SECURING ELECTIONS AND BEYOND

LESSONS FOR SINGAPORE FROM CANADA'S 2019 FEDERAL ELECTION

Policy Report

March 2020

Dymples Leong

RSIS
S. RAJARATNAM
SCHOOL OF
INTERNATIONAL
STUDIES
Nanyang Technological University, Singapore

NANYANG
TECHNOLOGICAL
UNIVERSITY
SINGAPORE

Policy Report

SECURING ELECTIONS AND BEYOND

LESSONS FOR SINGAPORE FROM CANADA'S 2019 FEDERAL ELECTION

Dymples Leong

March 2020

Table of Contents

Executive Summary

Democratic processes like elections are a growing target for foreign interference through cyber means. The 2019 Canadian Federal Election is one recent case study that has useful lessons for Singapore.

This paper analyses the strategies deployed by foreign interference campaigns (e.g., influencing voters, cyberattacks on electoral and voting systems), as well as the preventive and mitigating measures undertaken by the Canadian government during the 2019 Canadian Federal Election. We apply the lessons learnt from this case study to derive implications for Singapore. These include the threats from the micro-targeting of divisive social media messages to undermine social cohesion, disinformation campaigns (hostile information campaigns) targeting elections, and subversion by influential individuals.

The paper concludes with recommendations: (i) Singapore should consider studying and (if applicable) implementing some of the preventive and mitigating measures taken by Canada – heavier regulation of social media platforms, (ii) forming a protocol for critical election incidents, (iii) establishing a task force on election threats, (iv) providing cybersecurity assistance and advice to major political parties, and (v) enhancing citizen awareness.

New legislation may be needed to restrict the activities of foreign actors in Singapore politics, just as the Protection from Online Falsehoods and Manipulation Act or POFMA helps to deal with disinformation found on online platforms. Public agencies should share a clear, succinct and transparent definition of foreign interference. Policy makers should explain new laws (if any) and policy decisions in a concise and engaging way, tailored to different audiences. Digital literacy campaigns should be supported as they build public resilience against foreign interference from hostile information campaigns. These measures proposed can provide a more holistic awareness of the interlinked nature of cyber threats and foreign interference.

Introduction

The alleged foreign interference in the 2016 Presidential election in the United States has raised concerns in many states over covert influence campaigns which could undermine the national sovereignty and the integrity of electoral institutions.

Foreign influence – the routine diplomatic influence commonly practised by countries – becomes foreign interference when the influence exerted is conducted in a non-transparent manner.[1] Foreign interference activities seek to advance the interests of foreign governments by influencing the political or governmental processes of a target country beyond acceptable standards (such as diplomacy).The Australian government has for example defined foreign interference as covert, deceptive and coercive activities to affect foreign and domestic policies of a targeted country.[2]

Canada had previously experienced cyber threats to its federal elections – such as the "robocalls" scandal in the 2011 federal elections; and the cyberattacks during the 2015 federal elections. The 2019 Canadian Federal election saw a fresh set of challenges.

In 2017, the Canadian Communications Security Establishment (CSE) published a report on the Cyber Threats to Canada's Democratic Process.[3] The CSE defined "cyber threats" as "threats against Canada are individuals or groups that use cyber capabilities against Canadian computers, networks, and other information technology, or the information they contain."[4] More specifically, the CSE categorised **"foreign cyber interference"** occurring when "foreign threat actors use cyber tools to covertly manipulate online information in order to influence voters' opinions and behaviours". Foreign cyber interference targeting voters has been classified as the most common type of cyber threat activity worldwide. Foreign threat actors manipulate online information, often using cyber tools, in order to influence voters' opinions and behaviours.

[1] Australian Government, Attorney-General's Department, "Foreign Influence Transparency Scheme – What is the difference between 'foreign Influence' and 'foreign Interference'?", February 2019, https://www.ag.gov.au/Integrity/foreign-influence-transparency-scheme/Documents/fact-sheets/influence-versus-interference.pdf

[2] Australian Government, Federal Register of Legislation, "Foreign Influence Transparency Scheme Rules 2018", https://www.legislation.gov.au/Details/F2019C00352

[3] "Cyber Threats to Canada's Democratic Process", Canadian Centre for Cybersecurity, Communications Security Establishment, 2017, https://cyber.gc.ca/en/guidance/cyber-threats-canadas-democratic-process/table

[4] Ibid.

