CASES OF FOREIGN INTERFERENCE IN ASIA

Muhammad Faizal Bin Abdul Rahman
Gulizar Haciyakupoglu
Benjamin Ang
Dymples Leong
Jennifer Yang
Teo Yi-Ling

Policy Report

March 2020

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

NANYANG TECHNOLOGICAL UNIVERSITY SINGAPORE

Policy Report

CASES OF FOREIGN INTERFERENCE IN ASIA

Muhammad Faizal Bin Abdul Rahman
Gulizar Haciyakupoglu
Benjamin Ang
Dymples Leong
Jennifer Yang
Teo Yi-Ling

March 2020

Table of Contents

Executive Summary

In the following pages, we examine cases of foreign interference in Asia, using a proposed framework to show the interplay between foreign interference, foreign influence, soft power, and hostile information campaigns. The cases are broadly categorised by tactics, including covert funding of politicians, parties, officials, influential persons, Non-Governmental Organisations (NGOs) and media; cyberattacks, and hostile information campaigns. The cases are taken from Singapore, Malaysia, Thailand, Taiwan, Hong Kong, and Australia.

We conclude that since there is a spectrum from open and legitimate influence to deceptive and illegitimate interference, it is necessary for states to clearly define the red lines which foreign entities must not cross in another state's domestic politics. States need to monitor and prevent said red lines from being crossed; and take effective countermeasures when foreign interference occurs.

1. Foreign Interference in the spotlight

Foreign interference has been in the international spotlight after Russia's alleged interference in the 2016 US Presidential and the 2017 French presidential election campaign. Although foreign interference is not a new problem, the term become a politicised buzzword in the years following the US elections, especially with different nations accusing one another of interference:

- The Russian Duma Commission on the Investigation of Foreign Interference in Russia's Internal Affairs has accused foreign media (BBC Russian Service, Voice of America) of breaking election laws. It alleged that foreign forces incited protests of the Russian opposition including unauthorized protests "coordinated by US intelligence agencies", and accused an American employee of the US Embassy in Russia of briefing the Russian opposition on "how to organize riots and "colour revolutions".[1]

- China's Defence Minister has warned other nations against interfering in China's internal affairs and inciting colour revolutions. China has blamed foreign countries, including the US, for inciting pro-democracy protests in Hong Kong.[2]

This is not new. Nations have attempted to interfere in one another's politics, for their own benefit, since the dawn of history.[3] The aggressor may have diverse motivations: the aggressor may want the target to change its foreign policy positions; it may have ideological motives like promoting democracy or discrediting it, and the aggressor may even seek regime change; or the target state might be of strategic value in the global power struggle between super powers.

Two new accelerators that have raised fresh alarms in governments are (i) the interconnected nature of the global economy, and (ii) use of technology to amplify this interference while keeping it disguised and plausibly deniable.

---

[1] Zdravko Ljubas, "Russian Duma Demands Measures Against Foreign Media." *Organized Crime and Corruption Reporting Project*, https://www.occrp.org/en/daily/10935-russian-duma-demands-measures-against-foreign-media.

[2] Danson Cheong, "Beijing Warns against Foreign Interference, Colour Revolutions." *The Straits Times*, 21 October 2019, https://www.straitstimes.com/asia/east-asia/beijing-warns-against-foreign-interference-colour-revolutions.

[3] 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.

- Globalisation and free trade have built the world economy but they have also made nations more interdependent as their supply chains for goods and services are now international. This has led to apprehensions concerning nations that supply key components of critical infrastructure, such as 5G technology, as they could have power over nations that depend on them. Akin to this, some argued that global trade programmes like China's "Belt and Road Initiative" – building networks of roads, ports, railways, power plants and other infrastructure projects in Southeast Asia, Europe and Africa– are actually intended to expand the country's political influence and military presence.[4]

- Technology has also increased the reach of aggressor states, acting as a "turbo-charger"[5] enabling "hostile information campaigns" to stoke protests, deepen divisions, increase hostility, and sow distrust in institutions. We discuss hostile information campaigns in greater detail further below.

This is of particular concern to nations like Singapore who have diverse, multi-cultural, multi-racial, multi-religious populations, and whose high level of connectivity enables aggressors to tap potential social fault lines or divisions.[6]

But because accusations of "foreign interference" often also have political implications and evidence is often murky, nations who are accused of foreign interference, as well as domestic actors who have been accused of being complicit in foreign interference, often contend that they have been wrongly accused.

[4] "Belt and Road Is No 'Win-Win' for China's Partners: US Study," *South China Morning Post*, 18 April 2018, https://www.scmp.com/news/china/diplomacy-defence/article/2142266/belt-and-roads-aim-promote-chinese-interests-and.

