FOREIGN INTERFERENCE IN DOMESTIC POLITICS: A NATIONAL SECURITY PERSPECTIVE

Policy Report

April 2020

Damien D. Cheong
Stephanie Neubronner
Kumar Ramakrishna

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

NANYANG TECHNOLOGICAL UNIVERSITY SINGAPORE

Policy Report

FOREIGN INTERFERENCE IN DOMESTIC POLITICS: A NATIONAL SECURITY PERSPECTIVE

Damien D. Cheong
Stephanie Neubronner
Kumar Ramakrishna
April 2020

Table of Contents

Executive Summary

This report seeks to raise awareness of the complexities, challenges and constraints pertaining to foreign interference in domestic politics in relation to Singapore.

Foreign interference in domestic politics has grown more sophisticated over the years, due in part to the availability and use of Information and Communications Technologies (ICTs). ICTs not only enable new pathways to influence a target state and its people, but also enable adversaries to develop ways to mask their true intentions.

Consequently, it is difficult to tell if deliberate online falsehoods and misinformation targeting a particular state is state-sponsored (i.e., a Hostile Information Campaign (HIC)), or if a foreign actor who interferes in the domestic politics of another state is doing so at the behest of a foreign state. Notwithstanding, global examples over the last five years suggest that foreign interference in domestic politics is growing.

The ultimate aim of foreign interference in domestic politics is to advance the interfering state's national interests at the expense of the targeted state. Political elites, public institutions/agencies, public policies and social fault lines can be potential targets of foreign interference.

Being "pressure points", foreign actors can use such targets to influence the actions and views of political elites, aligning them with their interests and/or the interests of their state clients. The foreign actor can also support oppositional voices and movements, stir up public unrest, and aggressively lobby for radical changes in policies through individuals as well as organisations. A key point to note is that targets can be attacked with sophisticated online, as well as offline methods.

As a potential target, Singapore is vulnerable due to its openness, multiracial/multi-religious composition and global interconnectivity (on and offline). The city-state has learnt lessons from past attempts by foreign actors to interfere in its domestic politics, and therefore, takes this threat very seriously.

There is no way to eliminate the threat of foreign interference in domestic politics, but the risks can be mitigated. Updates to existing legislation pertaining to foreign interference in domestic politics, policies to empower and equip law enforcement with the necessary tools to carry out deep investigations, enhancing the protection of election integrity, and educating/mobilising society to recognise and resist foreign interference, are possible approaches.

Indeed it is said that in statecraft there are no permanent friends, only permanent interests[1]

Introduction

On 9 August 1965, Singapore became an independent state. As an independent state, its survival, progress and destiny became the responsibility of Singaporeans. As a fledgling small state, Singapore continues to have "limited capacity" in shaping "rules, processes, norms, and outcomes", which are often defined by other states.[2] As a result, Singapore can find itself being drawn into contests involving other states.

Singapore has always chosen neutrality as it is in its national interests to do so.[3] Neutrality ensures that Singapore protects its sovereignty and independence.[4] However, this does not stop other states from nudging Singapore into aligning its interests with theirs.[5]

A sensitive and expectedly less discussed method of "nudging" is interfering in Singapore's domestic politics. As this is a high-stakes game of advancing the national interests of another state, countries considered friendly to Singapore may do it as well.[6] One must view this from a clear-eyed, dispassionate and Machiavellian lens.

---

1 See Prime Minister's Office, Singapore. "Message delivered by Ambassador Ashok Mirpuri on behalf of PM Lee Hsien Loong at private memorial service for Mr Lee Kuan Yew." Available from: https://www.pmo.gov.sg/newsroom/message-delivered-ambassador-ashok-mirpuri-behalf-pm-lee-hsien-loong-private-memorial.

2 See Global-is-Asian. "Punching above its Weight: Is Singapore more than a price taker in global governance?" 1 August 2018. Available from: https://lkyspp.nus.edu.sg/gia/article/punching-above-its-weight-is-singapore-more-than-a-price-taker-in-global-governance.

3 See Minister of Foreign Affairs Dr Vivian Balakrishnan's speech on the five core principles of Singapore's foreign policy – "Full speech: Five core principles of Singapore's foreign policy." *The Straits Times*, 17 July 2017. Available from: https://www.straitstimes.com/singapore/five-core-principles-of-singapores-foreign-policy.

4 Wong, Kan Seng. "Continuity and Change in Singapore's Foreign Policy", in *The Little Red Dot: Reflections by Singapore's Diplomats*, Tommy Koh and Chang Li Lin (eds.), 50. Singapore: World Scientific, 2005.

5 A major reason why Singapore joined the Non-aligned Movement during the Cold War. For more details, see Chua, Daniel. *US-Singapore Relations*, 1965-1975, 36. Singapore: National University of Singapore Press, 2017.

6 See Levin, Dov H., "When the Great Power Gets a Vote: The Effects of Great Power Electoral Interventions on Election Results." *International Studies Quarterly*, no. 60 (2), (2016): 189–202. See also, "No foreign country should ever influence our politics and divide our people: PM Lee." *TODAY*, 19 November 2017. Available from: https://www.todayonline.com/singapore/no-foreign-country-should-ever-influence-our-politics-and-divide-our-people-pm-lee.

Singapore has learnt several important lessons from historical experiences as well as from other states about dealing with attempts by foreign actors to interfere in its domestic politics. Singapore has endeavoured to: (i) develop and utilise credible intelligence; (ii) protect the integrity of its electoral processes; (iii) carry out pre-emptive action against foreign subversion attempts; and most importantly, (iv) ensure its citizens are discerning and vigilant.

Today, competition between states in the global arena has grown more intense. Pressure on Singapore to align itself to other states' positions is apparent.[7] Yet, adopting a partisan position is not in Singapore's national interests as it jeopardises its sovereignty, independence, and the essential values on which it was founded.[8]

The threat of foreign interference in Singapore's domestic politics is therefore, a reality. This has become more challenging due in part to the availability and use of advance Information and Communications Technology (ICT) tools that make attribution and detection difficult. Additionally, subverting domestic politics by influencing public opinion via information that might seem benign compounds existing complexities.