In 2018, the Canadian Centre for Cybersecurity (CSC) was launched, assisting the CSE in securing resilience and intelligence capabilities, including security operationalisation in ensuring adequate measures to secure the 2019 Canadian election.

An increase in foreign cyber interference[5] has been observed since the 2017 CSE Cyber Threat report. The National Security and Intelligence Committee of Parliamentarians (NSICOP) released a 2019 update to the report, addressing the potential for foreign influence in Canada – identifying Russia and China in particular.[6] This reflects the importance of targeted responses to ever-evolving cyber threats which could potentially disrupt elections and demonstrates the severity of the threat.

On account of the variegated and interlinked nature of cyber threats, this report will situate these threats against the wider canvas of foreign interference. It is only through a holistic examination that a realistic threat picture can be arrived at.

[5] Ibid.

[6] "2019 Update: Cyber Threats to Canada's Democratic Process", Canadian Centre for Cybersecurity Communications Security Establishment, 2019, https://cyber.gc.ca/en/guidance/2019-update-cyber-threats-canadas-democratic-process

Cyber threat Activities in Previous Federal Elections of Canada

2011 Canadian Federal Elections: Robocalls Scandal

The 2011 Federal Elections was marked by a high volume of "robocalls" allegedly made to dissuade and suppress voter turnout on election day. These automated phone calls were made to voters across various electoral districts in Canada, disseminating misinformation regarding voting centres and processes, allegedly to confuse and dissuade voter turnout amongst non-Conservative voters. A former Conservative party staffer was charged with having wilfully prevented electors from voting in the elections.[7] It was later concluded that there was insufficient evidence to conclude that political parties were directly involved.[8]

Following investigations, Elections Canada upgraded their robocalls detection capabilities and provided credible sources of information on voting procedures to the public.

2015 Canadian Federal Elections: Cyber threat by Hacktivists

The 2015 Federal Elections saw targeted cyber threat activity by hacktivists. An attempt was made to leak high-level federal documents to influence the Federal Elections. Investigations revealed it was highly probable the hacktivist group Anonymous was responsible for the attempt.[9]

[7] "Michael Sona guilty in robocalls trial – but 'did not likely act alone", *CBC News*, 14 August 2014, https://www.cbc.ca/news/politics/michael-sona-guilty-in-robocalls-trial-but-did-not-likely-act-alone-1.2735676

[8] Tonda Maccharles, "Robocalls: Widespread but thinly scattered vote suppression didn't affect election, judge rules", *The Star*, 23 May 2019, https://www.thestar.com/news/canada/2013/05/23/robocalls_widespread_but_thinly_scattered_vote_suppression_didnt_affect_election_judge_rules.html

[9] Adrian Humphreys, "Anonymous leaks another high-level federal document as part of vendetta against government", *The National Post*, 26 September 2015, https://nationalpost.com/news/canada/anonymous-leaks-another-high-level-federal-document-as-part-of-vendetta-against-government#

Global Trends and Threats to Canada

Analysis of the CSE's 2019 update by the author of this report provided insights into how the cyber threat landscape has evolved since CSE's first report in 2017. These insights were used to elaborate on the implications for Singapore and provide recommendations for securing elections.

Cyber interference against democratic processes is increasing worldwide

The number of elections targeted by cyber threat activity has tripled since 2015. In 2018, nearly half of all OECD member countries which held national elections saw some form of cyber threat activity. Nation states using cyber capabilities to influence the democratic processes of adversaries have 3 main goals: Immediate goals include affecting popularity of candidates, questioning the legitimacy of election process and promoting a desired election outcome; mid-term goals include polarising the political discourse and weakening confidence in leaders; long-term goals include promoting foreign economic, ideological and military interests, and reducing confidence in democracy.

Cyber interference against democratic processes increasingly targets voters

As of 2018, the bulk of cyber threat activity was comprised of targeting voters to influence opinions and behaviours.[10] Voters are a vulnerable avenue for manipulation – seen as effective and cheaper to influence as compared to interference efforts targeting political parties or candidates. Three likely factors contributing to the increase in voter targeting are: (i) voters' reliance on the internet and social media as key sources of information; (ii) false information which can be hard to differentiate from credible information, and (iii) the perception by foreign threat actors that targeting voters is low in cost and risk.[11]

[10] "2019 Update: Cyber Threats to Canada's Democratic Process", *Canadian Centre for Cybersecurity Communications Security Establishment*, 2019, https://cyber.gc.ca/en/guidance/2019-update-cyber-threats-canadas-democratic-process

[11] Ibid.