[5] Senior Parliamentary Secretary for Home Affairs Sun Xueling quoted by Matthew Mohan, "Singapore to Look at 'Entry Points' of Foreign Interference When Crafting Policy: Sun Xueling." *CNA*, 3 October 2019,

[6] Fabian Koh, "Foreign meddlers seek to stir anger in societies by exploiting divisive issues: Expert", *The Straits Times*, 25 Sept. 2019, https://www.straitstimes.com/politics/foreign-meddlers-seek-to-stir-anger-in-societies-by-exploiting-divisive-issues

- China's foreign ministry has said the Australian Security Intelligence Organisation's accusations of Chinese interference were "a ruthless trick of fabrication brought about by a small domestic faction in order to achieve ulterior political goals".[7]

- Political activists have cited fears that governments may use foreign interference as a pretext to target local dissent,[8] smear local activists,[9] and claimed that allegations of foreign interference have been used as a tactic to clamp down on political dissent, including arresting and detaining opposition members and critics.[10]

[7] "Australian intelligence agency wants more resources to counter foreign interference", *TODAY*, 17 October 2019, https://www.todayonline.com/world/australian-intelligence-agency-wants-more-resources-counter-foreign-interference

[8] Bhavan Jaipragas, "As Singapore gears up to fight foreign interference, could political critics be caught in the cross hairs?", *South China Morning Post*, 29 September 2019. https://www.scmp.com/week-asia/politics/article/3030722/singapore-gears-fight-foreign-interference-could-political

[9] Grace Ho, "New Naratif co-founder Kirsten Han responds to Shanmugam's remarks on foreign interference", *The Straits Times*, 26 September 2019, https://www.straitstimes.com/singapore/new-naratif-co-founder-kirsten-han-responds-to-shanmugams-remarks-on-foreign-interference

[10] Danisha Hakeem, "Foreign interference" narrative "a time tested tactic" preceding clampdowns by PAP govt: Function 8", *The Online Citizen*, 26 September 2019, https://www.theonlinecitizen.com/2019/09/26/foreign-interference-narrative-a-time-tested-tactic-preceding-clampdowns-by-pap-govt-function-8/

2. Framework

We propose in Figure 1 below a framework for understanding the relationship between foreign interference, foreign influence, and hostile information campaigns below. This framework should be viewed with the understanding that the definitions can be fluid, grey areas abound, and what is condemned as "foreign interference" by one nation may not be regarded as interference by another.

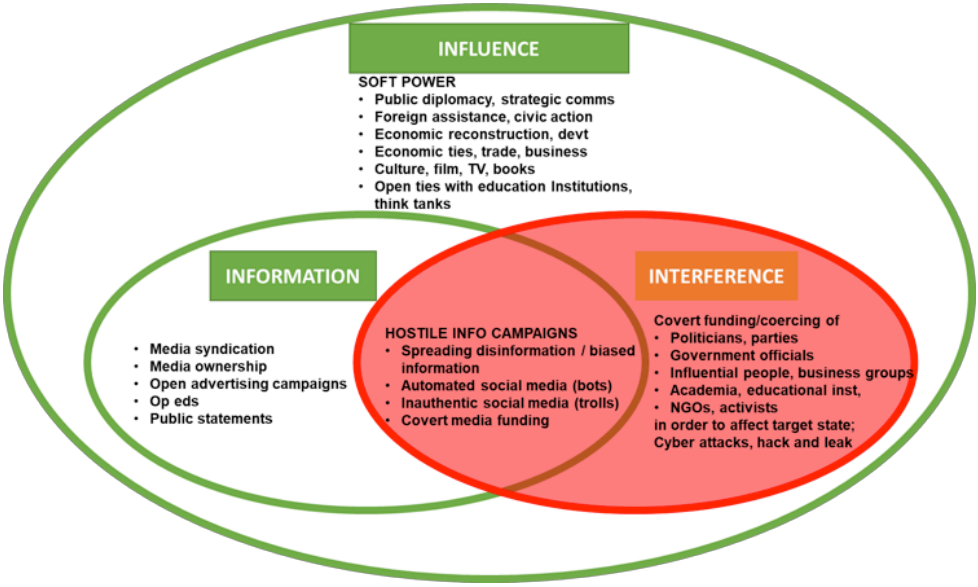

Figure 1- A framework derived by the authors for understanding the relationship between foreign interference, foreign influence, and hostile information campaigns.

2.1. Foreign Interference

Foreign interference occurs when a foreign entity (state or non-state actor), with hostile intent, takes actions to deliberately, covertly and deceptively disrupt the politics and policies of the target state. The foreign entity can leverage relationships which were cultivated over time to persuade the target and intermediaries to act "in their self-interest in ways that advance the objectives" of the foreign entity.[11] This can take the form of:

[11] Jarol B. Manheim, Strategy in Information and Influence Campaigns: How Policy Advocates, Social Movements, Insurgent Groups, Corporation, Governments and Others Get What They Want. New York and London: Routledge, 2011, p. 95

- Covert funding or coercion, in order to negatively affect the target state, of
  - Politicians and political parties, government officials
  - Influential people and business groups
  - NGOs and activists
  - Academics and educational institutions
  - Civil unrest
  - Cyberattacks (e.g., "hack and leak" campaigns)[12]

- Hostile Information Campaigns, which are explained in greater detail further below.

