse social media platforms to stir up hate). Because democracies have a natural aversion to government surveillance, a better answer than simply stepped-up government monitoring may be supporting non-profit, non-government initiatives and independent media. These groups can more credibly monitor for interference and more easily engage at the community level. In smaller states, where local media outlets are disappearing, government subsidies may be needed to ensure sufficient scrutiny of local and state political groups (which are often feeder groups for national politics).

3. Fund research to measure impact and measure the effectiveness of education campaigns to address public concerns

Governments should fund research to develop better ways to measure the impact of foreign interference to allow for a more informed decision on resourcing efforts to counter it. Notwithstanding the lack of current empirical data on impact, opinion polling points to a perception that foreign interference will occur, and in places such as the US to widely held views that elections have been swayed. Various efforts have been made to respond, including fact-checking services,[70] opening up social media data streams to election-oriented academic research,[71] and legislation to counter fake news.[72] Research is needed to understand which efforts are most effective, after which those tougher measures should be twinned with public awareness campaigns to address these concerns.

4. Publicly fund the defence of political parties

Political parties and politicians are clear targets of foreign adversaries. With their shoestring budgets and the requirement to scale up dramatically during election campaigns, they're no match for the resources of sophisticated state actors. Politicians are also vulnerable, including through the use of their personal devices. There's a strong public interest in preventing foreign states from being able to exploit breaches of both parties and individual politicians to undermine domestic political processes. Democratic governments should consider public funding to better protect all major political parties and to step up cybersecurity support to politicians.

5. Impose costs

Democracies need to look at better ways of imposing costs on adversaries. Because of spikes in interference activity around elections, they can be prone to being picked off or to discounting interference if the party that won benefited from it. Democracies should consider concerted joint global or regional action that looks beyond their own particular cases as well as more traditional approaches such as retaliatory sanctions. Legislation may also be needed to make it more difficult for foreign adversaries to operate (being mindful of the differing objectives of the two main actors)—this may be a second best for countries that find it too difficult to call out adversaries.

6. Look beyond the digital

Russian interference is detectable, if not immediately, then often after the event. This has generated a natural focus on Moscow's methods and activities. However, there are many more subtle ways to interfere in democracies. Research like this that focuses on digital attack mechanisms also misses more traditional and potentially more corrosive tactics, such as the provision of funding to political parties by foreign states and their proxies and the long-term cultivation of political influence by foreign state actors. Australia has recently passed legislation to counter more subtle forms of foreign interference[73] that were starting to be detected.[74] States, particularly those in the Indo-Pacific, should be attuned to these types of interference and make preparations to prevent, counter and expose them.

7. Look beyond states

Troubling public perceptions of democracy are unlikely to be explained by foreign interference alone. Foreign interference may, however, magnify or exploit underlying sources of tension and grievance in particular societies. A thorough response by government and civil society needs to consider a wider set of issues and threat actors, including trolls working for profit, and the health of the political and media environment (including by ensuring that local and regional media remain viable or are adequately funded).

Appendix: Examples of foreign interference (November 2016 to April 2019)

Sources for all examples can be found on the accompanying map at *Fortress.maptive.com*, online.[75]

Table 5: Voting infrastructure and voter turnout

Country/ year	Freedom House Freedom in the World status	Suspected state sponsor	Information
Colombia 2018	Partly free	Russia and Venezuela	According to *VOA News*, the Colombian Government and military officials have investigated 'tens of thousands' of cyber operations launched against the country's voter registration system in the lead-up to the 2018 parliamentary elections. The Colombian authorities traced the cyber operations to Venezuela, which was acting as 'a proxy for Russia'. It appears that the objective of the cyber operations was to jam the voter registration system.
Finland 2019	Free	Russia	According to the Finnish National Bureau of Investigation (Keskusrikospoliisi), a web service used to publish vote tallies was targeted by a denial of service (DoS) attack on the weekend of 6–7 April 2019, one week before the election was held. An attack like this on election night has the potential to impede the reporting of the election results and subsequently undermine the public's trust. The Finnish authorities have declined to speculate on the source of the DoS attack, as the police are still conducting their investigation; however, *Cybersecurity Insiders* noted that it's 'suspected to be the work of hackers backed by Russian Intelligence'. In response to the attack, Pekka Haavisto, the leader of Finnish political party the Green League, commented: 'This is one reason why a pencil and sheet of paper are still the best. Let's keep the system safe.'
Indonesia 2019	Partly free	Russia and China	The head of Indonesia's General Election Commission, Arief Buidman, alleged that Russian and Chinese hackers had attempted to discredit the polling process ahead of Indonesia's 2019 election by targeting the country's voter database. It was reported that attempts were made by the hackers to 'manipulate and modify' content on Indonesia's voter database and create fake voter identities, otherwise known as 'ghost voters'. According to *Bloomberg*, Buidman noted that 'it was unclear whether the motive was "to disrupt Indonesia" or to help one of the candidates win'.
North Macedonia 2018	Partly free	Russia	According to the *New York Times*, Russian operatives used Facebook to disseminate disinformation and depress voter turnout in the lead-up to the 2018 Macedonian referendum. They reportedly spread and promoted false articles and posts that would 'heighten social divisions, drive down participation and amplify public anger'. A key focus of the disinformation campaign was to encourage Macedonians to boycott the vote, and hundreds of new websites appeared, encouraging Macedonians to 'burn their ballots'. As the referendum required 50% of the registered voters to participate for it to be valid, this particular tactic was significant. While the Macedonian Government has declined to speculate on the source of the interference, in comments to reporters, then US Defense Secretary James Mattis accused Russia of financing 'influence campaigns' in an effort to spread disinformation ahead of the referendum.