Hostile Information Campaigns (HICs) in today's context can be understood to be covert and coordinated attempts by foreign actors to penetrate various segments and levels of society, with the intent of creating and spreading information intended to manipulate public sentiment and harm Singapore's interests. As HICs can include truths, half-truths, satire and a wide variety of other information forms, it is difficult to identify the many complex layers that often obscure the tactics of foreign actors.

---

[7] See for example, "Time for Singapore to move away from Uncle Sam's embrace?" *The Straits Times*, 7 January 2017. Available from: https://www.straitstimes.com/opinion/spore-china-ties-at-a-crossroads; "Singapore will not be seen as a stooge of US or China if it acts on its own interests: PM Lee." *TODAY*, 8 June 2019. Available from: https://www.todayonline.com/singapore/singapore-will-not-be-seen-stooge-us-or-china-if-it-acts-its-own-interests-pm-lee.

[8] See Rajaratnam, S. "Singapore's Foreign Policy, Untitled Speech 1965", reproduced in *S. Rajaratnam: The Prophetic and the Political*, Chan Heng Chee & Obaid Ul Haq (eds.), 279-296. Singapore: Institute of Southeast Asian Studies, 2007.

In light of recent international cases where foreign interference in domestic politics were detected (e.g., the French and the US presidential elections in 2017 and 2016 respectively),[9] and that Singapore's general election is forthcoming, this report discusses some of the major issues and challenges related to foreign interference in domestic politics, as it applies to the city-state.

It is envisaged that by doing so, we will increase awareness of the related risks and complexities of foreign interference in Singapore's domestic politics. For ease of reading, the report is written as responses to six key questions about the topic.

[9] For details, see Centre for Strategic Studies (CSIS) Brief. "Successfully Countering Russian Electoral Interference." 21 June 2018. Available from: https://www.csis.org/analysis/successfully-countering-russian-electoral-interference.; Council on Foreign Relations. "Russia, Trump, and the 2016 U.S. Election." 26 February 2018. Available: https://www.cfr.org/backgrounder/russia-trump-and-2016-us-election.

Six Key Questions and Responses

1. Why do foreign actors interfere in the domestic politics of another state? And, why is Singapore a target today?

Interfering with the aim of advancing state interests. An analysis of historical and contemporary case studies suggests that foreign actors interfere in the domestic politics of the target state to advance another state's national interests.

It is difficult to tell if these actors act on their own initiative, are state-sponsored or are state-aligned. However, their actions and the outcomes they pursue are often clearly in the service of the state they represent. The stakes are higher especially if the foreign actor's state is embroiled in a global competition for dominance with another state. Thus, having other states align with its position and interests is vital. Interference in domestic politics, even in a state that is considered an ally, is one method to ensure a favourable outcome.

For instance, the Cold War era from 1946 to 1991 that saw the United States of America (US) and the Union of Soviet Socialist Republics (USSR) embroiled in a geopolitical and ideological battle for dominance. "Aggressive arms race, proxy wars, and ideological bids" were tangible features of this conflict.[10]

[10] National Geographic. "What was the Cold War?" Available from: https://www.nationalgeographic.com/culture/topics/reference/cold-war/.

Overt, covert and technological means. Singapore, as part of Southeast Asia, was perceived by the US and USSR as strategically important.[11] Having a Singapore government and polity that was aligned with their interests was critical. Both overt and covert approaches were used for this purpose. These included establishing diplomatic ties and trade,[12] cultivating politicians, using propaganda to influence the ground,[13] and espionage.[14]

[11] See "Singapore attractive target for espionage, foreign subversion." *TODAY*, 21 March 2012.

[12] With regard to the USSR, see Hong, Mark. "Russia-Singapore Relations: Thirty-Seven Years of Cooperation and Dialogue", in *ASEAN-Russia Relations*, Gennady Chufrin, Mark Hong and Teo Kah Beng (eds.), 65–70. Singapore: Institute of Southeast Asian Studies – Yusof Ishak Institute, 2006. With regard to the US, see Chua, Daniel. *US-Singapore Relations*, 1965-1975, 163-188. Singapore: National University of Singapore Press, 2017.

[13] Carl Trocki describes some of the methods used by the US in Singapore. These include planting bogus news reports that were designed to support anti-communist movements. See Trocki, Carl A. *Singapore: Wealth, Power and the Culture of Control*. 110-111. Routledge: London and New York, 2006.

[14] "In the late 1970s, a code clerk working in the Singapore Embassy in Moscow, the then Soviet Union, was seduced by a Soviet spy. He started giving her decoded messages and eventually gave her the secret codes he worked with. This meant that the Soviets were able to decode and read all the messages sent and received by the Singapore Embassy in Moscow". See Ministry of Home Affairs, Singapore. "A Singapore Safe for all." Available from: https://www.mha.gov.sg/docs/ default-source/others/isa_booklet-english.pdf.; see also "Special Soviet privileges for cypher man", *The Straits Times*, 26 March 1980.
In 1960, the CIA attempted to bribe a Singapore intelligence officer for information but was unsuccessful. See "'Improper activities' by American officials." *The Straits Times*, 30 August 2015. Available from: https://www.straitstimes.com/singapore/improper-activities-by-american-officials.
In the 1990s, the government also moved against a Singapore Permanent Resident who was a "deep-cover operative of a foreign intelligence service", who had used "a Singaporean as a collaborator". See "6 held for Espionage." *The Straits Times*, 22 January 1999.
In 1982, Singapore expelled two Soviet nationals for espionage. One of the men had tried to cultivate a military officer. See Singapore Government Press Release. "Expelled for Espionage activities." 22 February 1982. Available from: http://www.nas.gov.sg/archivesonline/data/ pdfdoc/802-1982-02-22.pdf.

Today, inter-state competition has grown more intense. Southeast Asia has once again become an important theatre where this rivalry plays out.[15] Singapore has made it clear that being aligned to any particular state is not in its national interests.[16] Nevertheless, the possibility of Singapore becoming a target of foreign interference, in an effort to nudge it toward a particular policy position or action, cannot be ruled out.[17] That Singapore is open, multiracial/multi-religious and interconnected (on and offline), makes it particularly vulnerable.