Messaging applications with end-to-end encryption create further opportunities to proliferate misleading information. Misinformation can be used by third-party groups to sow discord and confusion amongst voters. These closed channels are often invisible to fact checkers and authorities. This was seen in the 2018 Brazilian elections, where misinformation regarding electoral processes and political candidates flourished on WhatsApp.[12]

The Canadian Security Intelligence Service (CSIS) also warned of direct attempts being made by foreign actors to disrupt the 2019 Federal election and the electoral process, particularly targeting diaspora Canadian communities.[13]

Voter targeting can be a long term process. In June and July 2019, Canadians reported receiving automated text messages from a third-party seeking their views on scrapping a carbon tax law. The text messages were allegedly used to identify voters who were opposed to the carbon tax, without obtaining permission from the individuals targeted. This information could be used later to target voters with misinformation about candidates' policies on this subject. The skirting of campaign restrictions by Canadian political parties and affiliated firms by using new technologies have made it harder to enforce political campaigning restrictions.

Cyber interference persists against political parties, candidates and staff

Political parties, candidates, and their staff have continued to be targeted worldwide by cyber threat activity, though to a lesser extent than voters.

For instance, during the 2017 French Presidential elections, the French political party En Marche! was the victim of a major cyber-attack – a cache of internal data documents was stolen, including confidential data such as personal emails, financial documents and photographs. News of the leaks were shared heavily on social media (#macronleaks), while bots and influencers amplified its reach. Investigations revealed that certain documents were doctored allegedly by an American neo-Nazi hacker before the data cache was publicly released (though a portion of documents were deemed authentic).[14] The cyber-attack was attributed to Russian-

[12] Daivd Nemer, "The three types of WhatsApp users getting Brazil's Jair Bolsonaro elected", *The Guardian*, 25 October 2018, https://www.theguardian.com/world/2018/oct/25/brazil-president-jair-bolsonaro-whatsapp-fake-news

[13] Alex Boutilier, Craig Silverman and Jane Lytvynenko, "Canadians are being targeted by foreign influence campaigns, CSIS says", *The Star*, 2 July 2019, https://www.thestar.com/politics/federal/2019/07/02/canadas-voters-being-targeted-by-foreign-influence-campaigns-spy-agency-says.html

[14] Jean-Baptiste Jeangène Vilmer, "The 'MacronLeaks' Operation: A Post-Mortem", *The Atlantic Council,* 20 June 2019, https://www.atlanticcouncil.org/images/publications/The_Macron_Leaks_Operation-A_Post-Mortem.pdf

linked cyber hacking groups, although the Russian government has categorically denied interfering in foreign elections. Ultimately, the leaks had minimal impact on the eventual election result: Emmanuel Macron was successfully elected as the President of France. “Macron Leaks” was unsuccessful due to various factors, including a failure of perpetrators to comprehensively understand the French political environment, language, media environment and the French people. The perpetrators attempted to spread rumours in English, without understanding that the French-speaking target audience would not engage with English language content[15] – thereby failing to engage its target audience.[16]

Cyber interference targets election processes

Cyber threat actors can attempt to disrupt election processes by affecting voter eligibility, upsetting ballot casting on election day, hacking of voter databases or defacing election websites. The attackers generally do so to cast doubt about the validity of an election result. The possibility of cyber threat attacks of federal election processes in Canada was predicted to be minimal, especially because of the use of hand-counted paper ballots.[17]

[15] Ibid

[16] Luke Harding and Alec Luhn, “Putin says Russian role in election hacking ‘theoretically possible’”, *The Guardian*, 1 June 2017, https://www.theguardian.com/world/2017/jun/01/putin-says-russian-role-in-election-hacking-theoretically-possible

[17] “Cyber Threats to Canada’s Democratic Process”, *Canadian Centre for Cybersecurity, Communications Security Establishment*, 2017, https://cyber.gc.ca/en/guidance/cyber-threats-canadas-democratic-process/table

Preventive and Mitigating Measures

Modernising the Electoral Process: The Canadian Elections Modernisation Act

Measures have been implemented to reduce the spread of disinformation about the Canadian electoral process. For instance, the composition of the Canadian House of Commons Special Committee on Electoral Reform was made public online, with brief explainers on the objectives and scope of the Special Committee.[18]

