



6 April 2021

Inquiry into the 2020 general election and referendums

InternetNZ submission to the Justice Committee

Introduction

InternetNZ supports a better Internet for people in New Zealand

1. InternetNZ is a not-for-profit that is the home and guardian for the .nz domain. Our work includes funding Internet research and community projects, hosting events like NetHui to bring together the Internet community, and doing policy work to support an Internet for all and an Internet for good.

We welcome the chance to submit in writing and wish to appear

2. We welcome the opportunity to submit on the Inquiry into the 2020 general election and referendums. Our submission is part of our work to help build an Internet for all and an Internet for good. We are most interested in theme 2: the integrity and security of our electoral system in light of emerging challenges, with a particular focus on technology and social media.
3. We wish to appear in person to speak to this submission. Please contact the policy team through james@internetnz.net.nz or call 0211565596.

Community trust depends on building trust online

New Zealanders need confidence in our election processes

4. New Zealanders deserve election processes that uphold public confidence, but that confidence faces challenges from shifts in technology and society.¹

The experience of COVID-19 has made online trust more vital

5. Building trust across the community is at the core of election processes, and has also been vital to the New Zealander's success in containing risks from COVID-19, which we have done by working together as a team of 5 million.
6. Living through COVID-19 has also made the Internet more vital to New Zealanders lives, with people relying more on online ways to work, shop, learn, and connect socially. But as the online environment has become more vital to daily life, it has also become a forum for serious risks to social trust.
7. We think the spread of misinformation online, in ways that affect people and communities in New Zealand, is a pressing risk for confidence in elections.

¹ Under section 4C of the Electoral Act 1993, objectives of the Electoral Commission include participation, understanding, and confidence in the electoral system.

Issues we raised in the previous inquiry remain unaddressed

8. [Our 2019 submission to the previous election inquiry \(attached\)](#) focused on online risks from foreign interference, raising concerns about cybersecurity issues for election campaigns, transparency for online election advertising, and risks to public confidence in elections from online misinformation.² We also recommended steps that could be taken to help address our concerns.
9. Over the past two years, our concerns have become more pressing, but as far as we know remain unaddressed. The one action we know of is the release of security guidance on foreign interference risks for elected officials.³ While this is a small positive step, it does not address our concerns with campaign security, transparency in online advertising, or risks that the spread of dis- and mis- information online could undermine confidence in elections.
10. To respond to these unaddressed concerns, we make the following recommendations drawn from our earlier 2019 submission. We recommend the following to address cybersecurity concerns for campaigns:

R1 We recommend the Committee request a briefing on options available to protect election campaigns against cybersecurity risks, including:

- (a) Creating a New Zealand equivalent of the Belfer Center's Cybersecurity Campaign Playbook before the next election**
- (b) Resourcing an independent agency to offer technical support to protect election campaigns from cybersecurity risks.**

11. To respond to concerns about online advertising we recommend:

R2 We recommend the Committee request a briefing on options available to increase the transparency of online advertising, including:

- (a) Tasking the Electoral Commission to review and implement requirements for transparent online election advertising;**
- (b) Considering options for online tools to allow easy compliance, monitoring, and reporting of election advertising as open data through the Electoral Commission;**
- (c) Extending the regulation of online campaigns to include the post-election, pre-government-formation time period;**
- (d) Considering lower spending thresholds to require registration for online election campaigns based on their potential reach and impact;**

² InternetNZ, Submission to the Justice Committee Inquiry into the 2017 General Election and 2016 Local Election, (24 April 2019) <internetnz.nz>.

³ NZ Government, "Protection against Foreign Interference" CAM010, (June 2020) <protectivesecurity.govt.nz>.