Inexpensive means. On a related point, the availability of ICTs is a game-changer. This is because ICTs not only enable new pathways to influence a target state and its people, but also allows the interfering state and/or its agents to conceal their true intentions. Furthermore, as using and deploying ICTs in HICs is relatively inexpensive, many more states can use such tactics without worrying about budgets.[18]

2. What does foreign interference in domestic politics look like? And, who is being targeted?

Often, many complex layers obscure the tactics of foreign actors when interfering in the domestic politics of another state. Designed to mask the true intent of their actions, such methods have become more sophisticated over the years.

---

[15] Shambaugh, David. "U.S.-China Rivalry in Southeast Asia: Power Shift or Competitive Coexistence?" *International Security*, 42, Issue 4 (Spring 2018): 85-127.

[16] See "Defence Minister Ng Eng Hen stresses neutrality amid US-China dispute on Tokyo visit." *The Straits Times*, 21 May 2019. Available from: https://www.straitstimes.com/asia/east-asia/singapores-defence-minister-ng-eng-hen-in-tokyo-stresses-neutrality-amid-us-china.; "Singapore will continue not to take sides between US and China, says PM Lee Hsien Loong." *South China Morning Post*, 18 August 2019. Available from: https://www.scmp.com/news/asia/southeast-asia/article/3023326/singapore-will-continue-not-take-sides-between-us-and.; "Bilahari Kausikan on Singapore and US-China Competition." *The Diplomat*, July 2019, Issue 56. Available from: https://magazine. thediplomat.com/#/issues/-Li7vjiLcZOln1Btc9rh/read.

[17] For example, in 2017, Singapore moved against a professor who had been identified as "an agent of influence of a foreign country". According to the Ministry of Home Affairs, "he knowingly interacted with intelligence organisations and agents of the foreign country, and co-operated with them to influence the Singapore Government's foreign policy and public opinion in Singapore. To this end, he engaged prominent and influential Singaporeans and gave them what he claimed was 'privileged information' about the foreign country, so as to influence their opinions in favour of that country". The professor also recruited others "in aid of his operations". See "MHA's statement on Huang Jing, LKY School professor who tried to influence S'pore foreign policy." *Channel NewsAsia*, 4 August 2017. Available from: https://www.channelnewsasia.com/news/singapore/mha-s-statement-on-huang-jing-lky-school-professor-who-tried-to-9093570.

[18] Belfer Center for Science and International Affairs. "National Counter Information Operations Strategy." *Defending Digital Democracy*, February 2019, p. 8. Available from: https://www.belfercenter.org/sites/default/files/files/publication/CounterIO.pdf.

Foreign entities as agents of influence. Direct interference by states might not always be the best tactic to employ. Rather, foreign non-state actors, i.e., those not affiliated with, directed by, or funded by a government can be deployed as agents of influence. These foreign non-state actors can be either sponsored, linked, or act on behalf of the interfering state, or can act on their own initiative. These entities can include individuals, corporations, private financial institutions, and non-governmental organisations (NGOs).

Interfering in domestic politics can be a long game. If the foreign entity conducting an influence campaign is state-linked or state-sponsored, or has sufficient privately-owned resources (financial or otherwise), then they can afford to play a long game. This means that the result, for instance, an election outcome that is favourable to the interfering state, or "friendlier policies" from the targeted state, may only be realised in the future.

Offline and online efforts work in tandem to increase effectiveness. In the past, influence through disinformation and/or misinformation was conducted via newspapers, radio/television broadcasts, periodicals, and word-of-mouth (e.g., public rallies). Influence was also disseminated through personal relationships (cultivation via personal ties and friendships) and infiltration of civic society organisations.[19]

[19] See for example, Lee, Ting Hui. *The Communist Organisation in Singapore, 1948-66*. Singapore: Institute of Southeast Asian Studies, 1976.; Lee, Ting Hui. *The Open United Front: The Communist Struggle in Singapore 1954-1966*. Singapore: South Seas Society, 1996.

Today, influence through disinformation and/or misinformation is carried out mainly on the Internet and social media as these platforms are inexpensive, offer anonymity, and reach a wider audience more quickly than traditional offline methods.[20] Furthermore, as so much information is available online, detecting the spread of disinformation and/or misinformation is challenging and takes time to decipher. Amplification tools like bots[21] and astroturfing[22] also ensures disinformation and/or misinformation are targeted, aligned to personal predispositions, and are disseminated quickly, impairing effective responses.

Although a lot of focus has been placed on dealing with online disinformation and/or misinformation, it should be noted that such media still require ***offline or tangible issues*** to feed off to appear credible. Hence, the most effective approach when attempting subversion of domestic politics is to use both offline and online methods in tandem.

Tactics can be both covert and overt. The challenge is that it is difficult to know if an incident or social media post is actually part of a state-sponsored HIC until a thorough investigation is carried out to determine intention. Yet, by the time such an investigation is completed, it could already be too late.

Singapore is particularly vulnerable as it is an "open, democratic, digitally-connected and diverse country".[23] Furthermore, it operates according to a whole-of-government/whole-of-society framework, such that a HIC attack on one sector (e.g., public institutions) can have major repercussions on another.

---

[20] Canadian Centre for Cyber Security. "Global Baseline of Known Events." Available from: https://cyber.gc.ca/en/guidance/global-baseline-known-events.

[21] As a report from *The Straits Times* highlights, "sophisticated botnets on Twitter were used to influence the results of the election of a new leader for the African National Congress in December 2017. These accounts were created to impersonate genuine Twitter users in order to seem more legitimate. They shared same names with Twitter users, but replaced lower-case 'Ls' with '1s' and 'Os' with numerical zeros". See "Disinformation in Action." *The Straits Times*, 16 March 2018. Available from: https://www.straitstimes.com/sites/default/files/attachments/2018/03/16/st_20180316_vnfake2_3839240.pdf.

[22] Astroturfing is the attempt to create a false impression of widespread grassroots support for or opposition to a particular agenda. For more information, see Bienkov, Adam. "Astroturfing: What is it and why does it matter?." *The Guardian*, 8 February 2012. Available from: https://www.theguardian.com/commentisfree/2012/feb/08/what-is-astroturfing.