Table 5: Voting infrastructure and voter turnout (continued)

Country/ year	Freedom House Freedom in the World status	Suspected state sponsor	Information
Ukraine 2019	Partly free	Russia	According to Serhiy Demedyuk, the head of the Ukrainian Cyber Police, Russian-backed hackers targeted the Central Elections Commission and its employees with phishing emails infected with malware in the lead-up to Ukraine's 2019 presidential election. Demedyuk noted that the 'virus-laden New Year's greetings have become … overwhelming'. Roman Boyarchuk, the head of Ukraine's Cyber Protection Centre, noted that since December around 8,000 targeted phishing emails were sent per week, as hackers attempted to probe the commission's website and obtain information on the communication network used to report the election results.
Ukraine 2019	Partly free	Russia	According to the *Kyiv Post*, in the lead-up to Ukraine's 2019 presidential election, the Central Election Commission was targeted by Russian-backed hackers and subjected to distributed denial of service (DDoS) attacks on 24 February and 25 February. Ukraine's then President, Petro Poroshenko, accused Russia of being the source of the attack.
US 2016	Free	Russia	According to Jeanette Manfra, head of cybersecurity at the Department of Homeland Security, Russian-backed hackers targeted the electoral systems of 21 US states to find vulnerabilities that would provide access to the voter registration databases. For the most part, the hackers engaged only in preliminary activities such as 'scanning and probing'; however, attempts were made to gain access to the electoral systems and 'an exceptionally small number of them were actually successfully penetrated'. Florida was one of the states targeted by the spear-phishing campaign targeting election officials; the *New York Times* reported that Russian-backed hackers had sent phishing emails containing 'a malicious Trojan virus' to 120 elections email accounts in the county. In 2019, Florida Senator Marco Rubio confirmed that at least one election office in his county had been compromised and that the hackers were 'in a position' to alter the voter roll data. Of the small number of electoral systems that were successfully penetrated, none has been reported to have had any voter rolls altered.
US 2016	Free	Russia	According to two reports commissioned by the Senate Intelligence Committee, produced by researchers from Oxford University's Computational Propaganda Project and cybersecurity firm New Knowledge, Russian operatives linked to the Internet Research Agency (IRA) specifically targeted African-Americans in the lead-up to the 2016 presidential election in an effort to suppress voter turnout. Bret Schafer, a social media analyst and communications officer at the Alliance for Securing Democracy, identified @WokeLuisa—an influential account in the #BlackLivesMatter community—as one of more than 3,000 accounts created by the IRA to target and manipulate the African-American community. Over a 12-month period, the fake @WokeLuisa account 'amassed more than 50,000 followers' and received 'hundreds of thousands of retweets and media coverage in more than two dozen prominent news outlets', enabling the widespread dissemination of disinformation. The Oxford University report noted that the Russian operatives posing as Americans online pushed the narrative that 'the best way to advance the cause of the African American community was to boycott the election and focus on other issues instead'. Renee DiResta, director of research at New Knowledge, noted that the IRA 'leveraged pre-existing, legitimate grievances wherever they could'. While it's difficult to determine the effect of the IRA's disinformation campaign, the Pew Research Center reported that the voter turnout of African-Americans fell in 2016.

Table 6: Information environment

Country/ year	Freedom House Freedom in the World status	Suspected state sponsor	Information
France 2017	Free	Russia	According to Richard Ferrand, then General Secretary of En Marche!, French presidential candidate Emmanuel Macron was the target of a disinformation campaign led by Russian state-sponsored media outlets. He commented: 'Two big media outlets belonging to the Russian state, *Russia Today* (*RT*) and *Sputnik*, spread fake news on a daily basis, and then they are picked up, quoted and influence the democratic [process].' For example, *Sputnik* published an interview on 4 February 2017 with French politician Nicolas Dhuicq, in which Dhuicq made derogatory comments about Macron's personal life and accused Macron of being an agent of 'the big American banking system' in an effort to undermine his electability.
France 2017	Free	Russia	En Marche! revealed in a statement that it had been the target of a 'massive, coordinated act of hacking' and that the hackers had obtained internal information, such as emails and documents. According to the Carnegie Endowment for International Peace, the hackers had used spear-phishing emails to obtain the login credentials of campaign staff; the emails redirected the targets to a fake Microsoft storage website where they were asked to enter their login details. Facebook confirmed that Russian operatives had set up 12 fake accounts and posed as acquaintances of people close to Macron to gain information. On the evening of 5 May 2017, just before the final vote between Macron and Le Pen, the 9 gigabytes of files and 21,000 emails stolen in the October 2016 data breach were released on the anonymous document-sharing website *Pastebin* under the username 'EMLEAKS'. Two months later, the documents and emails leaked to *Pastebin* were republished on WikiLeaks using the hashtag #MacronLeaks. Japanese cybersecurity firm Trend Micro confirmed that the initial phishing emails had been traced back to the Russian-backed hacker group, Fancy Bear.
France 2017	Free	Russia	According to *The Guardian*, state-sponsored media outlets were involved in the dissemination of disinformation in the lead-up to the 2017 presidential election. France's polling commission raised concerns over an article that contradicted 'the findings of mainstream opinion polls', placing François Fillon, the conservative presidential candidate, as the leading candidate in the election. The article had been posted and shared by several Russian state-sponsored media outlets, and *Sputnik* posted the article on 29 March 2017 under the headline: '2017 presidential elections: the return of Fillon at the head of polls'. *Sputnik*'s source was a study by Brand Analytics, a Russian-based 'online audience research firm', which France's polling commission noted was not representative of public opinion in France.
Israel 2019	Free	Iran	According to *Reuters*, Israel's security service, Shin Bet, alleged that hackers linked to Iran had accessed the phone of Benny Gantz, leader of the centrist political alliance Kahol Lavan, and retrieved personal and professional information. The timing of the data breach raised concerns that the stolen information could be used to discredit Gantz and undermine his electability.
Italy 2018	Free	Russia	According to *La Stampa*, five Twitter accounts with 'similar characteristics to those of Russian trolls' were engaged in the dissemination of disinformation and propaganda in the lead-up to the 2018 Italian election, providing a one-sided representation of the political discourse in favour of the populist parties. Russian-backed hackers reportedly stole the identities of Italian citizens and posed as political activists to manipulate the public discourse.

