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

RSIS COMMENTARY

www.rsis.edu.sg No. 045 – 20 March 2020

Guarding Against Foreign Interference in Elections

By Stephanie Neubronner

SYNOPSIS

Developed electoral processes in mature economies in the West have been compromised by external tampering. Singapore has not had to deal with serious cases of foreign interference in its elections. This could, however, change in the future. What can be done to pre-empt this?

COMMENTARY

THE RELEASE of the Electoral Boundaries Review Report on 13 March 2020 suggests that Singapore's next general election is just around the corner. With various political parties already gearing up for the next election, it is crucial that Singapore does not lose sight of the importance of protecting itself from foreign interference.

Foreign interference is not a new threat jeopardising the security, unity and autonomy of states. Throughout history, nations have attempted to interfere in other states' politics for their own benefit for a multitude of reasons. While the basis of foreign state motivations might not have changed much, the use of technology to amplify and markedly increase the reach and concealment of such interference has raised concerns for governments around the world.

Threat of Foreign Interference

Increasingly, Information and Communications Technologies (ICTs) are being used to target social fault lines and trust in public institutions. With the intention of mobilising people *against* something rather than *for* something, such Hostile Information Campaigns (HICs) are often directed at intangible targets with economic, political and social impact.

Such coordinated attempts are also usually covert and aim to sow confusion, fray civic threads, and intensify existing polarisations.

A proactive approach against the threat of foreign interference in Singapore's domestic politics is thus imperative. This is particularly important as Singapore's openness, interconnectivity, as well as its multiracial and multi-religious composition make it particularly vulnerable.

The 2016 United States presidential election is a recent example of the threat foreign interference poses. The Mueller Report indicated that a major foreign power that has been locked in ideological competition with the US utilised ICTs as part of a larger planned operation to create dissonance within the US political system.

Social media platforms like Twitter and Facebook were targeted, and by the end of the presidential election, the major foreign power had the ability to reach at least 29 million US individuals through their social media accounts.

The major foreign power was also in control of social media accounts that had hundreds of thousands of US participants, including media outlets, high-profile persons and US political figures who reposted or responded to the content it created.

Threat Facing Singapore

Singapore has been the target of cyber attacks and HICs in the past, and it continues to be so today. Two examples stand out, highlighting the ongoing threat Singapore faces:

First, the 2013 Anonymous cyber attack affecting the incumbent's webpage and leak of government employees' personal information; second, the unprecedented attack on SingHealth's national health database in June 2018, where personal information of 1.5 million individuals, including that of Prime Minister Lee Hsien Loong were illegally accessed.

These threats cannot be taken lightly given the increased threat foreign interference in domestic politics poses, especially when paired with the repercussions of deliberate online falsehoods.

In November 2018, an online news article falsely linking Prime Minister Lee to the 1Malaysia Development Berhad (1MDB) scandal was published and circulated online.

The article purported that Malaysia had signed several unfair agreements with Singapore in exchange for Singapore banks' assistance in laundering 1MDB's funds. The article also suggested that Singapore was reluctant to investigate the 1MDB scandal, only reopening its investigations after it was forced to do so.

Not Insignificant

Such forms of misinformation may appear relatively insignificant, but could actually cause serious damage to Singapore's credibility and interests if not corrected.

Additionally, such misinformation could potentially undermine public trust in government institutions, alter social behaviours and cause rifts within Singapore's multiracial society.

Technology's role in creating greater strains on individuals' trust in democracy, institutions, values and social systems cannot be overlooked. Should a culture of distrust and discontent erupt, preserving social cohesion and national security in Singapore will become even more arduous.

Preventing the interference of HICs in Singapore's domestic politics will likewise become exceptionally challenging.

Learning From Others' Experiences

Standing out from the long list of recent episodes of electoral interference overseas is the coordinated attempt to undermine Emmanuel Macron's candidacy in the 2017 French presidential election. The attempt failed to influence French politics as conscious efforts were made to prepare the country for the likelihood that electoral meddling would occur.

Having taken heed of the incidents during the 2016 US presidential election, provisions guaranteeing the integrity of the French electoral process were implemented. This included technical training for all campaign officials, equipping them with the necessary skills to monitor, identify and deal with suspicious activity in candidates' information systems.

The speed with which Macron's team responded to the HIC is a testament to the value of planning for the eventuality of a HIC.

There was also growing public awareness of the impact disinformation and HICs have. This further contributed to the French people and media viewing the leaked documents with suspicion, which helped weaken its influence.

Similarly, Canada has benefited from learning from the US' experience with foreign election meddling. The extent of measures implemented in the run up to its recently concluded election should also be viewed as a forewarning of the pervasiveness and seriousness the threat foreign interference poses.

Implications

Having planned a coordinated response to foreign interference attempts, Canada's reaction enabled it to successfully fend off online disinformation, cyberattacks and other foreign interference during its 2019 federal election.

Several measures were put in place. First, legislation to combat foreign funding and the spread of fake statements aimed at influencing election outcomes. Second, the enhancement of citizen preparedness through the setting up of the Critical Election Incident Public Protocol, which informs citizens of incidents that threaten Canada's ability to have a free and fair election.

Third, improvements in the coordination between Canada's government and security agencies via the establishment of the Security and Intelligence Threats to Elections Task Force; and fourth, requiring social media platforms to increase the transparency, authenticity and integrity of their systems.

As Singapore gears towards its own hustings, what can we learn from these overseas cases?

One, introduce new, more targeted laws enabling investigators to prevent and examine threats; two, update existing legislation to account for new methods of interference particularly in the cyber domain; three, generate more awareness amongst Singaporeans about the country's multiracial makeup and vulnerabilities, and how Singapore's different communities coexist harmoniously.

These are some ways Singapore could adopt in its own strategy against the threat of foreign interference. With other countries already implementing measures to deal with HICs and foreign interference, Singapore should take a proactive approach in safeguarding its national security, social cohesion and sovereignty. Waiting for more serious cases of foreign interference to occur before taking action will only prove to be foolish.

Stephanie Neubronner is a Research Fellow with the National Security Studies Programme (NSSP), a constituent research unit of the S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University (NTU), Singapore.

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