2.2. "Soft power" and foreign Influence

"Soft power" is a form of foreign influence, which is the ability to shape the preferences of others through appeal and attraction, through non-coercive means like culture, political values, and foreign policies.[13] This can include:

- Public diplomacy, strategic communications,
- Foreign assistance, civic action,
- Economic reconstruction and development[14]
- Culture, film, TV, books, and other media (more details below)
- Economic ties, trade, business
- Open ties with educational institutions, think tanks

"Soft power" activities are generally accepted by states except where relationships that were built through such "soft power" activities are leveraged into foreign interference (as defined above).

[12] For instance, during the French presidential election campaign, data was hacked from then presidential candidate Emmanuel Macron's campaign and leaked online. See "Parliament: Foreign Countries Hit by Hostile Information Campaigns." *The Straits Times*, 13 February 2019, https://www.straitstimes.com/politics/foreign-countries-hit-by-hostile-information-campaigns.

[13] Joseph S. Nye, Soft Power: the Means to Success in World Politics (New York: Public Affairs, 2004).

[14] All the above from Robert M. Gates, US Secretary of Defense (November 26, 2007). (Speech). Landon Lecture (Kansas State University). Manhattan, Kansas https://web.archive.org/web/20100801065608/http://www.defense.gov/speeches/speech.aspx?speechid=1199

2.3. Information Operations

A significant part of "soft power" influence is built through information. Information operations use information in communications to persuade and shape the interests and attitudes of the target. Most states are tolerant towards influence spread through:

- Media syndication (e.g. foreign TV shows like Game of Thrones)
- Media ownership (e.g. foreign-owned TV channels like CNN, Fox News, CCTV), with some exceptions
- Open advertisement campaigns (e.g. advertisements by foreign entities in local newspapers)
- Op-eds where authorship is transparent and it is clear that they are opinions and not facts (e.g. commentaries written by foreigners and published in local newspapers)
- Public statements (e.g. by foreign officials)

On the other hand, states generally will not tolerate when another state, with hostile intent, takes actions (using information) to deliberately, covertly and deceptively disrupt the politics and policies of the target state, especially in a coordinated manner. These actions have been identified by Singapore as "hostile information campaigns" which are "used to weaken countries' resolve or destabilise nations during times of conflict"[15] and which "states must be able to tackle as issues of sovereignty and national security".[16] These include:

- Spreading disinformation or biased information in the target state
- Spreading narratives by traditional media (such as newspapers), through proxies, or under covert identities
- Carrying out the above activities using automated social media accounts (bots) or inauthentic social media accounts (trolls) to create coordinated campaigns, often disguised as local opinions.

[15] "Early Detection, Exposure Key to Tackling Foreign Interference in Domestic Politics: Shanmugam." *CNA*, 1 March 2019, https://www.channelnewsasia.com/news/singapore/early-detection-exposure-key-to-tackling-foreign-interference-in-11302762.

[16] Agil Haziq Mahmud, "Shanmugam Warns of Foreign Interference in Singapore; Questions Agenda, Funding of The Online Citizen." *CNA*, 25 September 2019, https://www.channelnewsasia.com/news/singapore/the-online-citizen-toc-foreign-interference-singapore-shanmugam-11940004.

The orchestrator of coordinated inauthentic behaviour may hide behind intermediaries, including "cyber troops", i.e., "government or political party actors tasked with manipulating public opinion online."[17] It is often hard to pinpoint cyber troops amidst ideologically motivated groups, "fringe movements," "hacker collectives," social media influencers and others, especially when states may directly or indirectly endorse their activities, and these intermediaries may operate concurrently when they are working for the same cause.[18]

Domestic entities also use cyber troops to engage in various acts including "micro-targeting"; "trolling" of opponents, journalists and others; leveraging "political bots" and so on.[19] According to Samantha Bradshaw and Philip Howard's study on "organised social media manipulation" around the globe, the number of countries accommodating "organized social manipulation campaigns" increased, from 28 in 2017 and 48 in 2018, to 70 in 2019. Each of them identified a political party or government agency capitalising on social media manipulation to shape the opinions of the domestic audience.[20] We note for instance, in Indonesia, "buzzers" and "micro-celebrities" were allegedly employed, by both Prabowo's and Widodo's opposing campaign teams, to run multiple fake accounts to share political narratives for their respective employers.[21]

Some of these strategies and tools are not all illegal in themselves; a marketing company may conduct micro-targeting to reach a particular audience group with product advertisements. The dangers arise when an entity, with hostile intent, takes actions (using information) to deliberately, covertly and deceptively disrupt politics and policies.

---

[17] Samantha Bradshaw and Philip N. Howard, "The Global Disinformation Order: 2019 Global Inventory of Organised Social Media Manipulation," *The Computational Propaganda Research Project*, (2019): 1, https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2019/09/CyberTroop-Report19.pdf

[18] Ibid,p. 9.

[19] Ibid, p 1.https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2019/09/CyberTroop-Report19.pdf

[20] Ibid, p. i.

[21] Fanny Potkin and Agustinus Beo Da Costa, "In Indonesia, Facebook and Twitter are 'buzzer' battlegrounds as elections loom," *Reuters*, 13 March 2019, https://www.reuters.com/article/us-indonesia-election-socialmedia-insigh/in-indonesia-facebook-and-twitter-are-buzzer-battlegrounds-as-elections-loom-idUSKBN1QU0AS

3. Foreign Interference Cases in Asia

With this framework in mind, we have broadly categorised the cases according to the tactics listed in the section above.