The Canadian Elections Modernisation Act (Bill C-76) was introduced to safeguard Canadians' trust in democratic processes and increase public participation in democratic activities. The Act ensures resilience against misinformation and foreign cyber interference during an election period, and prohibits foreign spending to influence elections.[19]

Heavier regulation of social media platforms

The Canadian government has heavily advocated for greater regulation of social media platforms, leading to greater communication with them, and the platforms have so far been responsive to address government concerns. The CSC has also advocated for increased algorithmic transparency[20] by social media companies. The Canadian Minister of Democratic Institutions, Katrina Gould, has released the Canada Declaration on Electoral Integrity Online, which guides social and digital platforms to ensure integrity, transparency and authenticity ahead of the 2019 federal election.[21]

[18] The Honourable Larry Bagnell, "The Creation of an Independent Commissioner Responsible for Leaders' Debates", March 2018, https://www.ourcommons.ca/Content/Committee/421/PROC/Reports/RP9703561/procrp55/procrp55-e.pdf

[19] "Government of Canada passes Elections Modernization Act", 14 December 2018, https://www.canada.ca/en/democratic-institutions/news/2018/12/government-of-canada-passes-elections-modernization-act.html

[20] "Government of Canada passes Elections Modernization Act", 14 December 2018, https://www.canada.ca/en/democratic-institutions/news/2018/12/government-of-canada-passes-elections-modernization-act.html

[21] "Government of Canada passes Elections Modernization Act", 14 December 2018, https://www.canada.ca/en/democratic-institutions/news/2018/12/government-of-canada-passes-elections-modernization-act.html

The Elections Modernisation Act requires social media companies to maintain a database of online political advertisements and to ensure general public access to the advertisements for two years.[22] Companies have responded differently to the new bill. Google decided to ban political advertising from its platforms ahead of the 2019 Canadian Federal election as the new transparency rules "would be too challenging to comply with."[23] Twitter similarly banned political advertising on its platform until the election campaigning officially began.[24] On the other hand, Facebook enabled public access to its advertising library ahead of the Federal election. Advertisers must also disclose and verify identities when purchasing political ads on the platform.[25]

Formation of Critical Election Incident Public Protocol

To enhance citizen preparedness, the Critical Election Incident Public Protocol (CEIPP) – comprising 5 non-partisan senior public servants – was formed in January 2019.[26] In the event of foreign interference in the electoral process during the writ period, the CEIPP will determine if the Canadian elections department should go public with information. A public announcement will be made by the CEIPP only when the threshold for doing so is met. The considerations for meeting the threshold are: (i) the degree in which the incident undermines the ability of Canadians to have a free and fair election; (ii) the potential of the incident to undermine the credibility of the election; and (iii) the degree of confidence towards the intelligence assessment of foreign interference.

[22] Theresa Wright, "Facebook announces changes to political advertising to meet new federal rules", *Canada's National Observer*, 18 March 2019, https://www.nationalobserver.com/2019/03/18/news/facebook-announces-changes-political-advertising-meet-new-federal-rules

[23] Tom Cardoso, "Google to ban political ads ahead of federal election, citing new transparency rules", *The Globe and Mail*, 4 March 2019, https://www.theglobeandmail.com/politics/article-google-to-ban-political-ads-ahead-of-federal-election-citing-new/

[24] Elizabeth Thompson, "Twitter banning political ads in Canada until election campaign", *CBC News*, 26 June 2019, https://www.cbc.ca/news/politics/twitter-online-advertising-election-1.5190465

[25] Katie Paul, "Facebook expands rules on political ads to Canada and Ukraine", *Reuters*, 25 June 2019, https://www.reuters.com/article/us-facebook-advertising-politics/facebook-expands-rules-on-political-ads-to-canada-and-ukraine-idUSKCN1TQ1YS

[26] "Cabinet Directive on the Critical Election Incident Public Protocol", *Government of Canada*, https://www.canada.ca/en/democratic-institutions/services/protecting-democracy/critical-election-incident-public-protocol/cabinet.html

The CEIPP conducted table-top exercises of scenarios in which the CEIPP is required to act. It also discussed the various challenges the country could encounter during the election, including advanced disinformation techniques and cyber threats.[27]

Establishment of Security and Intelligence Threats to Elections Task Force

The Security and Intelligence Threats to Elections (SITE) Task Force was established in 2019 by the Canadian Federal government, to prevent "covert, clandestine and criminal activities" which could influence or interfere with free and fair elections.[28] The composition of the SITE Task Force includes multiple agencies comprised of the Royal Canadian Mounted Police), the Canadian Security Intelligence Service (CSIS), the CSE and Global Affairs Canada. The SITE Task Force assisted the government in assessing and responding to foreign threats during the 2019 federal election. The SITE Task Force closely consults with the CEIPP on potential threats to the integrity of the election.