Table 6: Information environment (continued)

Country/ year	Freedom House Freedom in the World status	Suspected state sponsor	Information
Italy 2018	Free	Russia	According to Alto Data Analytics, Russian state-sponsored media outlets *Sputnik* and *RT* played a significant role in the creation of anti-immigration narratives in the year prior to and in the lead-up to the 2018 Italian election. The analysis by Alto Data Analytics examined the polarising role of Russian state-sponsored media outlets within societal debates, as they tend to reinforce and exploit local narratives, leading to an imbalance in the narratives that are published. For example, one article published by *Sputnik* read: 'Migrant chaos, the beginning of a social war'.
Italy 2018	Free	Russia	According to *The Local*, Twitter accounts linked to the Internet Research Agency (IRA) launched an extensive disinformation campaign in the lead-up to Italy's 2018 general election in an effort to 'support the two Italian populist parties' and influence the outcome of the election.
North Macedonia 2018	Partly free	Russia	According to the Digital Forensic Research Lab (DFRLab), the coverage provided by Russian state-sponsored media outlets *Sputnik* and *RT* in the lead-up to the Macedonian referendum was unbalanced, providing one-sided content in an effort to create confusion and polarise Macedonia's information environment. An article that was widely shared falsely warned that, depending on the outcome of the vote, Google would remove Macedonian from its list of recognised languages. Similarly, before the Macedonians were due to vote, *Sputnik* published an article that falsely claimed 'between 80 percent and 90 percent of Macedonians will boycott the referendum'.
North Macedonia 2018	Partly free	UK	According to the *Bureau of Investigative Journalism*, British PR agency Stratagem International, which 'specialises in "under the radar" operations to influence voters', was employed by the Macedonian Government to assist with the 'Yes' campaign and received funding from the UK's Foreign and Commonwealth Office. Stratagem International confirmed that it was being funded by the Foreign Office as 'a resource for the referendum Taskforce (Yes Campaign)'.
Malta 2017	Free	Russia	According to the Maltese Government, Russian-backed hackers attempted to access and disrupt its server in the month before Malta's 2017 general election. A source working within the Maltese Government's IT agency noted that the hackers had attempted to gain access to the IT system by sending phishing emails, mounting DDoS attacks and using malware. In a one-month period, around 5 million phishing emails were sent. *The Observer* confirmed that Russian hacker group Fancy Bear had been identified by a 'confidential external risk assessment' as the source of the attack. *The Guardian* reported that 'the attacks come after recent claims from the prime minister, Joseph Muscat, that a foreign intelligence agency had suggested Malta would become a target for a Russian disinformation campaign.'
Netherlands 2017	Free	Russia	The annual report of the General Intelligence and Security Service in the Netherlands confirmed that Russia had attempted to influence the 2018 Dutch election through the dissemination of disinformation. Rob Bertholee, the head of the service, noted that Russia had 'tried to push voters in the wrong direction by spreading news items that are not true, or partially true.'

Table 6: Information environment (continued)

Country/ year	Freedom House Freedom in the World status	Suspected state sponsor	Information
Spain 2017	Free	Russia	According to *El País*, the Russian state-sponsored media outlets *Sputnik* and *RT* were openly spreading disinformation and propaganda in favour of independence in the lead-up to the controversial Catalonia referendum in 2017. *RT Actualidad*, *RT*'s Spanish-language outlet, 'spread stories on the Catalan crisis with a bias against constitutional legality', notably misrepresenting the EU's position regarding the referendum. Between 27 August and 28 September 2017, *RT Actualidad* published 42 articles concerning the referendum, all of which promoted some form of disinformation. Professor Javier Lesaca, a visiting scholar at George Washington University, analysed more than 5 million social media posts between 29 September and 5 October 2017 and found that there was an 'entire army of zombie accounts' dedicated to sharing content by *Sputnik* and *RT*. Lesaca noted that 'the digital disruption' observed in the public discourse surrounding the 2016 US presidential election and the 2016 Brexit referendum was also observed in the lead-up to the Catalonia referendum, and that the 'authors of the disruption are the very same'.
Spain 2017	Free	Russia and Venezuela	According to *El País*, WikiLeaks founder Julian Assange acted as a 'principal international agitator in the Catalan Crisis', promoted and amplified by Russian state-sponsored media outlets and Twitter bots, respectively. In the lead-up to the referendum, Assange used Twitter as a forum to criticise the Spanish Government, 'sharing opinions and half truths as if they were news'. Ben Nimmo, an analyst with the Digital Forensic Research Lab (DFRLab), noted that Assange had not tweeted on the crisis in Catalonia prior to September 2017, meaning that the decision by the Russian state-sponsored media outlets, in particular *Sputnik*, to amplify his tweets 'can't be justified on his experience'. Nimmo suggested that Assange's tweets were used purely because 'he was criticising Spain' and that it was consistent with the outlets' intended narrative. NewsWhip, a media monitor that tracks social media engagement, reported that a tweet published by Assange on 15 September 2017 had the most engagement in the lead-up to the referendum. The tweet received 12,000 retweets and 16,000 likes within a 24-hour period, which *El País* suggested was evidence of social media manipulation through amplification. The DFRLab confirmed *El País*' suggestion of bot amplification, noting that the 'speed of the traffic' supported *El País* reports that Venezuelan accounts had been used by the Russians to assist with the dissemination of disinformation, acting as a proxy.
Taiwan 2018	Free	China	Taiwanese officials alleged that the People's Republic of China launched an online disinformation campaign in the lead-up to Taiwanese 2018 midterm elections in an effort to undermine the Democratic Progressive Party, led by President Tsai Ing-Wen, and support 'candidates more sympathetic to Beijing', specifically the Kuomintang. According to *BBC Insight*, Chinese state-sponsored media outlets, such as the *Global Times*, *Straits Today* and *Taihai Net*, were actively engaged in the dissemination of disinformation 'circulating Taiwan-related '"fake news"'. According to Foreign Minister Joseph Wu, disinformation and propaganda in the lead-up to the elections was being spread 'not from newspapers or [China's] propaganda machine but through [Taiwan's] social media, online chat groups, Facebook, the zombie accounts set up somewhere, by the Chinese government'. Democratic Progressive Party politician Lo Chi-cheng told *al-Jazeera* that China's 'so-called "50 Cent Army" of online trolls and commentators' had been used to amplify the dissemination of disinformation.