- (e) **Legislation requiring major online advertising platforms to report election advertisements targeting New Zealanders to the Electoral Commission;**
- (f) **Legislation requiring major online advertising platforms to request that a natural person in New Zealand be registered as a promoter with the Electoral Commission before being able to purchase election advertisements targeting New Zealand during the regulated period;**
- (g) **Consideration of larger financial penalties, including penalties based on a percentage of global revenue for breaches of New Zealand election law.**

We can build trust to reduce misinformation risks

Misinformation is a pressing issue both online and offline

12. Research commissioned by InternetNZ shows that New Zealanders are getting more concerned about extremism and misinformation spreading online.⁴
13. While the spread of misleading information is a long-standing social issue, current impacts of misinformation are shaped by people using the Internet. The Internet enables people to share information quickly, broadly, and with spontaneous coordination, amplifying both good and bad behaviours in ways that have had tangible impacts in New Zealand over the past year.
14. During the 2020 election campaign, Whangarei and Auckland had anti-lockdown protests, some of which breached legal restrictions on gatherings.⁵ Related activity has continued in 2021 with a protest at Parliament.⁶ These protests showed how online misinformation can lead to people doing things offline and in-person. Protest events were advertised on social media, and participants held banners with messages developed and spread online, with a common thread of mistrust in shared institutions.⁷
15. The anti-lockdown protests illustrate how problems from misinformation cut across categories and boundaries, combining online and offline behaviour, global ideas and local action, and a range of different issues and motivations, from concerns about elections, to 5G towers, vaccines, and social issues. Some participants are sincere, others may be deliberately sowing mistrust. Election misinformation may be deeply linked to these broader issues.

⁴

<<https://internetnz.nz/new-zealands-internet-insights/new-zealands-internet-insights-2020/concerns-and-safety/>>

⁵ Caroline Williams, *Stuff*, “Coronavirus: Police ‘disappointed’ but no punishment for 500 protesters breaching lockdown” (29 August 2020) <[stuff.co.nz](https://www.stuff.co.nz)>.

⁶

<<https://www.rnz.co.nz/news/national/434533/billy-te-kahika-spreads-covid-19-misinformation-at-parliament-rally>>

⁷ <[wgtn.ac.nz](https://www.wgtn.ac.nz)>

Addressing misinformation requires working with communities

16. We think that more work needs to be done to understand misinformation. For now, we think the core problem posed by misinformation is a risk of undermining community trust in shared institutions and social participation.
17. We think the government can lead and support work to address this challenge, but cannot solve it alone. People and communities engaging with misinformation may not trust government agencies to tell the truth or respect their perspectives and interests.
18. We think the first step is to do more to understand misinformation online
19. We think any work to address misinformation needs to include a high level of support for participation from a diverse range of organisations and actors who are credible to different communities, and independent from government.

We support Tohatoha's work to address misinformation in NZ

20. Our strategic partner organisation Tohatoha is an independent not-for-profit focused on the social impacts of technology. Tohatoha has started community-based work to address misinformation in New Zealand. This work is in two parts.
21. Tohatoha proposes to deliver a data-based "Internet weather report". This would involve scanning mainstream and fringe social media for data about what is being shared in New Zealand and about New Zealand, and make the data available for independent analysis. This would help build understanding.
22. Tohatoha has already begun delivering community education to reduce the impact of people encountering misinformation online and offline, working with libraries, schools, and community organisations around New Zealand.
23. We are proud to support this work as an initial funder, but to achieve its promise more funding is needed. With the right support, we think the Internet weather report could deliver on our recommendation in the previous inquiry for public monitoring of influence efforts online.

R3 We recommend the committee ask the government for a briefing on support being offered for community-based work to address misinformation in New Zealand.

We want to see a broad media review on longer-term issues

24. Harms from misinformation result from problems in our broader information ecosystem. To participate in democratic elections, and in all areas of life, people need access to good information from sources they can trust.

Conclusion

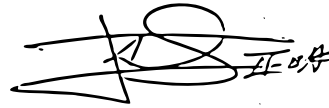
25. We thank the Committee for its consideration of these important issues, and look forward to speaking with you in person.