Cybersecurity Assistance and Advice to Political Parties

The CSE provides cyber briefings and assistance to all major political parties in Canada. Best practices and cybersecurity architecture reviews can be obtained through the Cybersecurity Guide for Campaign Teams. Selected key individuals from various political parties with valid and appropriate security clearances are briefed further on classified information concerning cyber threats. The CSE has conducted monthly teleconferences for federal political parties on cybersecurity and the threat environment.[29] The CSE has stated that no specific threats have been identified at present.[30]

[28] "Combatting Foreign Interference", Government of Canada, https://www.canada.ca/en/democratic-institutions/news/2019/01/combatting-foreign-interference.html

[29] Alex Boutilier, Craig Silverman and Jane Lytvynenko, "Canadians are being targeted by foreign influence campaigns, CSIS says", *The Star*, 2 July 2019, https://www.thestar.com/politics/federal/2019/07/02/canadas-voters-being-targeted-by-foreign-influence-campaigns-spy-agency-says.html

[30] Bill Curry and Janice Dickson, "Federal political parties receiving classified security briefings on potential campaign threats", *The Globe and Mail*, 3 July 2019, https://www.theglobeandmail.com/politics/article-federal-political-parties-receiving-classified-security-briefings-on/

Enhancing Citizen Preparedness

Public education is an important facet in safeguarding the 2019 Federal elections. The CSE cyber awareness “Get Cyber Safe” campaign published relevant advice on cybersecurity and social media tips to the public ahead of the 2019 elections. The government also highlighted the role which media and civic literacy plays in educating citizens – with an emphasis on younger Canadians – in combatting disinformation. The Federal government created the Digital Citizen Initiative, which aims to support digital, news and civic literacy initiatives, and to increase public awareness of deceptive online practices which could be weaponised by malicious actors.

Combatting Deep fakes

Developments in emerging technology such as the rise of deep fakes – human image synthetic videos generated by artificial intelligence – has led to concern over the potential deployment in the 2019 Canadian Federal Election. While deep fakes have not be used in previous Canadian elections, it could potentially be used to discredit candidates in the future.[31] Misleading video content can have significant impact: in the United States, a 2019 video of US Senator Nancy Pelosi was doctored (without using deep fake technology) to misconstrue her verbal misspeaking, and was shared widely on social media platforms. With such technology, it is conceivable that campaign videos of politicians could be manipulated to make them appear to say things which they never said.

Preventive measures have been adopted to mitigate the threat of deep fakes in the 2019 Federal election. Such measures include the Leaders Debate Commission’s initiative to provide a minute-by-minute transcription of online videos created and posted by political candidates and party leaders.[32] The Commission has also called for an increase in the accessibility of televised debates to the public. The initiative would also be verified independently with the support of the Canadian media. These improvements would widen the accessibility for audiences and enable additional levels of veracity to minimise opportunities for misinformation and manipulation.

[31] Tim Hwang, “The Future of the Deepfake and what it means for fact checkers”, *Poynter*, 17 December 2018, https://www.poynter.org/fact-checking/2018/the-future-of-the-deepfake-and-what-it-means-for-fact-checkers/

[32] Joan Bryden, “Federal Election 2019 Debates Need To Be More Civil And Educational For Voters, Commission Told”, *The Huffington Post*, 5 March 2019, https://www.huffingtonpost.ca/2019/05/03/election-2019-debates-commission_a_23721185/

The nature of deep fakes may well evolve beyond current limitations and be deployed in future Canadian elections. There are concerns that deep fakes would damage the credibility and reputation of Canadian media agencies as trustworthy sources for news and information. Therefore, the involvement and dependence on the media in Canada to counter misinformation cannot be understated. For instance, the Canadian media often reports on the various techniques of online manipulation, and raises public awareness of global manipulation efforts to the public.

Beyond the Elections

After the election, the Canadian government confirmed that it observed attempts to meddle in the election. Canadian officials from the Privy Council Office reported that the federal government did detect attempted misinformation or disinformation during the election campaign, but not at a level high enough to compromise the election or for the CEIPP to alert the public.