Table 6: Information environment (continued)

Country/ year	Freedom House Freedom in the World status	Suspected state sponsor	Information
Ukraine 2019	Partly free	Russia	The Security Service of Ukraine reported that it had countered a Russian attempt to use Facebook to undermine the vote in the 2019 Ukrainian election. In an effort to circumvent Facebook's new safeguards and interfere in the election, instead of setting up fake accounts, Russian operatives sourced 'people in Ukraine on Facebook who wanted to sell their accounts or temporarily rent them out' and then used the accounts to manipulate voter attitudes through the dissemination of disinformation.
Ukraine 2019	Partly free	Russia	According to the *Kyiv Post*, the website of presidential candidate Volodymyr Zelenskiy was subjected to a DDoS attack on 1 January 2019. The attack occurred after Zelenskiy had announced his intention to run for president and called on his supporters to join his team by registering online using the website. Zelenskiy's website received 5 million requests within minutes of its launch and was quickly taken offline. While Zelenskiy and his team declined to speculate on the source of the attack, *Vice News* reported that cyber experts suspected Russia as the source of the attack.
US 2016	Free	Russia	According to the DFRLab, Twitter accounts linked to Russia's IRA were involved in a widespread disinformation campaign in the lead-up to the 2016 presidential election in an effort to influence US public opinion. Two reports released by the Senate Intelligence Committee, commissioned by researchers from Oxford University's Computational Propaganda Project and cybersecurity firm New Knowledge, examined the Russian disinformation campaign led by the IRA. New Knowledge's report found that, as part of the disinformation campaign, the IRA created fake and deceptive social media accounts on almost every social media platform to engage with and manipulate the public discourse. Russian operatives used the accounts, which were designed to look like they belonged to everyday Americans, to amass followers based on an innocuous theme before shifting to another more divisive theme. The accounts were also used to promote fake advertisements targeted at specific users.
US 2016	Free	Russia	According to cybersecurity firm Trend Micro, in March 2016 a hacker group with links to the Russian military intelligence agency, known as Fancy Bear, targeted members of the Democratic National Committee (DNC) with phishing emails. After gaining access to the DNC network, the group stole a significant amount of data, including nearly 20,000 emails and 8,000 attachments, sent by and to the DNC. The hackers released the stolen data over several months. The first lot was released by Guccifer 2.0., a hacker persona created by Russian military intelligence officers, and *DCLeaks.com*. The second lot were released three days before the Democrats' national convention, when WikiLeaks published 19,252 documents that it had received from Russian-backed hackers through an intermediary.
US 2016	Free	Russia	According to Meredith Kelly, spokeswoman for the Democratic Congressional Campaign Committee, the committee was targeted by a hacker group in an intrusion that resembled the Russian-backed hacking of the DNC. *Techcrunch* reported that the hackers were able to obtain the credentials of a systems administrator with 'unrestricted access' to the committee's server. The Mueller Report confirmed that the actors involved were part of the hacker group with links to the Russian military intelligence agency known as Fancy Bear.
US 2016	Free	Russia	According to the *New York Times*, on 19 March 2016 Russian-backed hackers sent a phishing email to John Podesta, then Hillary Clinton's campaign chairman, which contained a link redirecting him to a login site prompting him to enter his credentials. When Podesta did so, the hackers gained complete access to his email account, from which they stole 50,000 emails. The Mueller Report confirmed that the actors involved were part of the Russian-backed hacker group known as Fancy Bear.

Table 6: Information environment (continued)

Country/ year	Freedom House Freedom in the World status	Suspected state sponsor	Information
US 2018	Free	Russia	According to the *New York Times*, the Twitter accounts linked to Russia's IRA that were involved in the widespread disinformation campaign in the lead-up to the 2016 presidential election 'were at it again before the Midterms'. Nathaniel Gleicher, Facebook's head of cybersecurity policy, confirmed that Facebook had removed more than 100 accounts from Facebook and Instagram 'due to concerns that they were linked to the Russian-based Internet Research Agency'.
US 2018	Free	Russia	According to *The Daily Beast*, the office of US Senator Claire McCaskill was targeted by a phishing campaign in which staffers received 'forged notification emails' claiming that their Microsoft Exchange password had expired and prompting them to change it using a link provided in the email. The link redirected the target to a 'convincing replica of the US Senate's Active Directory Federation Services … login page', which displayed a 'single sign-on point for e-mail and other services'. The *Beast* noted that the tactic used 'was a variant of the password-stealing technique used by Russia's so-called "Fancy Bear" hackers against [Hillary] Clinton's campaign chairman, John Podesta in 2016'. Following the report by the *Beast*, Senator McCaskill confirmed that Russian-backed hackers had attempted to gain access to her office's server, but noted that they were 'not successful'. This incident was the first reported case of Russian interference in the 2018 midterm elections and involved 'a critical vote that could shape the remainder of the President Donald Trump's presidency'. The week before the *Beast* published its report, Tom Burt, the corporate vice president for customer security and trust at Microsoft, noted that Russian-backed hackers had registered a phishing page as a Microsoft account to target several midterm candidates.
US 2018	Free	Russia	According to the DFRLab, Russian state-sponsored media outlet *RT*'s coverage of the 2018 US midterms was decidedly one-sided, favouring the Republican party and its candidates, as well as providing links to Republican campaign advertisements.
US 2018	Free	Russia	According to the *New York Times*, a group of internet trolls linked to the Russian IRA attempted to influence American voters in the lead-up to the 2018 midterm elections using social media platforms, such as Facebook and Instagram, to disseminate disinformation. In response, Facebook removed 115 accounts engaged in 'inauthentic coordinated behaviour'.