Kim Connolly-Stone

Policy Director

InternetNZ



James Ting-Edwards

Senior Policy Advisor

InternetNZ

Foreign Interference in our democratic processes

**Justice Committee Inquiry into the 2017
General Election and 2016 Local Election**

24 April 2019

Table of Contents

1.	Introduction.....	2
2.	Campaigns need protection from cyber-threats.....	2
3.	Campaign transparency is needed online.....	4
4.	Monitor influence operations during and between campaigns.....	6
5.	Conclusion	8

1. Introduction

We welcome consideration of interference in elections

- 1.1 Thank you for re-opening submissions to consider foreign interference in New Zealand's elections. InternetNZ's concerns and expertise relate to the Internet, so our submission focuses on online aspects of foreign interference in elections. We do not address the risk that donations to political parties are made by foreign governments or entities.
- 1.2 We address **the ability of foreign powers to hack the private emails of candidates or parties** in part one of our submission.
- 1.3 We divide **the risk that political campaigns based through social media can be made to appear as though they are domestic but are, in fact, created or driven by external entities** into:
 - a) delivering transparency for online election advertising
 - b) monitoring influence campaigns targeting New Zealand's democracy.
- 1.4 This submission follows on from our previous submission to the Committee on the issue of foreign influence campaigns and disinformation.¹ We offer a summary of evidence on disinformation and influence campaigns overseas in **Appendix A**.
- 1.5 We would welcome the opportunity to appear in person to speak to this submission. Please contact our policy team on policy@internetnz.net.nz to arrange our oral submission.

2. Campaigns need protection from cyber-threats

- 2.1 Risks of emails being hacked are one example of a cyber-threat to political campaigns in New Zealand. Candidates and political parties face a variety of threats online, which require both broad and targeted responses.
- 2.2 Addressing targeted attacks requires tailored advice, which this submission cannot provide. If you have concerns about your own cybersecurity you should seek out the advice of a cybersecurity professional and your first port of call should be Parliament's information security team.

¹ We spoke to the Committee on these issues on November 8 2018, see our blog post at <https://internetnz.nz/blog/talking-parliament-about-disinformation> (9 November 2018).

Campaigns are a confirmed target for cyber-threats

- 2.3 Canada's Communications Security Establishment (CSE), the equivalent of New Zealand's GCSB, reports on a variety of confirmed hacking activities targeting political campaigns.² These activities aim to:
- a) steal sensitive campaign documents
 - b) steal a party's voter information (eg for targeting disinformation)
 - c) release unauthorised information (eg to online or local media)
 - d) impede use of the campaign's devices and networks.
- 2.4 These targeted actions against campaigns are much broader than attempts to access email.

All candidates need support to be safe online

- 2.5 Cyber-threats are varied, but there are some basic steps that offer a starting point to be safer online. CERT NZ are the experts on protecting New Zealanders from cyber-threats. Their list of ten "Critical Controls" offer the key steps to protect against the most common cybersecurity problems CERT NZ's staff see.³
- 2.6 Experience in the United States has prompted the development of a *Cybersecurity Campaign Playbook*, designed by a non-partisan group of campaign and cybersecurity professionals.⁴

We recommend work to create a trusted, credible NZ equivalent of the Belfer Center's *Cybersecurity Campaign Playbook* by 2020.

We recommend that candidates and campaigns seek help with basic steps to promote their safety online, starting with CERTNZ

Campaigns need an expert advisor on cyber-threats

- 2.7 Some online threats can be addressed by improving on basic security practices. However, political campaigns need support to address targeted attacks. We think CERT NZ is the natural agency to take up that role, but this will require addressing two main challenges. CERTNZ is now hosted within a central government department (MBIE), and may need greater independence to help with campaigns. CERTNZ will also need extra resources to support for specialist advice to political campaigns.

We recommend that the Committee consider which organisation(s) would be best placed to work with political parties and candidates, to support their cybersecurity in local and general elections.

We recommend Crown funding for work to help campaigns address cyberthreats.