[23] Parliamentary Speeches and Responses, Ministry of Law, Singapore. "Oral Answer by Senior Minister of State for Law, Mr Edwin Tong to Parliamentary Question on Foreign Interference." 12 February 2019. Available from: https://www.mlaw.gov.sg/content/minlaw/en/news/parliamentary-speeches-and-responses/Oral-Answer-by-Senior-Minister-of-State-for-Law-Edwin-Tong-to-Parliamentary-Question-on-Foreign-Interference.html.

Targeting political elites. As political elites wield considerable policy and decision-making powers, they are often the prime targets of the interfering state. The intensity of interference is contingent upon how aligned the thinking and behaviour of the political elites are to the interests of the interfering state.

If the geopolitical views of the targeted state's political elites are severely misaligned from the intentions of the foreign actor or state, then a change of government would be deemed necessary. However, accomplishing this task would not be simple, especially when considering political office holders in most democracies remain in office only for approximately four to five years. Nevertheless, this does not mean that the interfering state will be discouraged from trying.

If the geopolitical views of the targeted state's political elites are slightly misaligned, then a change of government would not be necessary. Rather, agents of influence operating within political elite circles could be deployed to help nudge the targeted state toward policies that are more favourable to the interfering state.

As political elites are answerable to their constituents who comprise different sectors of society, the interfering state and/or foreign actors need to ensure that the citizenry is also included in the influence operation.

Targeting different sectors of society. If the goal is to change the government of the day, in addition to targeting the political elites of the target state, agents of the interfering state could target public institutions/agencies, public policies and social fault lines. The key objective would then be to foment public dissatisfaction against the government as a whole.

Over time, the loss of confidence and trust in the government, public institutions and public policies, would make it easier to attain an election outcome that was favourable to the interfering state's interests. If the objective is to extract "friendlier policies", then agents could direct their influence and leverage important non-government sectors to indirectly exert pressure on political elites.[24]

[24] Abdul Rahman, Muhammad Faizal. "Defending Singapore against Foreign Interference." *RSIS Commentaries*, 3 September 2019. Available from: https://www.rsis.edu.sg/rsis-publication/cens/defending-singapore-against-foreign-interference/#.XXnoT2kza70.

3. Has Singapore been targeted in the past?

As mentioned earlier, Singapore has experienced attempts by other states to interfere in its domestic politics. As a result, Singapore has drawn lessons from these incidents, as well as the experiences of other countries that have been targeted by foreign interference campaigns. The examples listed below underscore some of the points made above.

Targeting political elites. A 1959 Commission of Inquiry revealed that a senior political office holder from the Singapore People's Alliance had received funds from a foreign source as a "political gift" to the Labour Front, to help fight "subversion in the colony" and strengthen the Labour Front "as an effective party and bulwark against communism".[25]

Targeting the citizenry. In the 1970s, the government moved against three publications – The Eastern Sun,[26] The Singapore Herald,[27] and Nanyang Siang Pau[28] – for attempting to influence readers through their reports.[29] In the Nanyang Siang Pau case for example, newspaper executives were charged with implementing policies that aroused "communal emotions over issues of Chinese language and culture".[30]

---

[25] See "2nd Reading Speech by Minister for Home Affairs Mr Wong Kan Seng – Political Donations Bill", 22 May 2000, Available from: https://web.archive.org/web/20130122223736/http://www.mha.gov.sg/basic_content.aspx?pageid=66. See also Lee, Kuan Yew. *The Singapore Story: Memoirs of Lee Kuan Yew*, 293-295. Singapore: Straits Times Press and Marshall Cavendish, 1998.; Long, Joey. "The Chew Swee Kee affair revisited: Querying the American involvement in Singapore." *South East Asia Research*, 10, no.2 (2002): 217-239.

[26] See Lee, Kuan Yew. *From Third World to First: The Singapore Story: 1965-2000: Memoirs of Lee Kuan Yew*, 215-218. Singapore: Straits Times Press and Marshall Cavendish, 2000.

[27] Ibid.

[28] A Nanyang "Confession". *The Straits Times*, 23 May 1971. See also Singapore Infopedia, National Library Board, Singapore. "Nanyang Siang Pau." Last modified 6 January 2017. Available from: http://eresources.nlb.gov.sg/infopedia/articles/SIP_2017-01-10_095946.html.

[29] For how this was done, see Mothership. "3 local newspapers spread misinformation under 'black operations' & were taken to task in 1971." 11 January 2018. Available from: https://mothership.sg/2018/01/1971-fake-news-black-operations/.

[30] Ibid.

Investigations also revealed that foreign state actors covertly supported some of these publications.[31] For instance, the "The Eastern Sun was exposed by the government for having received HK$8 million from a Communist intelligence agency from Hong Kong. The funds were provided on the condition that it would not oppose… [the interfering state]…on major issues and publish news items of the communists' choice. The newspaper eventually folded in 1971."[32]

Targeting the electoral process. In 1988, a foreign diplomat was expelled for attempting to interfere in Singapore's elections by mobilising disaffected professionals to attack the government, as well as instigate their contestation in the general election.[33]

[31] Lee, Hsien Loong. "When the Press Misinforms", 8-9. Text of speech delivered at the 40th World Congress of Newspaper Publishers held at Helsinki. 26 May 1987. Available from: http://eresources.nlb.gov.sg/printheritage/detail/12d299c0-25e8-4b8c-ae26-edf0c5d49e90.aspx.

[32] See Ministry of Communications and Information, Singapore. "Speech by Dr Yaacob Ibrahim, Minister for Communications and Information, at the Parliament Sitting on 10 January 2018, on the Motion to convene a Select Committee to tackle online falsehoods". Available from: https://www.mci.gov.sg/pressroom/news-and-stories/pressroom/2018/1/speech-by-dr-yaacob-ibrahim-on-the-motion-to-convene-a-select-committee-to-tackle-online-falsehoods.