Table 7: Long-term erosion of public trust

Country/ year	Freedom House Freedom in the World status	Suspected state sponsor	Information
Australia 2019	Free	China	On 18 February 2019, Australian Prime Minister Scott Morrison confirmed that a hacker group had targeted the Liberal, Labor and National parties and accessed the servers at Parliament House. The Prime Minister has noted that the breach, which occurred on 8 February 2019, was the work of a 'sophisticated state actor'. While the Australian Government hasn't specified which state was suspected of carrying out the operation, many commentators publicly identified China as the most likely.
Brazil 2018	Free	Russia	According to cybersecurity firm FireEye, a front group for Russia attempted to interfere in the 2018 Brazilian elections by using Twitter bots. The bots were used to artificially increase the reach of Facebook and Twitter posts that questioned Brazil's democratic model and the legitimacy of the election. For example, the bots increased the reach of the hashtag #OpEleiçãoContraOFascismo (Operation Against Fascism).
Czech Republic 2017	Free	Russia	According to *The Guardian*, Russian state-sponsored media outlets *Sputnik* and *RT* published disinformation, largely concerning migrants, to disrupt the public discourse in the lead-up to the Czech Republic's 2017 general election. Despite the difficulty of attribution, officials were convinced that Russia was behind the disinformation campaign. Then Czech State Secretary for European Affairs Tomáš Prouza commented that Russia was aiming to 'sow doubts into the minds of the people that democracy is the best system to organise a country … and discourage people from participation in the democratic processes'. Polls revealed that the online disinformation campaign had influenced public opinion, which in turn threatened to destabilise the Czech Republic's democratic system.
Germany 2018	Free	Russia	According to the DFRLab, in the lead-up to the 2017 German federal election the far-right Alternative für Deutschland party (AfD) 'pushed a narrative warning about possible fraud and calling on supporters to volunteer as election observers'. The DFRLab found that the AfD's questionable narrative concerning the electoral process was amplified by Russian-language bots on the Russian social media platform Vkontakte, which reportedly 'boasts a significant German audience' and is 'the 8th most popular website in Germany based on traffic'. The bots' amplification of the AfD's narrative had the potential to erode public trust in the electoral process.
Montenegro 2018	Partly free	Russia	According to *Balkan Insight*, Montenegrin institutions were targeted with phishing emails in the months before the country's 2017 election. The first cyber operation occurred at the start of January 2017, when spear-phishing emails with the subject line 'NATO_secretary_meeting.doc' were sent to the Montenegrin Defence Ministry. The same tactic was used later that month to gain access to the Podgorica government's server, when two spear-phishing emails were sent with the subject lines 'Draft schedule for British army groups' visit to Montenegro' and 'Schedule for a European military transfer program'. Cybersecurity firms FireEye, Trend Micro and ESET all confirmed that the hacker group Fancy Bear was responsible for the cyber operations against the Montenegrin institutions.

Table 7: Long-term erosion of public trust (continued)

Country/ year	Freedom House Freedom in the World status	Suspected state sponsor	Information
Netherlands 2017	Free	Russia	According to *de Volkskrant*, two Russian-backed hacker groups, Fancy Bear and Cozy Bear, attempted to gain access to ministries in the Netherlands, including the Ministry of General Affairs, where Prime Minister Mark Rutte has his office. The hacking attempts took place over six months and were apparently unsuccessful, as the hackers were unable to obtain any confidential information or credentials. Rob Bertholee, head of the General Intelligence and Security Service in the Netherlands, confirmed that Russia was 'trying to penetrate secret government documents'. In response to concerns over Russian 'hacking', and vulnerabilities found in the counting software, the Dutch Government decided to change the way votes were counted and reverted to paper ballots prior to the elections on 15 March.
Norway 2017	Free	Russia	According to *The Local Norway*, the Norwegian Police Security Service discovered that the Labour Party had been 'subjected to an attempted digital attack' by a hacker group with 'ties to foreign intelligence'. *Dagbladet* reported that the attempted digital attack had been carried out by the same group that hacked the Democratic National Committee in the US: the Russian-backed hacker group Fancy Bear.
Singapore 2017	Partly free	China	According to *BBC News*, hackers gained access to Singapore's national health database and stole the personal data of 1.5 million people who had visited clinics between May 2015 and July 2017. The data breach occurred between 27 June and 4 July 2017. In a statement, the government confirmed that the breach had been part of a 'deliberate, targeted and well-planned attack' and that the hackers had stolen '[i]nformation on the outpatient dispensed medicines of about 160,000' people, including the medical information of Prime Minister Lee Hsien Loong. While the Singaporean authorities have declined to speculate on the source of the attack, commentators have publicly identified China as the most likely.
Ukraine 2019	Partly free	Russia	According to *Coda*, following the first round of voting in Ukraine's 2019 presidential election, Russian state-sponsored media outlets criticised the results, which placed Volodymyr Zelenskiy ahead in the polls, and claimed that the election was 'a rigged contest'. Russian state-sponsored media also published disinformation about Zelenskiy, linking him to the 2019 Notre Dame fire to undermine his electability.
US 2018	Free	Russia	According to Suzanne Spaulding and Harvey Rishikof, the leaders of the Defending Democratic Institutions Project at the Center for Strategic and International Studies, Russia has been engaged in a long-term campaign to 'weaken our institutions of American democracy'. Spaulding and Rishikof's project has examined Russia's attempts to undermine democracy by weakening 'faith in the rule of law as administered by the justice system' through the use of disinformation and the exploitation of 'legitimate criticisms of the justice system'.
US 2018	Free	Russia	According to the *New York Times*, Russian operatives engaged in an elaborate disinformation campaign, known as Project Lakhta, in the lead-up to the 2016 presidential election. David Holt, a special agent from the Federal Bureau of Investigation, noted that the goal of the Russian disinformation campaign was to 'sow division and discord in the US political system'. The *New York Times* reported that Project Lakhta's 'chief accountant', Elena Alekseevna Khusyaynova, purchased 'internet domain names and Facebook and Instagram ads' and exploited thousands of social media accounts by funding the promotion of 'divisive posts'.