3.1. Covert funding / coercion of politicians, political parties, government officials, influential people, business groups, academics

We start with cases where Singapore has identified foreign entities as attempting to use Singaporeans as proxies to influence the domestic politics of Singapore.

- In 1987, Hank Hendrickson, who was the First Secretary (Political) in the US Embassy, cultivated several Singapore lawyers and urged them to "contest the elections against the government." He was subsequently removed from his position.

- In 2017, Prof Huang Jing was expelled from Singapore for using his former position at Singapore's Lee Kuan Yew School of Public Policy to advance the agenda of a foreign country.[22] He had engaged with foreign intelligence operatives and recruited others as he sought to influence the Singapore government's foreign policy and public opinion in Singapore. His actions were classified by the Ministry of Home Affairs of Singapore as "subversion and foreign interference".[23]

There are also instances where foreign diplomats have been accused of interfering in domestic politics, including stoking racial tensions. In Malaysia in 2015, Huang Huikang, then the Chinese Ambassador to Malaysia, told ethnic Chinese Malaysian citizens in Kuala Lumpur's Chinatown that China would "not sit idly by" when there "is infringement on China's national interests or violations of legal rights and interests of Chinese citizens and businesses".[24] The Chinese government subsequently apologised.[25]

---

[22] "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

[23] Leslie Schaffer, "Pro-Beijing professor expelled from Singapore for being 'agent' of foreign power", *CNBC*, 7 August 2017, https://www.cnbc.com/2017/08/07/pro-beijing-professor-expelled-from-singapore-for-being-agent-of-foreign-power.html. Huang Jing is currently a University Professor and Dean (Academic Affairs) of the Institute of International and Regional Studies at Beijing Language and Culture University (BLCU).

[24] Shannon Teoh And Eunice Au, "KL wants Chinese envoy to explain remarks", *The Straits Times*, 2 October 2015, https://www.straitstimes.com/asia/se-asia/kl-wants-chinese-envoy-to-explain-remarks

[25] "Ambassador's remarks stir controversy", *The Economist Intelligence Unit*, 1 October 2015, , http://country.eiu.com/article.aspx?articleid=273551011&Country=Malaysia&topic=Politics&subtopic=_1. This remark was made in the aftermath of a pro-Malay "red shirt" rally in September 2015, which was organised to counter a purported plot by ethnic Chinese to usurp political power from Malays. The situation escalated when Huang reiterated that China would always be the "maternal home" of the ethnic Chinese in Malaysia.

On the other hand, there are cases where foreign interference has been alleged but not conclusively proved:

- China has blamed foreign governments, including the US, for inciting the pro-democracy protests in Hong Kong.[26] Hong Kong media has accused the National Endowment for Democracy (NED), which they describe as "a CIA soft-power cut-out that has played a critical role in innumerable US regime-change operations" of funding groups involved in the protests.[27]

- Hong Kong business tycoon Jimmy Lai has also been accused of funding protests and of colluding with the US. South China Morning Post (SCMP) had previously reported in 2014 that Lai had funded the Occupy Central protests in Hong Kong and provided advice and propaganda material to them.[28]

In some cases, authorities have found circumstantial evidence, such as the conduct of persons who have received money from foreign sources, that leads them to believe that a foreign power has been attempting to interfere. In Australia, Labour Senator Sam Dastyari (who has since resigned) was found to have accepted Chinese funding for his political campaign and used money from alleged Chinese business interests to pay for his expenses and personal debts. Dastyari had warned Chinese billionaire Huang Xiangmo that the latter's phones were tapped by Australian intelligence agencies while Huang was a person of interest to the Australian government, and also provided Huang counter-surveillance advice.[29] Dastyari also defended China's position on the South China Sea, which contradicted his party's policy on the same issue. Then-Prime Minister Malcolm Turnbull criticised this is as "foreign policy for sale" or "cash for comment".[30]

---

[26] Danson Cheong, "Beijing Warns against Foreign Interference, Colour Revolutions." *The Straits Times*, 21 October 2019, https://www.straitstimes.com/asia/east-asia/beijing-warns-against-foreign-interference-colour-revolutions.

[27] "The Cost of the Hong Kong Protests: The Star Columnist." *The Straits Times*, 5 August 2019, https://www.straitstimes.com/asia/the-cost-of-the-hong-kong-protests-the-star-columnist.