² Communications Security Establishment of Canada, "2019 Update: Cyber threats to Canada's Democratic Process" <<https://cyber.gc.ca/en/>> ("Cyber threats: 2019") p 20.

³ CERT NZ, "Critical Controls 2019" <<https://www.cert.govt.nz/it-specialists/critical-controls/10-critical-controls/>>

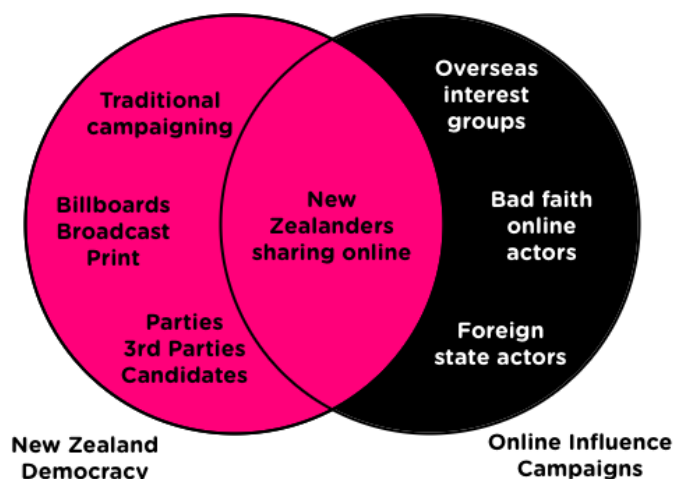
⁴ Belfer Center, Cybersecurity campaign playbook here: <https://www.belfercenter.org/publication/cybersecurity-campaign-playbook>

3. Campaign transparency is needed online

Transparency: who says, who pays, who shares?

- 3.1 Our election rules should allow New Zealanders to engage in good faith online and offline, but should protect against outside influences which would undermine democratic trust and transparency using online tools.

Figure One: Campaign activities and New Zealand's democracy



Online campaigns offer new threats to transparency

- 3.2 Current election laws recognise the importance of transparent election campaigns. However, rules designed for print and broadcast media do not work well for modern online election campaigns. Online campaigns are different, putting at risk the idea that New Zealanders can see who is seeking office, who is funding campaigns, and how campaigns are working to influence opinions and votes (see Table One below).

Table One: Online campaigns are different

Cost	Online advertising can allow broader reach at lower cost than print or broadcast media.
Anonymity	Anonymous actors can target New Zealanders. Overseas actors can pose as New Zealanders engaging in good faith.
Overseas media	Campaigns can be coordinated from overseas, and delivered to New Zealanders through overseas platforms.
Targeting	Targeted advertising or social sharing allows messages to be shared to particular audiences, without being visible to local campaigns, journalists, or other New Zealanders.
Timing	Online messages and advertising can be shared instantly, and can be linked to news stories and events in real-time.
Automation	Computer-driven "bot" accounts can amplify messages or disrupt online conversations between New Zealanders.

Social sharing	Overseas actors can promote social sharing of their messages to influence New Zealanders.
Messaging	Targeting allows extreme messages to be shared without broader visibility or accountability.

Deliver transparency for online election advertising

- 3.3 To protect trust in our democratic processes, we need to extend and update election laws to protect transparent election campaigns online, so voters know who is involved in funding, creating, and sharing messages. Canada's new *Elections Modernization Act* addresses online risks, and offers one useful model for protecting online campaign transparency.⁵

Resource the Electoral Commission with rules and tools

- 3.4 The Electoral Commission regulates elections, with objectives that include maintaining confidence in the administration of the electoral system.⁶ Part of its role is to administer election advertising rules. We think there is a clear case to consider how election advertising rules should be updated to apply effectively online.

We recommend resourcing the Electoral Commission to review and implement requirements for transparent online election advertising

We recommend considering online tools to allow easy compliance, monitoring, and public reporting of election advertising as open data through the Electoral Commission

- 3.5 The window after an election and before a coalition Government has been agreed is a key period for our democratic processes under MMP. We remain concerned that this could be targeted by campaigns to influence the shape or policy commitments of a coalition Government.