Table 7: Long-term erosion of public trust (continued)

Country/ year	Freedom House Freedom in the World status	Suspected state sponsor	Information
US 2018	Free	Russia	According to *ThinkProgress*, a website claiming to be associated with Russia's IRA published a list of social media accounts that it had purportedly created and suggested that the social media platforms and intelligence services had captured only '1/25 of the whole picture', highlighting the failure of Facebook's identification methods and security protocols.
US 2018	Free	Russia	According to a report by cybersecurity firm New Knowledge, the Russian IRA has used fake and deceptive social media accounts to amplify President Donald Trump's attacks against Robert S Mueller and his investigation into Russian interference in the 2016 presidential election.

Notes

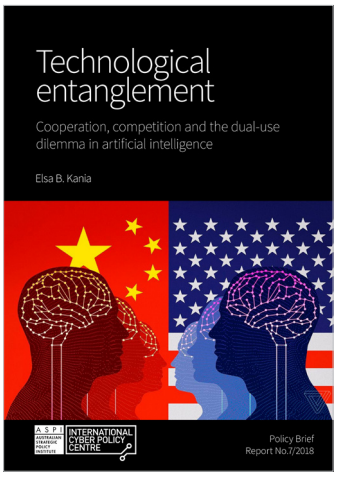
1 This has been comprehensively documented; see, for example, Office of the Director of National Intelligence (ODNI), *Background to 'Assessing Russian activities and intentions in recent US elections': the analytic process and cyber incident attribution*, US Government, 6 January 2017, online; PN Howard, B Ganesh, D Liotsiou, J Kelly, *The IRA, social media and political polarization in the United States, 2012–2018*, Computational Propaganda Research Project, Oxford University, 2018, online.
2 ElectionGuide: democracy assistance and elections news, online.
3 Malcolm Turnbull, 'Speech introducing the National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017', 7 December 2017, online.
4 Jacob Poushter, Janell Fetterolf, *International publics brace for cyberattacks on elections, infrastructure, national security*, Pew Research Center, 9 January 2019, online.
5 'Americans' views on Russia, the 2016 election, and US–Russian relations (trends)', news release, Gallup, August 2018, online.
6 Matthew Cole, Richard Esposito, Sam Biddle, Ryan Grim, 'Top-secret NSA report details Russian hacking effort days before 2016 election', *The Intercept*, 6 June 2017, online; Zeynep Tufekci, 'The election has already been hacked', *New York Times*, 3 November 2018, online.
7 Ishaan Tharoor, 'The long history of the US interfering with elections elsewhere', *Washington Post*, 13 October 2016, online.
8 'As many as 146 million people on Facebook may have received information from Russian agency, Zuckerberg says', *PBS News Hour*, 9 April 2018, online.
9 Mark Clayton, 'Ukraine election narrowly avoided "wanton destruction" from hackers', *Christian Science Monitor*, 17 June 2014, online.
10 Claire Allbright, 'A Russian Facebook page organized a protest in Texas. A different Russian page launched the counterprotest', *Texas Tribune*, 1 November 2017, online.
11 Karen Yourish, Troy Griggs, '8 US intelligence groups blame Russia for meddling, but Trump keeps clouding the picture', *New York Times*, 2 August 2018, online.
12 *Freedom in the world 2018: democracy in crisis*, Freedom House, 2018, online.
13 Zoe Hawkins, *Securing democracy in the Digital Age*, ASPI, Canberra, 29 May 2017, online.
14 Brett Worthington, 'Scott Morrison reveals foreign government hackers targeted Liberal, Labor and National parties in attack on Parliament's servers', *ABC News*, 18 February 2019, online.
15 Danielle Cave, Tom Uren, 'Espionage or interference? The attack on Australia's parliament and political parties', *The Strategist*, 21 February 2019, online.
16 Michael Shoebridge, 'Attributing the hack on Australia's parliament will give clarity to the China relationship', *The Strategist*, 7 May 2019, online.
17 Many examples from other countries were excluded where there was insufficient evidence tying it to state-backed interference.
18 ODNI, *Background to 'Assessing Russian activities and intentions in recent US elections': the analytic process and cyber incident attribution*.