[28] ibid

[29] Nick McKenzie, James Massola and Richard Baker, "Labor senator Sam Dastyari warned wealthy Chinese donor Huang Xiangmo his phone was bugged", *The Sydney Morning Herald*, 29 November 2017, https://www.smh.com.au/politics/federal/labor-senator-sam-dastyari-warned-wealthy-chinese-donor-huang-xiangmo-his-phone-was-bugged-20171128-gzu14c.html

[30] Quentin McDermott, "Sam Dastyari defended China's policy in South China Sea in defiance of Labor policy, Covert recording reveals", *Australian Broadcasting Corporation*, 29 November 2017, https://www.abc.net.au/news/2017-11-29/sam-dastyari-secret-south-china-sea-recordings/9198044

3.2. Covert funding of NGOs

States have also long suspected aggressors of using NGO's and multilateral institutions to destabilise them,[31] while some have actually used NGO's to carry out actions like espionage.[32] NGO's come under most suspicion when it is discovered that they are not truly "non-governmental" but actually linked to foreign governments. The Australian Council for the Promotion of the Peaceful Reunification of China (ACPPRC), established in 2015, claimed to be an NGO. Investigations later revealed that it was linked to the United Front Work Department, an agency of the Communist Party of China, whose primary purpose is to conduct influence activities overseas.[33] The Australian Security Intelligence Organization (ASIO) cancelled the permanent residency of ACPPRC's Chairman, Huang Xiangmo, on grounds that he was "amenable to conducting acts of foreign interference" and had shown a willingness to do so in the past.[34]

3.3. Covert funding of educational institutions

Educational institutions are also at risk of foreign interference, because they can shape domestic public discourse as well as students' thinking on political issues. While collaborations between educational institutions are usually welcomed, others have come under suspicion. Confucius Institutes, funded by the Ministry of Education of China, have become the de facto Chinese studies programmes in some Australian universities, and while they do not actively push a party line, they are accused of restraining debate about China by steering discussion away from sensitive subjects. Chinese Students and Scholars Association (CSSA), funded by Chinese embassies, offer assistance to Chinese students on foreign campuses, but are also accused of monitoring and reporting students who take part in activities seen as hostile to the party.[35]

---

[31] Russia accuses the US of doing this, Jānis Bērziņš, "Russian New Generation Warfare is not Hybrid Warfare", in (eds.) Artis Pabriks and Andis Kudors (Riga: The Center for East European Policy Studies, University of Latvia Press, 2015) , accessed http://appc.lv/eng/wp-content/uploads/sites/2/2015/05/gramata-ar-vaku.pdf#page=41

[32] Tsvetelia Tsolova, "Bulgarian NGO official charged with spying for Russia", *Reuters*, 10 September 2019, https://www.reuters.com/article/us-bulgaria-russia-espionage/bulgarian-ngo-official-charged-with-spying-for-russia-idUSKCN1VV1W7

[33] Nick McKenzie and Chris Uhlmann, "'A man of many dimensions': the big Chinese donor now in Canberra's sights", *The Sydney Morning Herald*, 6 February 2019, https://www.smh.com.au/politics/federal/a-man-of-many-dimensions-the-big-chinese-donor-now-in-canberra-s-sights-20190206-p50vzt.html

[34] Grant Wyeth. "Why Did Australia Push Out a Chinese Communist Party-Linked Billionaire?" *The Diplomat*, 12 February 2019, https://thediplomat.com/2019/02/why-did-australia-push-out-a-chinese-communist-party-linked-billionaire/.

[35] "How China's "sharp power" is muting criticism abroad", 14 December 2017, *The Economist*, https://www.economist.com/briefing/2017/12/14/how-chinas-sharp-power-is-muting-criticism-abroad

3.4. Covert funding of media

The ability to influence domestic public opinion is a key reason for foreign entities to fund media outlets. Different states have different restrictions on foreign investment in their domestic media, as this investment can often be financially beneficial. However, covert funding is usually not acceptable.

- In 1964, Aw Kow, a prominent Singaporean businessman, received a substantial loan from high-ranking officials of a Communist intelligence service based in Hong Kong, to establish "the Eastern Sun", an English language daily newspaper in Singapore. In return for this loan, he agreed that the paper would follow principles laid down by the foreign state, in their long term political objective of gaining control of the press in Singapore.[36] Aw admitted it was true and the paper closed down as the editorial staff resigned.[37]

- In 1971, Singapore expelled three foreign journalists working for the newspaper The Singapore Herald[38] and revoked its license. One of the paper's primary investors was Donald Stephens, then Malaysian high commissioner to Australia. The paper was accused of spreading misinformation to work up feelings against Singapore's national service policy.[39]

- In 2015, Reuters reported that China Radio International (a subsidiary of the Chinese government but hidden by front companies) was covertly backing at least 33 radio stations in 14 countries, including Australia and Thailand, to form a global network broadcasting positive news about China.[40]

---

[36] Singapore Government Statement." *National Archives of Singapore*, 15 May 1971. http://www.nas.gov.sg/archivesonline/data/pdfdoc/SGPress_3_15.5.71.pdf

[37] "3 Local Newspapers Spread Misinformation under 'Black Operations' & Were Taken to Task in 1971." Mothership.sg, https://mothership.sg/2018/01/1971-fake-news-black-operations/.

[38] "Singapore Expelling 3 Foreign Newsmen." *The New York Times*, 18 May 1971, https://www.nytimes.com/1971/05/18/archives/singapore-expelling-3-foreign-newsmen.html.

[39] "3 Local Newspapers Spread Misinformation under 'Black Operations' & Were Taken to Task in 1971." *Mothership*.sg.