Preliminary analysis from researchers and academics on inauthentic behaviour from Twitter and Facebook observed that bot activity during the election was at a lower level than expected. Low levels of disinformation and influence campaigns were also observed. Some researchers have therefore suggested that the threat of foreign interference for the election was overhyped. It is currently premature to attribute or infer the reasons for the low levels of online activity – misinformation could have been shared by voters in closed channel platforms (e.g., WhatsApp groups), making it hard for researchers to monitor.[33] Disinformation attempts were observed online. For instance, political memes on current Prime Minister Justin Trudeau's blackface scandal were created by third-party groups to amplify emotional sentiment surrounding the issue. Fake political ads were also created - these "cheap fakes" tapped on Trudeau's blackface controversy to include racist defacement of actual political ads.[34] This was shared widely on Twitter, and encouraged domestic entities to feature this in online attack ads.[35]

[33] Roberto Rocha, "Fears of election meddling on social media were overblown, say researchers", *CBC News*, 3 November 2019, https://www.cbc.ca/news/canada/social-media-bots-trolls-canadian-election-2019-1.5343210

[34] Ibid.

[35] Fatima Syed, "Memes, fake news and partisan ads", *National Observer*, 21 October 2019, https://www.nationalobserver.com/2019/10/21/analysis/memes-fake-news-and-partisan-ads

Post-election, the SITE Task Force will continue to work within their respective mandates to detect and counter possible foreign threats to Canada and its democratic institutions. The CEIPP will assess how the election protocol worked in addressing any threats, prepare classified recommendations on whether the protocol should be a permanent part of future elections, and publish an unclassified public version of the report in spring 2020.[36]

[36] Elizabeth Thompson, "'More needs to be done,' Gould says after some online election meddling detected", *CBC News*, 28 October 2019, https://www.cbc.ca/news/politics/election-misinformation-disinformation-interference-1.5336662

Implications for Singapore

Singapore shares many similarities with Canada – including a multi-ethnic, multi-racial and multi-religious society. Hostile state actors are motivated to search for weaknesses and cracks in a target society, to facilitate covert building and projection of influence. The online space enables them to engage in deliberate and covert actions leading to foreign interference.

Cyber threats through social media micro-targeting

There is much concern over micro-targeting of divisive social media messages which may undermine the social cohesion of Singapore. Coordinated inauthentic behaviour, automated accounts (bots) and fake accounts (trolls) could spread divisive content to inflame social and racial tensions, thereby disrupting social cohesion.

During Singapore's Select Committee on Deliberate Online Falsehoods, the use of news articles and social media to influence segments of Singapore's population (e.g., ethnic diaspora) were highlighted. It is "absurdly easy" for people to "conduct covert and subversive campaigns to manipulate opinions and influence elections", where disinformation campaigns, especially targeting elections, become the new normal due to the prevalence of social media platforms.[37] These disinformation campaigns are also known as "hostile information campaigns".

Subversion

There are also concerns over academics who could be willingly or unwillingly used by foreign powers to influence Singapore's position in relation to foreign policy. A recent example in Singapore was the case of Huang Jing, a former academic working in Singapore. Huang Jing abused his position at the Lee Kuan Yew School of Public Policy to advance the agenda of a foreign country, knowingly engaging with foreign intelligence operatives in Singapore to influence and interfere with Singapore's foreign policy and public opinion. He also recruited others to further his agenda. His collaboration was classified as "subversion and foreign interference".[38]

[37] "Online falsehoods law will tackle attempts to 'manipulate opinions, influence elections': PM Lee", *Channel NewsAsia*, 25 April 2019, https://www.channelnewsasia.com/news/singapore/anti-fake-news-law-tackle-attempts-manipulate-elections-pm-lee-11478054

[38] "In full: MHA's statement on revoking PR status of academic Huang Jing and wife", *TODAY* , 4 August 2017, https://www.todayonline.com/singapore/ministry-home-affairs-full-statement-huang-jing

Recommendations

Legislative Measures

Canada is introducing legislation to address cyber interference. The Canadian Digital Charter aims to defend freedom of expression and protect against online threats and disinformation designed to undermine the integrity of elections and democratic institutions.[39] The Charter is designed to target fake news and hate speech, holding social media platforms accountable to their role in allowing disinformation to spread. However, the Charter does not specifically state a definition for "fake news", or provide information on how penalties to social media platforms would operate.