We recommend that regulation of online campaigns is extended to include the post-election, pre-government formation time period.

Review spending limits for online election advertisements

- 3.6 Current rules allow anonymous, unregistered parties to spend up to \$13,000 on campaign advertising. That amount may be reasonable for offline campaigns, but does not make sense for online advertising.

We recommend consideration of lower thresholds to register online election campaigns based on their potential reach and impact

Require cooperation of online advertising platforms

- 3.7 The largest platforms for online advertising around the world and in New Zealand are Google and Facebook. Both offer tools to monitor and report on election advertising. Google includes political advertising as part of its Transparency Report, but this feature is currently only available for India and

⁵ Canadian Government, <<https://www.canada.ca/en/democratic-institutions/news/2018/12/government-of-canada-passes-elections-modernization-act.html>>

⁶ Electoral Act 1993, s 4C(c)

the United States of America.⁷ Facebook offers a tool for viewing political issue advertising targeting a country by topic and by total spending.⁸

We recommend requiring online platforms to report election advertisements targeting New Zealanders

We recommend scaling obligations of online platforms based on their global resources and activity levels in New Zealand

Ban foreign election advertising during election campaigns

- 3.8 Current election laws in New Zealand require a named promoter who is accountable for candidate, party, or third-party campaigns. We think the same principle should apply to online advertising, requiring a natural person in New Zealand to register and be accountable for election advertising during campaigns.

We recommend that online election advertisements require a natural person in New Zealand to register as a promoter with the Electoral Commission, before advertisements can be placed through platforms

Update and increase penalties for serious breaches

- 3.9 Current financial penalties in the Electoral Act are limited to \$40,000, or \$100,000 for very serious breaches. These amounts are not enough to motivate difficult compliance steps from large online platforms, which can have revenues in the hundreds of billions per year.
- 3.10 We recognise that current large online platforms do make some efforts to support election transparency. However, New Zealand should not take this for granted.

We recommend consideration of larger financial penalties, including penalties based on a percentage of global revenue, for breaches of New Zealand election law

4. Monitor influence operations during and between campaigns

Is there foreign election interference? How can we tell?

- 4.1 Informal online sharing allows overseas actors to influence democratic processes, in ways that are not readily addressed through advertising laws. We think it is vital to monitor influence activities targeting New Zealand, through credible, well-resourced, and independent agencies.

Deliver ongoing monitoring of outside influences

- 4.2 As a fundamental step to protect trust in our democracy, New Zealand needs effective monitoring and reporting of outside influences targeting our democratic system. To be effective, this monitoring and reporting must be credible, independent, and able to adapt quickly as outside threats change.
- 4.3 Election advertising is only one method by which outside actors may try to influence our democracy. The most dangerous influence campaigns are those

⁷ Google, Google transparency Report <<https://transparencyreport.google.com/political-ads/home>>

⁸ Facebook, Facebook Ad Library, <https://www.facebook.com/ads/library/?active_status=all&ad_type=political_and_issue_ads>

which mimic legitimate democratic engagement, and which seek to imitate and provoke engagement by New Zealanders, particularly online.

- 4.4 As set out below, we think it is important to have independent monitoring of our democracy on different time scales:

- a) **Detection within the election period**, allowing quick responses to influence campaigns as they emerge
- b) **Reflection over time**, with continuous monitoring by a trusted and independent agency to report on influences in our democracy

Detecting influence operations: an election “war room”

- 4.5 To respond to emerging influence operations, immediate information is needed on messages targeting New Zealand’s political system, through content, targeted advertising, or patterns of online sharing. In the busy election period, journalistic or political responses may not be sufficient.
- 4.6 We think New Zealand needs a dedicated agency to monitor, report on, and coordinate responses to influence operations during the election period. Online platforms are a logical partner, because they have access to information who starts, shares and sees campaign messages. For example, Facebook has operated an election “war room” to address misinformation in overseas election campaigns.⁹ We think a domestic agency is needed to coordinate with online platforms, to ensure reporting facilities meet New Zealand’s needs, and to monitor and report in a way that reflects New Zealand’s norms and culture.
- 4.7 This function overlaps to some extent with the Electoral Commission’s monitoring of election advertising in the election period, with NetSafe’s role as Approved Agency responding to harmful communications online, and with CERTNZ’s role monitoring and responding to cyberthreats.