[33] See "Hand of US officials in local." *The Straits Times*, 8 May 1988; "Not in our interest to add to problems of US leaders." *The Straits Times*, 2 June 1988; see also, Mothership. "An American diplomat once tried to influence the 1988 Singapore General Election." 13 October 2017 Available from: https://mothership.sg/2017/10/an-american-diplomat-once-tried-to-influence-the-1988-singapore-general-election/.

Targeting civic organisations. The Malayan Communist Party (MCP)[34] infiltrated unions, student bodies, political associations and other civic groups as part of its United Front strategy[35] to seize political power in Singapore.[36] By doing so, it was able to exploit communal issues and/or existing social fault lines, and use such organisations as fronts to agitate against or pressure the government.[37]

4. What do new methods of influence look like?

While the use of offline methods is still common today, the availability of ICTs has expectedly made online methods more appealing.[38] The challenge today is not limited to disinformation and/or misinformation, but can also involve cyber attacks, particularly the theft of personal data. Several global and local examples elucidate.

---

[34] Bilveer Singh argues that "what should be noted about the MCP's attempt to promote communism in Malaya and Singapore, and to capture political power was the fact that the MCP was in active consultation with, and receiving support and guidance from communist China, which was locked in a bitter Cold War with the US and its allies, and after the Sino-Soviet split, with the USSR as well. In agreeing to the armed struggle on CCP's advice and financial support, the MCP was in effect taking instructions from a foreign communist party, furthering the goals and objectives of international communism or more specifically, China, at the expense of the national interests of Malaya and Singapore." See Singh, Bilveer. *Quest for Political Power: Communist Subversion and Militancy in Singapore*, 33. Singapore: Marshall Cavendish, 2015.

[35] The MCP had scaled down its violent activities in favour of non-violent ones as the former had been unsuccessful. See Singh, Bilveer. *Quest for Political Power: Communist Subversion and Militancy in Singapore*, 174. Singapore: Marshall Cavendish, 2015.

[36] Singh, Bilveer. Quest for Political Power: Communist Subversion and Militancy in Singapore. Singapore: Marshall Cavendish, 2015.

[37] For example, a declassified 1955 CIA report on Communist Prospects in Malaya and British Borneo observes that in Singapore, "…Communists are most active in infiltrating Chinese youth groups and Chinese schools; and they have registered considerable success...Agitators helped organise student strikes against compulsory registration for military service, and resistance to government measures regulating schools and youth associations...They recently demonstrated their power to exploit a union grievance by organising a large-scale disorder, in which Chinese students combined with strikers to paralyse a section of the city". See Central Intelligence Agency. "Communist Prospects in Malaya and British Borneo." *National Intelligence Estimate*, Number 64-55. 24 May 1955. Available from: https://www.cia.gov/library/readingroom/docs/CIA-RDP79R01012A006000030014-9.pdf.

[38] "Fears about the possibility of foreign actors sowing discord and disinformation in an election campaign are well-founded…The tactics have included fake online news articles, doctored photos and audio recordings. The content is often shared and promoted using fake online accounts and automated Twitter bots". See "Canadian academics, scientists fight back against online election disinformation." *Global News*, 13 September 2019. Available from: https://globalnews.ca/ news/5901707/canadian-academics-scientists-election-disinformation/.

Targeting political elites (offline). In 2017, an Australian state senator "resigned from his post after he was found to have accepted money from foreign donors that had links with a foreign state". He had also gone against his party's position in favour of the state in question's position.[39]

In 2018, an opposition party leader in New Zealand allegedly tried to disguise a donation from a businessman who had links with a foreign government.[40]

Targeting the electorate (online). In the 2017 French presidential election[41], hackers stole a cache of emails from the campaign staff of Emmanuel Macron's *En Marche!* Party. They also carried out a disinformation campaign that comprised of rumours, disinformation and forged documents, and leaked 15 gigabytes of stolen data, which included 21,075 emails, two days before the second and final round of the French presidential election, just hours before the media cooling off period was to begin.[42] Investigations revealed that this was done to influence voters and get them to vote for National Front leader Marine Le Pen.[43]

---

[39] "Singapore eyes new laws as other countries grapple with foreign influence." *TODAY*, 12 February 2019. Available from: https://www.todayonline.com/singapore/singapore-eyes-new-laws-other-countries-grapple-foreign-influence.

[40] "China donations claims throw New Zealand politics into turmoil." *Financial Times*, 18 October 2018. Available from: https://www.ft.com/content/7f1eba1c-d1e8-11e8-a9f2-7574db66bcd5.

[41] Owing largely to the conscious efforts by the French government and the Macron campaign, coupled with the missteps made by the hackers themselves, Macron won the French presidency in a landslide victory. For more, see Aisch, G. et al. "How France Voted". *The New York Times*, 7 May 2017. Available from: https://www.nytimes.com/interactive/2017/05/07/world/europe/france-election-results-maps.html.

[42] Vilmr, Jean-Baptiste. "The '#Macron Leaks' Operation: A Post- Mortem." *Atlantic Council*, 20 June 2019. Available from: https://www.atlanticcouncil.org/publications/ reports/the-macron-leaks-operation-a-post-mortem.

[43] Wemer, David. "How to Weather a Hack: Lessons from the Macron Leaks." *Atlantic Council*, 26 June 2019. Available from: https://www.atlanticcouncil.org/blogs/new-atlanticist/how-to-weather-a-hack-lessons-from-the-macron-leaks.; Vilmr, Jean-Baptiste. "The '#Macron Leaks' Operation: A Post-Mortem." *Atlantic Council*, 20 June 2019. Available from: https://www.atlanticcouncil.org/publications/ reports/the-macron-leaks-operation-a-post-mortem.

Cyber attacks. In 2018, state-sponsored hackers attacked SingHealth's national database and stole data of 1.5 million individuals, including that of Prime Minister Lee Hsien Loong's (PM Lee).[44] While it is still unclear as to how the hackers intend to use the stolen information, the potential for the data to be used against specific individuals cannot be ruled out.[45]

Targeting public institutions. According to a 2019 Home Team Behavioural Science Centre (HTBSC) report,[46] government agencies are the most frequently targeted vis-à-vis deliberate online falsehoods. Such articles/reports often attempt to either accuse the agency of missteps or magnify the alleged missteps of the agency to undermine public confidence.