[40] Louisa Lim and Julia Bergin, "Inside China's audacious global propaganda campaign," *The Guardian*, 7 December 2018, https://www.theguardian.com/news/2018/dec/07/china-plan-for-global-media-dominance-propaganda-xi-jinping

3.5. Cyberattacks

Cyberattacks are another tactic for aggressors to deliberately, covertly and deceptively disrupt the politics and policies of the target state.

- One direct way is to tamper with electronic voting results. Electronic voting systems are particularly vulnerable to cyberattack. Hackers at the Voting Village section of the annual Defcon security conference have demonstrated numerous ways to breach voting machines and tamper with results.[41] Even the suspicion of breach and falsified results, proven or otherwise, can cast doubt on an election's integrity.

- A less direct way is to use cyberattacks to erode the confidence of citizens in their state. This could be a major cyberattack, such as the takedown of power utilities in the Ukraine, or more insidiously could be a "low-level but nonetheless persistent and insidious cyber effort to chip away at the resilience of our people"; "slow burn issues" which sap the will of the people.[42]

- Cyberattacks can also be used in combination with information operations, called "hack and leak" operations, where a foreign state breaches sensitive databases in the target state and exposes sensitive and embarrassing information. One recent example was foreign actors who tried to interfere with the 2017 French presidential election, by hacking data from (then presidential candidate) Emmanuel Macron's campaign and leaking it online, reaching 47,000 tweets in 3 hours, with the help of automated accounts.[43]

---

[41] Taylor Telford, "Hackers Were Told to Break into U.S. Voting Machines. They Didn't Have Much Trouble." *The Washington Post*, 13 Aug. 2019, https://www.washingtonpost.com/business/2019/08/12/def-con-hackers-lawmakers-came-together-tackle-holes-election-security/. Many of the voting machines are still used in elections across the United States, despite having well-known vulnerabilities that have not been patched by their manufacturers to date.

[42] Shashi Jayakumar, "Commentary: Beware the Slow-Burn Threats to Singapore." *CNA*, 9 March 2017, https://www.channelnewsasia.com/news/singapore/commentary-beware-the-slow-burn-threats-to-singapore-7629738.

[43] "Parliament: Foreign Countries Hit by Hostile Information Campaigns." *The Straits Times*, 13 February 2019, https://www.straitstimes.com/politics/foreign-countries-hit-by-hostile-information-campaigns.

3.6. Hostile Information Campaigns

Last but not least, states are justifiably concerned that modern technologies have "turbo-charged" foreign interference, enabling "hostile information campaigns" to stoke protests, deepen divisions, increase hostility, and sow distrust in institutions.[44] Singapore's parliamentary Select Committee on Deliberate Online Falsehoods reported in its findings that Singapore "has been and will continue to be a target of hostile information campaigns" which attack Singapore's national security, racial harmony, democratic processes, social cohesion and trust in public institutions.

Hostile information campaigns are not limited to spreading disinformation. They can consist of coordinated behaviour from a large number of inauthentic accounts (either automated or manually controlled) to create the illusion that there is widespread public sentiment, or to provoke divisive issues. They can be an insidious way to influence large segments of the population without them being aware.[45] It can be difficult for the public to distinguish this from genuine (and essential) domestic discourse on sensitive issues like race, religion, and politics.

- In 2018, at the peak of Singapore's dispute with Malaysia over maritime and airspace issues, the Singapore government observed a "curious" spike in online comments critical of Singapore on social media, and that these posts were made using anonymous accounts.[46]

- In Taiwan, the National Security Bureau briefed the Legislative Yuan's Foreign Affairs and National Defense Committee in 2018 that China was "behind a propaganda campaign to interfere with Taiwan's elections by creating disinformation and fake news targeting Taiwanese media outlets, radio and television programs and Web sites."[47] Sources also said that Chinese teams spread "divisive commentary" into Taiwanese social media sphere on sensitive topics with the aim of creating social conflict.[48]

---

[44] Prashanth Parameswaran, "Singapore's Foreign Interference Challenge in the Spotlight," *The Diplomat*, 1 October 2019, https://thediplomat.com/2019/10/singapores-foreign-interference-challenge-in-the-spotlight.

[45] Olivia Ho, "Be Vigilant about Foreign Interference: Jayakumar." *The Straits Times*, 26 September 2019, https://www.straitstimes.com/singapore/be-vigilant-about-foreign-interference-jayakumar.

[46] Adrian Lim, "Parliament: 'Curious' spike in online comments critical of S'pore during dispute with Malaysia, says Edwin Tong." *The Straits Times*, 12 February 2019. https://www.straitstimes.com/politics/parliament-curious-spike-in-online-comments-critical-of-spore-during-dispute-with-malaysia

[47] Chung Li-hua and William Hetherington, "China targets polls with fake accounts", *Taipei Times*, 5 November 2018, http://www.taipeitimes.com/News/front/archives/2018/11/05/2003703618 .

[48] Ibid.

- North Korea is accused of using inauthentic social media accounts (trolls) to stir discussions on wedge issues on South Korea's platforms. This is sometimes masked with stolen accounts of legitimate South Korean users to give the impression of authenticity.[49]

The large social media platforms have identified and attempted to take action against this.