19 For example, the favouring of then-presidential candidate Donald Trump over Hillary Clinton; ODNI, *Background to 'Assessing Russian activities and intentions in recent US elections': the analytic process and cyber incident attribution*.
20 James Reinl, '"Fake news" rattles Taiwan ahead of elections', *al-Jazeera*, 23 November 2018, online.
21 Chris Uhlmann, Andrew Greene, 'Chinese donors to Australian political parties: who gave how much?', *ABC News*, 8 June 2017, online.
22 For broader perspectives on how China is undermining democracies and using these and other techniques, see Andrea Kendall-Taylor, David Shullman, 'How Russian and China undermine democracy', *Foreign Affairs*, 2 October 2018, online; John Garnaut, 'Australia's China reset', *The Monthly*, August 2018, online.
23 See appendix for details.
24 Clayton, 'Ukraine election narrowly avoided "wanton destruction" from hackers'.
25 Techniques not yet documented.
26 Howard et al., *The IRA, social media and political polarization in the United States, 2012–2018*, 19.
27 See, for example, Renee DiResta, Kris Shaffer, Becky Ruppel, David Sullivan, Robert Matney, Ryan Fox, Jonathan Albright, Ben Johnson, *The tactics and tropes of the Internet Research Agency*, no date, 8, online.
28 Martin Arostegui, 'Colombia probes voter registration cyberattacks traced to Russia's allies', *VOA*, 15 March 2018, online.
29 Viriya Singgih, Arys Aditya, Karlis Salna, 'Indonesia says election under attack from Chinese, Russian hackers', *Bloomberg*, 13 March 2019, online.
30 Cynthia McFadden, William M Arkin, Kevin Monahan, 'Russians penetrated US voter systems, top US official says', *NBC News*, 8 February 2018, online.
31 Kati Pohjanpalo, 'Finland detects cyber attack on online election-results service', *Bloomberg*, 10 April 2019, online.
32 'Poroshenko reports on DDOS-attacks on Ukrainian CEC from Russia on Feb. 24–25', *Kyiv Post*, 26 February 2019, online.
33 Marc Santora, Julian E Barnes, 'In the Balkans, Russia and the West fight a disinformation-age battle', *New York Times*, 16 September 2018, online.
34 DiResta et al., *The tactics and tropes of the Internet Research Agency*.
35 Howard et al., *The IRA, social media and political polarization in the United States, 2012–2018*, 19.
36 Howard et al., *The IRA, social media and political polarization in the United States, 2012–2018*; Jens Manuel Krogstad, Mark Hugo Lopez, *Black voter turnout fell in 2016, even as a record number of Americans cast ballots*, Pew Research Center, 12 May 2017, online.
37 Bret Schafer, 'Race, lies and social media: how Russia manipulated race in America and interfered in the 2016 elections', *State of Black America*, 2019, online.
38 *Democracy Perception Index 2018*, Alliance of Democracies, June 2018, 7, online.
39 Lydia Saad, 'Military, small business, police still stir most confidence', news release, Gallup, 28 June 2018, online.
40 DiResta et al., *The tactics and tropes of the Internet Research Agency*.
41 'French presidential candidate Macron target of Russian "fake news," his party chief claims', *Deutsche Welle*, 13 February 2017, online.
42 Schafer, 'Race, lies and social media: how Russia manipulated race in America and interfered in the 2016 elections'.
43 'WikiLeaks publishes searchable archive of Macron campaign emails', *Reuters*, 1 August 2017, online.
44 David Alandete, 'Russian meddling machine sets sights on Catalonia', *El Pais*, 28 September 2017, online.
45 *The construction of anti-immigration electoral messages in Italy*, Alto Data Analytics, no date, online.
46 Santora & Barnes, 'In the Balkans, Russia and the West fight a disinformation-age battle'.
47 Reinl, '"Fake news" rattles Taiwan ahead of elections'.
48 Michael Schwirtz, Sheera Frenkel, 'In Ukraine, Russia tests a new Facebook tactic in election tampering', *New York Times*, 29 March 2019, online.