In November 2018, an online news article falsely linking PM Lee to the 1Malaysia Development Berhad (1MDB) scandal was published on the States Times Review website, and was circulated on a Malaysian website known as The Coverage.[47] The article, which was labelled by Singapore's High Commission in Malaysia "as fake news and libellous", "alleged that Malaysia had signed several unfair agreements with Singapore, in exchange for Singapore banks' assistance in laundering 1MDB's funds".[48] The article also purported that Singapore was reluctant to investigate the 1MDB scandal, only reopening its investigations after it was forced to do so after the change in political leadership in Malaysia.[49] The Monetary Authority of Singapore was unfairly and inaccurately implicated in the article as well.

---

[44] Tham, Irene. "Personal info of 1.5m SingHealth patients, including PM Lee, stolen in Singapore's worst cyber attack." *The Straits Times*, 20 July 2018. Available from: https://www.straitstimes.com/singapore/personal-info-of-15m-singhealth-patients-including-pm-lee-stolen-in-singapores-most.

[45] Kwang, Kevin. "SingHealth cyberattack likely by nation state, medical data 'can fetch a high price': Experts.", *Channel NewsAsia*, 20 July 2018. Available from: https://www.channelnewsasia.com/news/singapore/singhealth-cyberattack-likely-nation-state-medical-data-price-10549372.

[46] Chen, Xingyu and Neo, Loo Seng "The threat of fake news in Singapore: Prevalence, impact, and methods of transmission" (HTBSC Research Report 14/2019). Singapore: Home Team Behavioural Sciences Centre.

[47] "Online article on PM Lee libellous and fake: Singapore". *The Straits Times*, 8 November 2018. Available from: https://www.straitstimes.com/singapore/online-article-on-pm-lee-libellous-and-fake-spore.

[48] "MAS files police report against author of defamatory article relating to 1MDB." *The Straits Times*, 8 November 2018. Available from: https://www.straitstimes.com/singapore/report-linking-pm-lee-to-1mdb-is-fake-libellous-singapore-high-commission-in-malaysia.

[49] Ibid.

Using organisations and HICs in tandem. A state-linked company was found to have attempted to influence politics in the US between 2014 and 2018, via various methods ranging from: using social media accounts designed to appeal to US audiences; organising political rallies through its employees' collaboration with US political activists; and hacking computers and email accounts of organisations, employees and volunteers associated with the Clinton Campaign.[50] The company also targeted and recruited Americans to augment its messages on both social media and various political activities.[51]

5. What steps have been taken to minimise the risks?

It should be emphasised that there is no way to eliminate the threat of foreign interference in domestic politics. Hence, the next best option is to try and mitigate the risks. That foreign influence can emanate from a variety of sources suggests that a multi-pronged approach involving different segments of society is required.

Singapore has in place several online and offline measures designed to minimise the risks from interference in its domestic politics by foreign actors. These include:

Protecting election integrity. In 2001, the Singapore government introduced the Political Donations Act to "prevent foreigners from interfering in Singapore's domestic politics through funding of candidates and political associations".[52] Election candidates and political associations are required to declare their funding sources to the Registrar. "Donors who have made multiple small donations with an aggregate value of $10,000 or more to a political association in a calendar year" must also make a declaration to the Registrar.[53]

---

[50] Besides asserting Russia's interference in the 2016 US presidential election, the Mueller Report highlights the use of ICTs and in particular, social media platforms like Twitter and Facebook as part of a larger planned operation to undermine the outcome of the 2016 US presidential election. By the end of the 2016 US presidential election, the report stated that the IRA had the ability to reach at least 29 million US individuals through their social media accounts. IRA-controlled Facebook groups and Instagram accounts also had hundreds of thousands of US participants while IRA-controlled Twitter accounts had tens of thousands of US followers, including media outlets, high profile US political figures and persons, such as former US Ambassador to Russia Michael McFaul, Sean Hannity, and Michael Flynn Jr who had retweeted or responded to the IRA accounts and IRA-created content. See Mueller, Robert. "Report On The Investigation Into Russian Interference in the 2016 Presidential Election." Volume I. *US Department of Justice*, 2019. Available from: file:///E:/NSSP/ MHA%20-%20 FIDPA/muellerreport.pdf.

[51] Mueller, Robert. "Report On The Investigation Into Russian Interference in the 2016 Presidential Election." Volume I. *US Department of Justice*, 2019. Available from: file:///E:/NSSP/MHA%20-%20 FIDPA/muellerreport.pdf.

[52] Elections Department, Singapore. "Overview of Political Donations Act". Available from: https://www.eld.gov.sg/registry.html.

[53] Ibid.

Protecting civic organisations. Organisations that are not political parties, but wish to be involved in domestic political issues are required to register as political associations.[54] This requirement extends to organisations that operate socio-political websites as well.[55] The rationale for this approach is to mitigate the risks of influence in such organisations via funding from foreign states or proxies.

Preventing deliberate online misinformation and falsehoods. With regard to online disinformation and misinformation, Singapore passed the Protection from Online Falsehoods and Manipulation Act (POFMA) in May 2019. This law aims to correct falsehoods, control and or prevent further dissemination of such falsehoods, and in serious cases, disable the means of dissemination.

POFMA's primary tool is "correction notices, which counter [the] effects of falsehoods", and does not "impose criminal liability" on "sharing falsehoods in good faith".[56] POFMA also applies "to false statements of fact, as opposed to opinions". For more serious cases, "take-downs", "account restrictions" and "declaration of online location" may be used.[57]

Cybersecurity and digital media literacy. Resources have been devoted to enhance cyber security awareness, particularly cyber hygiene,[58] and digital media literacy.[59] These are designed to minimise the risks from cyber attacks as well as to help individuals become more discerning when they engage with online information.

---

[54] "Under the Political Donations Act, the government can declare an organisation to be a political association as long as the organisation's objectives or activities 'relate wholly or mainly to politics in Singapore'". See "The Online Citizen website and two other groups no longer considered political associations." *The Straits Times*, 9 February 2018. Available from: https://www.straitstimes.com/politics/the-online-citizen-website-and-two-other-groups-no-longer-considered-political-associations. For in-depth coverage on some of the issues, see "When activists cross a line." *The Straits Times*, 4 May 2013.