- Facebook announced in early 2019 that it took down accounts with "coordinated inauthentic behaviour" on Facebook and Instagram that were orchestrated from Iran,[50] and removed accounts linked to an Israeli commercial entity, Archimedes Group[51]. Some of these fake accounts had mounted actions targeting Southeast Asia.[52]

- Facebook also took down multiple "Facebook and Instagram assets" some of which were traced to an individual in Thailand linked to a "Russian government-funded journal based in Moscow."[53] The fake accounts managed Pages, boosted "engagement," "creat[ed] fake personas," directed people to blogs claiming to be news outlets, and spread "divisive narratives and comments" concerning "Thai politics, geopolitical issues…, protests in Hong Kong, and criticism of democracy activists in Thailand."[54]

[49] Leo Benedictus, "Invasion of the troll armies: from Russian Trump supporters to Turkish state stooges," *The Guardian*, 6 November 2019, https://www.theguardian.com/media/2016/nov/06/troll-armies-social-media-trump-russian

[50] Nathaniel Gleicer, "Removing Coordinated Inauthentic Behavior From Iran," *Facebook Newsroom*, 31 January 2019, https://newsroom.fb.com/news/2019/01/removing-cib-iran/. Indonesia was one of the countries where the activities of these accounts were observed.

[51] Ibid.

[52] Nathaniel Gleicher, "Removing Coordinated Inauthentic Behavior From Israel," *Facebook Newsroom*, 16 May 2019, https://newsroom.fb.com/news/2019/05/removing-coordinated-inauthentic-behavior-from-israel/. The fake accounts faked ownership by locals and local news organisations; claimed to share leaked information about politicians, disseminated political news and critiques, and tried to boost engagement artificially.

[53] Lain Robertson, Kanishk Karan, and Ayushman Kaul, "Facebook Takes Down Inauthentic Pages with Connections to Thailand," *DFRLab at Medium*, 26 July 2019, https://medium.com/dfrlab/facebook-takes-down-inauthentic-pages-with-connections-to-thailand-7dbf331f5ba5.

[54] Ibid.

These challenges are immense as hostile information campaigns can proliferate on multiple platforms. Several Australian sources, including the International Cyber Policy [Centre],[55] a constituent of the Australian Strategic Policy Institute, have raised concerns about the potential use of WeChat for "disinformation, censorship and propaganda"[56] in the run-up to the Australian elections.[57] This is particularly important given the number of Mandarin speakers in the country "expect[ing] to receive most of their information about the parties' policies via WeChat."[58]

[55] While the cited article refers to the organisation as International Cyber Policy Institute, it is called International Cyber Policy Centre on ASPI's webpage.

[56] Max Koslowski, "Warning WeChat could spread Chinese propaganda during federal election," *The Sydney Morning Herald*, 28 January 2019, https://www.smh.com.au/politics/federal/warning-wechat-could-spread-chinese-propaganda-during-federal-election-20190118-p50s90.html.

[57] John Power and Meaghan Tobin, "Fears of China and WeChat as Australia heads to the polls," *South China Morning Post*, 16 May 2019, https://www.scmp.com/week-asia/politics/article/3010216/fears-china-and-wechat-australia-heads-polls.

[58] Ibid.

4. Conclusion

There is a spectrum of activity across Asia which foreign entities (states and non-state actors) will seek to undertake in domestic issues, to promote their national, commercial, or ideological interests.

Foreign influence is not bad in itself: all nations, including Singapore, commonly make efforts to influence important issues and policies overseas to benefit their own interests. On one end, there are open, lawful and transparent actions that are often accepted or tolerated by domestic governments in the interests of building international relationships, trade, business, and other strategic reasons. On the other end, foreign interference – deliberate, covert and deceptive actions which disrupt the politics and policies of the target state – is not accepted or tolerated, because foreign interference infringes on the sovereignty of the target and is detrimental to its national security and economy.

In between these two extremes are many cases which may look like one but turn out to be the other. Characterising too many activities as "foreign interference" can damage state to state relationships, harm trade and business, or even lead citizens to (mis)interpret their government's actions as restricting freedom of speech and expression – which in itself can cause division.

On the other hand, taking too lax an approach (e.g., not banning foreign donations to political parties) can give foreign entities too much leeway to disrupt the domestic polity. States therefore need to clearly define the red lines that foreign entities must not cross in domestic politics, for the foreign entities as well as domestic citizens to be aware. These red lines will vary from state to state depending on political culture and social conditions, especially in the Asian context. When these red lines are defined, the state can then take steps to monitor and prevent them from being crossed and prepare countermeasures for when foreign interference occurs.