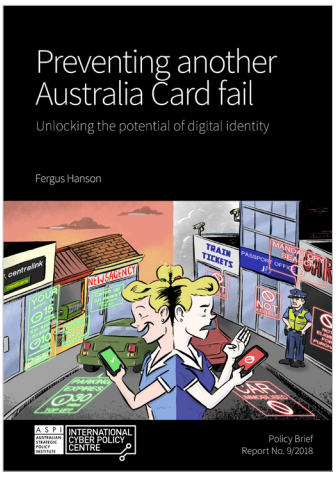
49 Jessica Purkiss, 'Russian warriors and British PR firms: Macedonia's information war', *Bureau of Investigative Journalism*, 28 September 2018, online; Jessica Purkiss, 'Macedonia name referendum: Russian warriors and British PR firms fight it out for the country's soul', *The Independent*, 28 September 2018, online.
50 Suzanne Spaulding, Harvey Rishikof, 'How Putin works to weaken faith in the rule of law and our justice system', *Lawfare*, 17 September 2018, online.
51 David Wroe, 'China key suspect in pre-election hack against major parties', *Sydney Morning Herald*, 18 February 2019, online.
52 See, for example, Pavel Polityuk, 'Exclusive: Ukraine says it sees surge in cyber attacks targeting election', *Reuters*, 26 January 2019, online; Singgih et al., 'Indonesia says election under attack from Chinese, Russian hackers'.
53 Melissa Etehad, 'Pencil or pen? An unusual conspiracy theory grips Brexit vote', *Washington Post*, 23 June 2016, online.
54 See Jeffrey Karp, Alessandro Nai, Ferran Martinez i Coma, Max Grömping, Pippa Norris, *New policy report: the Australian voter experience*, Electoral Integrity Project, January 2017, 17, online. Potentially, this result was affected by the interruption to the 2016 census administered by the Australian Bureau of Statistics and caused by a DDoS attack; *Census 2016: Lessons learned—improving cyber security culture and practice*, Institute of Public Administration, 13 December 2016, online.
55 Karp et al., *New policy report: the Australian voter experience*, 17.
56 Karp et al., *New policy report: the Australian voter experience*, 16.
57 The author drafted this question; Sam Roggeveen, 'Lowy poll: Are we losing faith in democracy?', *The Interpreter*, 23 June 2017, online.
58 *Democracy Perception Index 2018*, Alliance of Democracies.
59 'France fuel protests: who are the people in the yellow vests?', *BBC News*, 1 December 2018, online.
60 See, for example, Niraj Chokshi, 'Trump voters driven by fear of losing status, not economic anxiety, study finds', *New York Times*, 24 April 2018, online.
61 Saad, 'Military, small business, police still stir most confidence'.
62 Darren Lim, Isabella Hansen, 'Doxing democracy: lessons from election interference in the US and France', *The Strategist*, 17 July 2018, online.
63 Bruno Benevides, 'Russian hackers are trying to interfere in Brazilian elections, cybersecurity firm says', *Folha de S. Paulo*, 5 October 2018, online.
64 '#ElectionWatch: disinformation in Deutschland', *Medium.com*, 28 September 2017, online.
65 Spaulding & Rishikof, 'How Putin works to weaken faith in the rule of law and our justice system'.
66 Michael Workman, Stephen Hutcheon, 'Facebook trolls and scammers from Kosovo are manipulating Australian users', *ABC News*, 16 March 2019, online.
67 See John Garnaut's analysis of Chinese Communist Party interference in Australia, 'How China interferes in Australia: and how democracies can push back, *Foreign Affairs*, 9 March 2018, online.
68 Schafer, 'Race, lies and social media: how Russia manipulated race in America and interfered in the 2016 elections'.
69 Mike Isaac, 'Facebook's Mark Zuckerberg says he'll shift focus to users' privacy', *New York Times*, 6 March 2019, online.
70 'Fact-checking on Facebook: what publishers should know', *Facebook*, no date, online.
71 'Facebook will open its data up to academics to see how it impacts elections', *MIT Technology Review*, 30 April, online.
72 'Germany approves plans to fine social media firms up to €50m', *The Guardian*, 30 June 2017, online.
73 National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2018, online.
74 Legal and Constitutional Affairs Legislation Committee, *Estimates*, Australian Senate, 24 May 2018, online.
75 'ASPI election interference map', *Fortress.maptiv.com*, online.

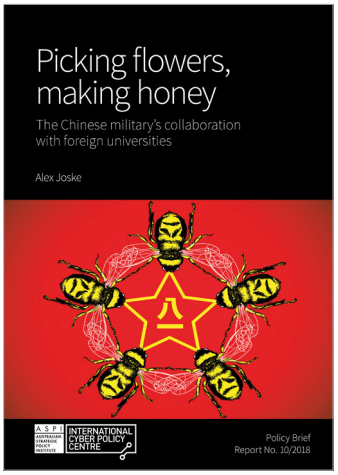
Acronyms and abbreviations

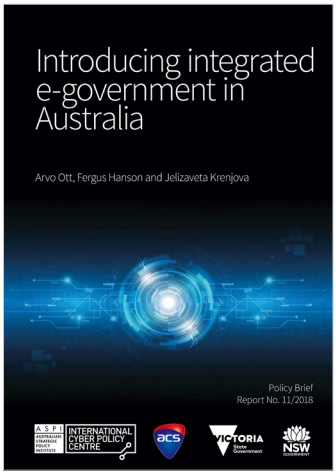
AfD	Alternative für Deutschland
CCP	Chinese Communist Party
DDoS	distributed denial of service
DNC	Democratic National Committee (US)
DoS	denial of service
EU	European Union
NATO	North Atlantic Treaty Organization
RT	*Russia Today*
UK	United Kingdom

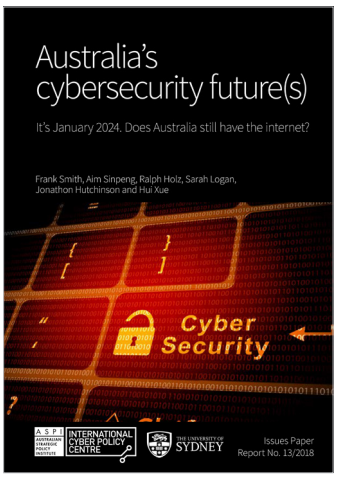
Some previous ICPC publications

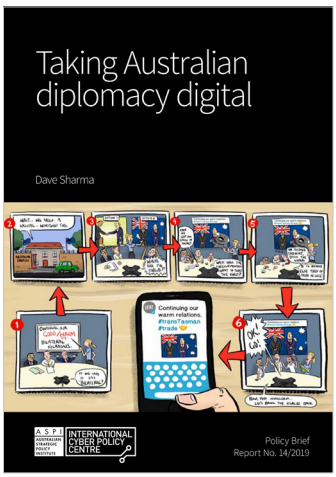


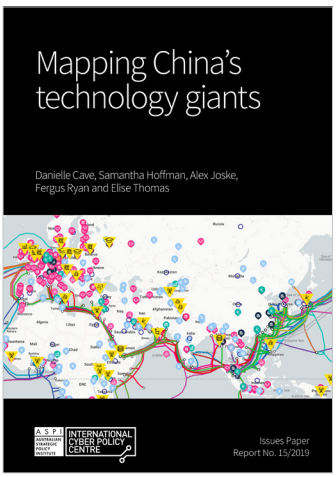












ASPI
AUSTRALIAN STRATEGIC POLICY INSTITUTE

INTERNATIONAL CYBER POLICY CENTRE

acs