[55] "Blog to register as political group." *The Straits Times*, 12 January 2011.

[56] Ministry of Law, Singapore. "Protection from Online Falsehoods and Manipulation Act." Available from: https://www.mlaw.gov.sg/content/dam/minlaw/corp/News/Press%20Release/POFMB/POFMA-Brochure.pdf.

[57] Ibid.

[58] "More users aware of cyber risks, but some complacent." *The Straits Times*, 12 September 2019. Available from: https://www.straitstimes.com/tech/more-users-aware-of-cyber-risks-but-some-complacent.

[59] See for example, "National framework to build information and media literacy to be launched in 2019: S Iswaran." *Channel NewsAsia*, 2 November 2018. Available from: https://www.channelnewsasia.com/news/singapore/framework-build-information-media-literacy-launched-2019-iswaran-10890438. See also the National Library Board's (NLB) S.U.R.E Initiative. Available from: http://www.nlb.gov.sg/sure/category/fake-news/page/3/.; "More users aware of cyber risks, but some complacent." *The Straits Times*, 12 September 2019. Available from: https://www.straitstimes.com/tech/more-users-aware-of-cyber-risks-but-some-complacent.

6. Is there more that can be done?

There are of course additional measures Singapore could implement to tackle the challenge of foreign interference. These include updating existing legislation pertaining to foreign interference in domestic politics, empowering and equipping law enforcement with the necessary tools to carry out deep investigations, enhancing the protection of election integrity, and educating/mobilising society to resist foreign interference.

Regulation. While Singapore may not be able to control what happens beyond its borders, it can and does have control over what happens within them. Regulating certain activities through legislation is one way of doing so as it will help deter possible instances of foreign subversion in the future.[60]

Additionally, as foreign influence can emanate from a variety of sources, updating legislation in other related fields (e.g., telecommunications) is necessary.[61] This will ensure Singapore's response is compatible with current technologies and methods of foreign interference. Doing so will also enable Singapore to carry out swift responses that are targeted, so as to address the issues at hand in a timely manner.

[60] "Government to consider legislation against foreign interference: Edwin Tong." *Channel NewsAsia*, 12 February 2019. Available from: https://www.channelnewsasia.com/news/singapore/foreign-interference-singapore-foreign-actors-update-to-law-11232564.

[61] In 2018, Australia passed new legislation to guard against foreign interference that applied to many different sectors. The laws introduced "new spying offences", updated "sabotage offences", made industrial espionage on behalf of a foreign government an offence, and introduced the "Foreign Influence Transparency Scheme…[where]…people or companies in Australia who are acting on behalf of foreign principals in the political sphere will have to register and detail their activities on a public website". Australia also banned foreign political donations. See "Sweeping foreign interference and spying laws pass Senate." *The Guardian*, 28 June 2018. Available from: https://www.theguardian.com/australia-news/2018/jun/29/sweeping-foreign-interference-and-spying-laws-pass-senate.; Lowy Institute. "Australia's new foreign-influence laws: Who is targeted?." 5 December 2018. Available from:https://www.lowyinstitute.org/the-interpreter/australia-new-foreign-influence-laws-who-targeted; "Australia passes foreign interference laws amid China tension." *BBC*, 28 June 2018. Available from: https://www.bbc.com/news/world-australia-44624270.

Empowering law enforcement. Investigations to determine if a particular offline and/or online activity is state-linked or state-sponsored have become more challenging. As such, investigators and law enforcement agencies require both legislative support and technological tools to conduct deeper analyses and investigations to uncover and determine the intent of foreign subversion.

Enhancing election integrity protection. Elections comprise many components: candidates, political parties, political donations, election infrastructure, individuals connected to political parties (e.g., campaigners and volunteers), and so on.

A comprehensive review of Singapore's electoral process to determine possible avenues for foreign interference by offline and online means should be carried out.

This is especially so as more components of electoral systems now have online dimensions. For example, campaign funding, which used to be conducted primarily offline, can now be done online (e.g., crowdsourcing, donation drives, and appeals). The use of crypto and digital currencies in campaign funding also poses another challenge, adding to the complexity of ensuring the integrity of the electoral process.[62]

Mobilising all segments of society to resist foreign interference in domestic politics. Lessons can be drawn from the Swedish response to foreign interference in its domestic politics. The Swedes deployed a "whole-of-society approach", which was spearheaded by the government and involved a "high-level inter-agency coordination forum… [that served]…as a national platform for election planning, preparation, and protection". Election officials were trained to "identify and resist such influence", while "major media outlets collaborated to combat fake news". In addition, a "pop-up" newsroom of "students, international journalists, and fact-checkers" were deployed to track "sources of disinformation ahead of the election, and published a daily newsletter addressed to news organisations".[63]

---

[62] See for instance, Burcher, Catalina Uribe. "Cryptocurrencies and Political Finance." *International IDEA Discussion Paper*, Volume 2, 2019. Available from: https://www.idea.int/sites/default/files/publications/cryptocurrrencies-and-political-finance.pdf; "Bitcoin is gaining currency in political campaign donations." *ABC News*, 7 February 2018. Available from: https://abcnews.go.com/Politics/bitcoin-popular-political-campaign-donations/story?id=52873921.

[63] See Taylor, Margaret. "Combating disinformation and foreign interference in democracies: Lessons from Europe." *Brookings Institute*, 31 July 2019. Available from: https://www.brookings.edu/blog/techtank/2019/07/31/combating-disinformation-and-foreign-interference-in-democracies-lessons-from-europe/.

The French government's efforts in preparing electoral campaign staff with tools necessary to deal with disinformation attacks before the 2017 French presidential election, coupled with growing public awareness of the impact disinformation and HICs can have, as well as the Macron campaign having planted false flags[64] to slow the hackers down after the email dump occurred, contributed to the French people and media viewing the leaked Macron documents with suspicion.