About the Authors

Muhammad Faizal is a Research Fellow with the Centre of Excellence for National Security (CENS) at the S. Rajaratnam School of International Studies (RSIS). He holds a Bachelor of Business Administration (with Merit) from the National University of Singapore. He completed his Master of Science in Strategic Studies at RSIS, specialising in terrorism studies. His dissertation examined the grand strategies of Al Qaeda and the Islamic State (Daesh), focussing on asymmetric warfare and cities as a jihadi battlespace. Prior to joining RSIS, Faizal served with the Singapore Ministry of Home Affairs where he was a Deputy Director and had facilitated international engagements with foreign security counterparts. He also had postings in the Singapore Police Force where he supervised and performed intelligence analysis, achieving several commendation awards including the Minister for Home Affairs National Day Award (2009) for operational and analysis efficiency; and in the National Security Research Centre (NSRC) at the National Security Coordination Secretariat (NSCS), where he led a team to research emergent trends in domestic security and monitor terrorism-related developments. Faizal also has certifications in Counter-Terrorism, Crime Prevention and Business Continuity Planning.

Faizal is also a regular resource person for international media such as MediaCorp on issues of extremism, terrorism and homeland security; and given lectures at conferences such as the Stockholm Security Conference 2017 and Security Industry Conference (SIC) 2018.

Gulizar Haciyakupoglu is a Research Fellow at the Centre of Excellence for National Security (CENS), S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University (NTU). Her research explores deliberate attempts of manipulation in information space, influence operations, and trust investment and activism in online platforms. Her recent publications appeared in various academic and policy outlets, including the Journal of Computer Mediated Communication, Defence Strategic Communications, The Diplomat, and The Interpreter. She holds a Ph.D. with Lee Kong Chian scholarship from the National University of Singapore (NUS), Communications and New Media Department (CNM), and an MA in Political Communication from the University of Sheffield. She received her bachelor's degree in Global and International Affairs from the Dual-Diploma Programme of the State University of New York (SUNY) Binghamton, and Bogazici University, Turkey.

Benjamin Ang is a Senior Fellow in the Centre of Excellence for National Security (CENS) at RSIS. He leads the Cyber and Homeland Defence Programme of CENS, which explores policy issues around the cyber domain, international cyber norms, cyber threats and conflict, strategic communications and disinformation, law enforcement technology and cybercrime, smart city cyber issues, and national security issues in disruptive technology.

Prior to this, he had a multi-faceted career that included time as a litigation lawyer arguing commercial cases, IT Director and General Manager of a major Singapore law firm, corporate lawyer specialising in technology law and intellectual property issues, in house legal counsel in an international software company, Director-Asia in a regional technology consulting firm, in-house legal counsel in a transmedia company, and senior law lecturer at a local Polytechnic, specialising in data privacy, digital forensics, and computer misuse and cybersecurity.

Benjamin graduated from Law School at the National University of Singapore and has an MBA and MS-MIS (Masters of Science in Management Information Systems) from Boston University. He is qualified as an Advocate and Solicitor of the Supreme Court of Singapore, and was a Certified Novell Network Administrator back in the day. He also serves on the Executive Committee of the Internet Society Singapore Chapter.

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.

Jennifer Yang Hui is an Associate Research Fellow at the Centre of Excellence for National Security (CENS), a constituent unit of the S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University (NTU). Jennifer has an Honours degree in History from the National University of Singapore (NUS). In 2010, she graduated as a Tun Dato Sir Cheng Lock Tan Master of Arts (M.A.) scholar in Southeast Asian Studies, also from NUS. Prior to joining CENS, Jennifer had worked at the National Archives of Singapore and the Institute of South East Asian Studies (ISEAS). In CENS, Jennifer researches on the evolution and

weaponisation of social media and technology by individuals and movements. Her other research interests are: ethno-religious relations and the role of the social media in contemporary Indonesia; epistemology, knowledge-making and their implications on digital maturity. Jennifer is currently examining digital manipulation campaign and electoral politics in Indonesia.

Teo Yi-Ling is a Senior Fellow with the Centre of Excellence for National Security (CENS) at RSIS. She is part of the Cyber and Homeland Defence Programme of CENS, engaged with exploring policy, legal, and regulatory issues around the cyber domain including international cyber norms, threats and conflict, crime and law enforcement technologies, and smart city issues; strategic communications and disinformation, and national security issues in disruptive technology.

A qualified Barrister-at-Law (England & Wales) and an Advocate & Solicitor (Singapore), Yi-Ling has practice experience with international and local law firms in the areas of intellectual property, technology, media and entertainment, and commercial law. Her clients included production companies, technology and innovation companies, creative agencies, and government and regulatory agencies. In her capacity as Senior Faculty and Principal Legal Counsel for the IP Academy at the Intellectual Property Office of Singapore (IPOS), she led the team that developed and launched a postgraduate degree programme in IP management, and a specialist certificate programme in intangible asset management.

Yi-Ling holds an LL.B. (Hons) from the University of Liverpool, and an LL.M. (cum laude) from Northwestern University School of Law in Chicago. She is the author of “Media Law in Singapore”, published by Sweet & Maxwell; a pioneering and definitive text examining the development of media and communication-related laws in Singapore, alongside the practical management of media issues. Her book is used as a course and reference text by most media-related diploma, degree and postgraduate programmes in Singapore tertiary institutions. She has extensive academic experience, having developed and taught courses in media law, intellectual property law, entertainment business transactions, and media ethics at a number of tertiary institutions in Singapore, and in the U.S., Dutch, and Australian university systems.

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