We recommend resourcing an independent agency to monitor, report on, and coordinate responses to influence operations during the election period.

We recommend consulting with the Electoral Commission, NetSafe, and CERTNZ on the design and home for this function.

Reflecting on influences: an Internet observatory

- 4.8 To address risks to democratic trust, New Zealand needs routine monitoring and reporting of political campaigns targeting New Zealanders.
- 4.9 To block external efforts to sow division, monitoring should consider the authenticity, sharing, reach and targeting of messages, in the same way that traditional rules have considered funding and broadcast advertising activity. This requires ongoing, credible work outside our Electoral Commission, which must retain a focus on the election process. Options include an office of Parliament, a component of Parliamentary Services or a dedicated research centre at a New Zealand University.

We recommend that the Committee calls for an independent Internet Observatory to monitor foreign influence campaigns.

⁹ ‘Inside Facebook’s Election War Room - The Verge’
<<https://www.theverge.com/2018/10/18/17991924/facebook-election-war-room-misinformation-fake-news-whatsapp>>.

5. Conclusion

- 5.1 Thank you for reading our submission. We would welcome the opportunity to present to the Committee in person.

Yours sincerely,

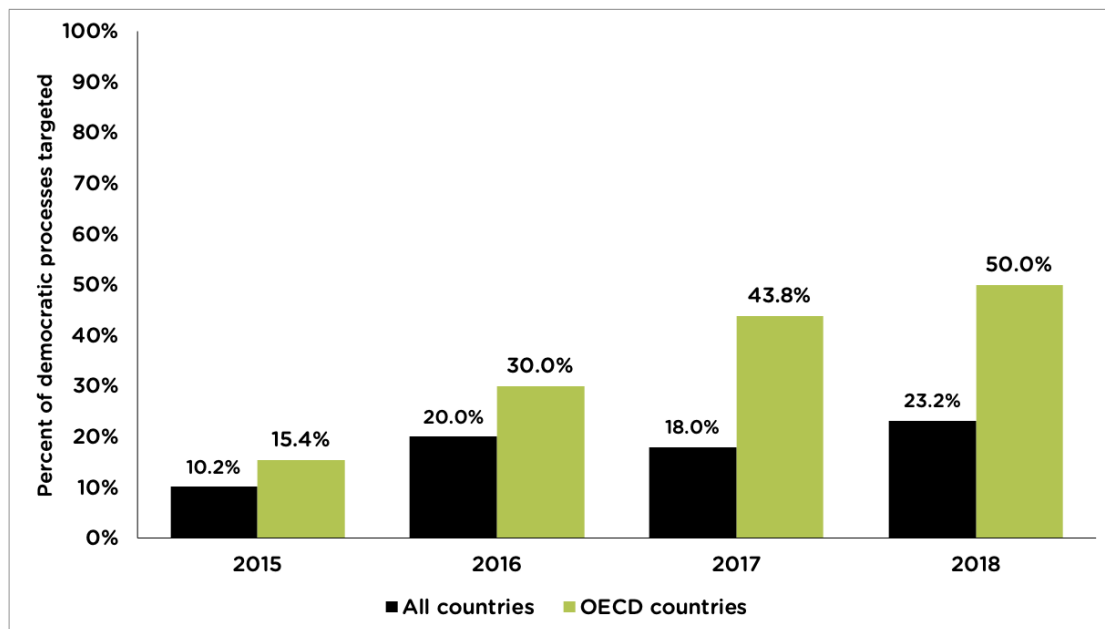
Ben Creet
Policy Manager

Appendix 1: Disinformation and campaigns targeting elections

Elections are global targets for overseas influence

1. Research shows that overseas actors are targeting democratic elections around the world. The Oxford Internet Institute records 48 influence campaigns affecting elections between 2010 and 2018.¹⁰ Canada's Communications Security Establishment (CSE), the equivalent of New Zealand's GCSB, regularly reports on threats to democracy. The 2019 CSE report notes:
 - a. half of national elections in OECD countries during 2018 were targets for cyber threat activity (a threefold increase since 2015)¹¹
 - b. of online threats targeting democratic processes since 2010, 88% were strategic efforts to influence outcomes¹²
 - c. coordinated online campaigns targeting voter behaviour are the most common online threat to democratic processes.¹³
2. Coordinated efforts to influence overseas elections are increasingly common, and are increasingly targeting OECD countries like New Zealand.

Figure Two: Democratic processes are increasingly targeted by cyber-threats¹⁴



¹⁰ Oxford Internet Institute: *Challenging Truth and Trust: A Global Inventory of Organized Social Media Manipulation* <https://comprop.oii.ox.ac.uk/research/cybertroops2018/>