Singapore introduced its own legislation in October 2019, the Protection from Online Falsehoods and Manipulation Bill (POFMA). POFMA aims to guard against disinformation efforts in Singapore, and hold online platforms and tech companies accountable for regulating their platforms, including closed messaging platforms such as WhatsApp and Facebook Groups. Unlike the United States, Singapore does not have a specific legislation which addresses the threat of deep fakes, but POFMA is expected to be continually revised and updated as emerging policy issues and technological developments arise.[40] In the event that online falsehoods pose a threat to the integrity of Singapore elections, the Minister can issue Correction Directions to the online platforms under POFMA, though this must be done carefully because the use of POFMA could become politicised.

Singapore is also set to introduce legislation to tackle the issue of foreign interference in domestic politics and opinion.[41] This may be similar to the Foreign Agents Registration Act (FARA) of the United States, Australia's Foreign Interference Transparency Scheme introduces registration requirements of entities or individuals who undertake activities for foreign principals, not limited to political lobbying, donations and fundraising.[42] Such legislation could increase requirements transparency of the funding (and influence) received by political parties, politicians, and other participants in the political process.

[39] "Canada's Digital Charter: Trust in a digital world", Government of Canada, https://www.ic.gc.ca/eic/site/062.nsf/eng/h_00108.html

[40] Adrian Lim, "Parliament: Fake news law covers closed platforms like chat groups and social media groups, says Edwin Tong", *The Straits Times*, 7 May 2019, https://www.straitstimes.com/politics/parliament-fake-news-law-covers-closed-platforms-like-chat-groups-and-social-media-groups

[41] Adrian Lim, "Singapore needs laws to tackle foreign interference in domestic matters: Shanmugam", *The Straits Times*, 25 September 2019, https://www.straitstimes.com/politics/singapore-needs-laws-to-tackle-foreign-interference-in-domestic-matters-shanmugam

[42] Australian Government, Department of Foreign Affairs, "Foreign Influence Transparency Scheme", https://dfat.gov.au/international-relations/Pages/foreign-influence-transparency-scheme.aspx

Non-Legislative Measures

Singapore could consider some of the steps that Canada has taken to mitigate threats to elections

(1) **Establishment of a task force on security threats to elections.** This could include multiple agencies such as the Singapore Police Force, intelligence agencies, Elections Department, MCI, and MHA.

(2) **Cybersecurity assistance and advice to political parties.** CSA could provide cyber briefings and assistance to all major political parties in Singapore, on best practices for cybersecurity, and brief selected key individuals from various political parties with valid and appropriate security clearances on cyber threats.

(3) **Enhancing citizen preparedness.** Just as Canada has the "Get Cyber Safe" campaign and the Digital Citizen Initiative, Singapore is also deeply interested in enhancing citizen preparedness.

Policymakers should clearly explain the importance of proposed legislation to the public. Concise explainers on policy decisions to safeguard the integrity of elections from foreign interference should be conducted in a manner to engage various demographics across the population over relevant media platforms.

The terms "interference" and "influence" are often conflated by the public and media, resulting in confusion and a blurring of definitions, acceptance and legality of the two terms. It becomes a buzzword similar to "fake news" – a blanket term commonly used to broadly describe a series of issues regarding disinformation, rumours and untruths. A clear, succinct and transparent definition of foreign interference should be devised and then disseminated to the public. For instance, the Foreign Influence Transparency Scheme of Australia, provided a fact-sheet for public dissemination on the difference between foreign influence and foreign interference. The fact-sheet clearly defined the criteria for an activity or event to be classified as foreign interference.[43] A clear definition of foreign interference also assists public awareness of appropriate countermeasures required against potential foreign interference. The messaging for public awareness should also be tailored to various audiences, e.g., simple videos can be utilised to educate the elderly population in Singapore.

[43] Ibid.

One suggestion could involve identifying groups to engage various demographics. For instance, Canada's approach has been to identify non-governmental groups (NGO) who can engage well with various demographics. "Apathy Is Boring", a non-partisan organisation, was actively involved in providing accurate information about the electoral process. Grants by the Canadian government of up to $7 million Canadian dollars were approved for NGO usage. These initiatives help citizens critically assess and become resilient against harmful online disinformation.[44] More than 20 projects are being launched to strengthen critical thinking about disinformation.