By overwhelming the hackers with false information, as well as inserting pop culture references that the French audience was able to recognise as ridiculous caricatures rather than as potentially scandalous political actors, it was possible for Macron's campaign team to discredit the leaks even before the media blackout occurred.[65] Additionally, the attackers underestimated the ability of Macron's campaign team to respond as swiftly and as aptly as they did. The short time period the hackers left to disseminate the leaked documents, coupled with the use of English terms and expressions, thus backfired, as their content had limited reach within the French-speaking audience.

Such preparation and alertness having weakened the influence of the Macron Leaks, ultimately resulted in the failed attempt to undermine Emmanuel Macron's candidacy.[66]

[64] Greenburg, Andy. "Hackers Hit Macron with Huge Email Leak Ahead of French Election". *Wired*, 5 May 2017. Retrieved from: https://www.wired.com/2017/05/macron-email-hack-french-election/.

[65] Vilmr, Jean-Baptiste. "The "#Macron Leaks" Operation: A Post-Mortem". *Atlantic Council*, 20 June 2019. Retrieved from: https://www.atlanticcouncil.org/publications/reports/the-macron-leaks-operation-a-post-mortem.

[66] See Vilmr, Jean-Baptiste. "The '#Macron Leaks' Operation: A Post-Mortem." *Atlantic Council*, 20 June 2019. Available from: https://www.atlanticcouncil.org/publications/reports/the-macron-leaks-operation-a-post-mortem.; Wemer, David. "How to Weather a Hack: Lessons from the Macron Leaks." *Atlantic Council*, 26 June 2019. Available from: https://www.atlanticcouncil.org/blogs/new-atlanticist/how-to-weather-a-hack-lessons-from-the-macron-leaks.

Conclusion

Singapore has by and large tried to be a good student of history. Singapore has learnt a lot from its past experiences and those of other countries on how to resist foreign interference in its domestic politics. But, the game has changed significantly. Inter-state competition, together with advanced technologies that create new avenues for exploitation and influence, suggest greater complexity pertaining to the challenge of foreign interference in Singapore's domestic politics.

This challenge is not partisan, but affects Singapore's national security and interests. Suffice to say, an interfering state's national interests must not be advanced at the expense of Singapore's national interests.

Given that advanced ICTs are readily available to interfering states and their associates, to severely impact the domestic political sphere of a highly digitised society like Singapore's – and to do so in sophisticated ways so as to mask the true source of such hostile interventions, Singapore cannot afford to be complacent. As the protagonist in the movie The Usual Suspects, put it: "The greatest trick the devil ever pulled was to convince the world he didn't exist".[67]

[67] Medium. "The Greatest Trick the Devil Ever Pulled Was Convincing the World God Didn't Exist." Available from: https://medium.com/@sergiofmonteiro/the-greatest-trick-the-devil-ever-pulled-was-convince-the-world-he-didnt-exist-3698070b83e0.

About the Authors

Damien D. Cheong is a Research Fellow and Acting Head of the National Security Studies Programme (NSSP), S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University, Singapore. Prior to this, he was Research Fellow and Coordinator of the Homeland Defence Programme at the Centre of Excellence for National Security (CENS) at RSIS from 2011-2017. He has researched and written on various topics related to homeland security, strategic communication and political violence. His current research focuses on small state security.

Stephanie Neubronner is a Research Fellow in the National Security Studies Programme at the S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University, Singapore. Her research interests include socio-cultural identity, governance and social relations, and the influence of new media. Stephanie obtained First Class Honours in Anthropology and Sociology from the University of Western Australia (UWA). She was subsequently awarded UWA's Postgraduate Award Scholarships and completed her PhD in Anthropology, Sociology and Geography. Prior to joining RSIS, Stephanie was a researcher at the Institute of Policy Studies, Lee Kuan Yew School of Public Policy, National University of Singapore.

Kumar Ramakrishna is a tenured Associate Professor, Associate Dean in charge of Policy Studies, as well as Head of the International Centre for Political Violence and Terrorism Research, S. Rajaratnam School of International Studies (RSIS), in Nanyang Technological University, Singapore. He is Research Advisor to the National Security Studies Programme. He was previously the Head of the Centre of Excellence for National Security (CENS) at RSIS from 2006-2015.

A historian by background, Associate Professor Ramakrishna has been a frequent speaker on counter-terrorism before local and international audiences, a regular media commentator on counter-terrorism, and an established author in numerous internationally refereed journals. His first book, Emergency Propaganda: The Winning of Malayan Hearts and Minds 1948-1958 (2002) was described by the International History Review as “required reading for historians of Malaya, and for those whose task is to counter insurgents, guerrillas, and terrorists”. His second major book, Radical Pathways: Understanding Muslim Radicalisation in Indonesia (2009) was featured as one of the top 150 books on terrorism and counterterrorism in the respected journal Perspectives on Terrorism, which identified Associate Professor Ramakrishna as “one of Southeast Asia’s leading counterterrorism experts”. His most recent books are Islamist Terrorism and Militancy in Indonesia: The Power of the Manichean Mindset (2015), Original Sin? Revising the Revisionist Critique of the 1963 Operation Coldstore in Singapore (2015), and Singapore Chronicles: Emergency (2016).

About the National Security Studies Programme

In April 2016, **National Security Studies Programme (NSSP)** was launched in RSIS. Coordinated then by Associate Professor Kumar Ramakrishna, Head of Policy Studies, Office of the Executive Deputy Chairman, RSIS, the aim of NSSP is to foster and enhance intellectual capital pertaining to the milestone episodes in Singapore's diplomatic and security history.

In particular, the NSSP will seek to promote broad-ranging research into the "Singapore model" for addressing national security challenges and other insights pertinent for small, globalised, multi-ethnic city-states.

Apart from producing research for RSIS and other academic audiences, and teaching on the Masters programme in RSIS, NSSP researchers will also be invited to share their insights with public officers in seminars or training courses, with a view to enhancing the academic rigour of such course content. In addition, seminars involving thought leaders from Singapore and elsewhere on the subject of the governance and security challenges facing city-states will also be organised by NSSP at periodic intervals.

For more information about NSSP, please visit www.rsis.edu.sg/research/national-security-studies-programme-nssp/

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 https://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