¹¹ Canadian Communications Security Establishment, *2019 Update: Cyber threats to Canada's Democratic Process* ("CSE: Cyber threats 2019") <https://cyber.gc.ca/sites/default/files/publications/tdp-2019-report_e.pdf>

¹² CSE: Cyber threats (2019).

¹³ CSE: Cyber threats (2019).

¹⁴ Data and figure adapted from Figure 5 in CSE: Cyber threats 2019, p 16.

Overseas actors targeting elections have strategic goals

3. Canada's Communications Security Establishment (CSE) summarises the immediate, medium and long term goals of foreign powers who interfere in nations' the democratic processes (see Figure Three below).

Figure Three: Foreign power motivations for interference in democratic processes¹⁵



Russia's Internet Research Agency

Internet Research Agency (IRA) is a Russian company which, as documented by Oxford University researchers, "launched an extended attack on the United States by using computational propaganda to misinform and polarize US voters" from at least 2013 to 2018.¹⁶

Through social media, the IRA created fake online identities, and targeted messages to different political groups to drive intense social conflicts. During the US election in 2016, the IRA encouraged activity by local activist groups,

¹⁵ Data and figure adapted from Figure 2 in CSE: Cyber threats 2019, p 11.

¹⁶ Cindy Ma, 'The IRA and Political Polarization in the United States', The Computational Propaganda Project <<https://comprop.oii.ox.ac.uk/research/ira-political-polarization/>>.

offering payment to people who spread online content or organised real-world rallies.¹⁷

New Zealand is a likely target for influence campaigns

4. A recent survey shows New Zealanders have high levels of confidence in its democracy.¹⁸ New Zealand plays a visible role in international institutions and trade agreements. These traits are positive for a democratic society but could make New Zealand a target for foreign interference. New Zealand holds several of the vulnerability factors that have been shown to make a society vulnerable to disinformation campaigns:¹⁹

Figure Four: Vulnerability factors for disinformation campaigns

1. Diverse populations	4. External divisions
2. The presence of minorities	5. A vulnerable media ecosystem
3. Internal divisions	6. Contested institutions.

¹⁷ Scott Shane and Sheera Frenkel, 'Russian 2016 Influence Operation Targeted African-Americans on Social Media', The New York Times (online at 18 December 2018) <<https://www.nytimes.com/2018/12/17/us/politics/russia-2016-influence-campaign.html>>.

¹⁸ Institute for Governance and Policy Studies, School of Government, VUW, *Public Trust Survey* (June 2018) <https://www.victoria.ac.nz/_data/assets/pdf_file/0007/1616380/IGPS-Trust-Presentation-June2018.pdf#download%20the%20Public%20Trust%20PDF>

¹⁹ French Government, "Information Manipulation" https://www.diplomatie.gouv.fr/IMG/pdf/information_manipulation_rvb_cle838736.pdf