A variation of this approach could be adopted by Singapore. Students could be encouraged to develop similar campaigns or initiatives on tackling disinformation / hostile information campaigns. A format similar to "N.E.mation!" – a platform for students to create short animation videos on Total Defence in Singapore – could be used to strengthen awareness of resilience against disinformation by having a competition or initiative dedicated solely to strengthening critical thinking about disinformation and misinformation.[45] Ground-up initiatives such as the youth-led "Sure Anot" campaign for older and less technologically-savvy Singaporeans can also contribute to greater awareness on critical thinking efforts.[46]

The increase in digital literacy efforts by the government and civil organisations can improve the public ability to spot disinformation / hostile information campaigns. A digitally literate and discerning public will be more resilient against hostile information campaigns aimed at dividing and exploiting the multi-racial, ethnic and religious society in Singapore.

[44] "Backgrounder – Helping Citizens Critically Assess and Become Resilient Against Harmful Online Disinformation", Government of Canada, https://www.canada.ca/en/canadian-heritage/news/2019/07/backgrounder--helping-citizens-critically-assess-and-become-resilient-against-harmful-online-disinformation.html

[45] Lim Min Zhang, "Students learn to tackle fake news and online scams in N.E.mation! workshop", *The Straits Times*, 3 September 2018, https://www.straitstimes.com/singapore/students-learn-to-tackle-fake-news-and-online-scams-in-nemation-workshop
https://www.bbc.com/news/world-australia-44624270.

[46] Mandy Lee, "NTU undergraduates create campaign to combat 'fake news' spreading among older S'poreans", *TODAY,* 2 February 2020, https://www.todayonline.com/singapore/ntu-undergraduates-create-campaign-combat-fake-news-among-older-sporeans

Conclusion

Canadian efforts to safeguard and protect its democratic processes emphasises the urgency in which foreign interference should be tackled. It is expected that other countries will respond to this issue with foreign interference legislation or policies to mitigate against interference.

Legislation is important but requires complementary active initiatives, including, but not limited to digital media literacy, education and public awareness efforts. Singapore can also consider implementing the measures that Canada implemented for their elections, such as establishing a task force, and briefing political parties on cybersecurity. Public communication on the importance of safeguarding democratic processes should be highlighted. These measures proposed can provide a more holistic awareness of the interlinked nature of cyber threats and foreign interference.

About the Author

Dymples Leong is a Senior Analyst with Centre of Excellence for National Security (CENS) at the S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University, Singapore. Her research focuses on behavioural insights and policymaking, strategic communications, social media and online radicalisation. Her commentaries have been published in newspapers and journals such as The Straits Times, New Straits Times, Asian Journal of Pacific Affairs and International Policy Digest. Dymples holds a Bachelor of Business majoring in Marketing and Management from the University of Newcastle Australia.

About the Centre of Excellence for National Security

The **Centre of Excellence for National Security (CENS)** is a research unit of the S. Rajaratnam School of International Studies (RSIS) at the Nanyang Technological University, Singapore.

Established on 1 April 2006, CENS raison d'être is to raise the intellectual capital invested in strategising national security. To do so, CENS is devoted to rigorous policy-relevant analysis across a range of national security issues.

CENS is multinational in composition, comprising both Singaporeans and foreign analysts who are specialists in various aspects of national and homeland security affairs. Besides the work undertaken by its full-time analysts, CENS boosts its research capacity and keeps abreast of cutting edge global trends in national security research by maintaining and encouraging a steady stream of Visiting Fellows.

For more information about CENS, please visit www.rsis.edu.sg/cens.

About the S. Rajaratnam School of International Studies

The **S. Rajaratnam School of International Studies (RSIS)** is a think tank and professional graduate school of international affairs at the Nanyang Technological University, Singapore. An autonomous school, RSIS' mission is to be a leading research and graduate teaching institution in strategic and international affairs in the Asia Pacific. With the core functions of research, graduate education and networking, it produces cutting-edge research on Asia Pacific Security, Multilateralism and Regionalism, Conflict Studies, Non-traditional Security, Cybersecurity, Maritime Security and Terrorism Studies.

For more details, please visit www.rsis.edu.sg. Follow us on www.facebook.com/RSIS.NTU or connect with us at www.linkedin.com/school/rsis-ntu.

RSiS S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES
Nanyang Technological University, Singapore

Nanyang Technological University, Singapore
Block S4, Level B3, 50 Nanyang Avenue, Singapore 639798
Tel: +65 6790 6982 | Fax: +65 6794 0617 | www.rsis.edu.sg