COUNTERMEASURES AGAINST FOREIGN INTERFERENCE

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

Policy Report
April 2020

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

NANYANG TECHNOLOGICAL UNIVERSITY
SINGAPORE

Policy Report

COUNTERMEASURES AGAINST FOREIGN INTERFERENCE

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

April 2020

Table of Contents

Executive Summary

This paper takes reference from and builds upon our prior report “Cases of Foreign Interference in Asia”. In that report, we had proposed a framework for understanding the relationship between foreign interference, foreign influence, and hostile information campaigns. We had also proposed a definition of foreign interference as occurring when a foreign entity (state or non-state actor described as the “Adversary”), with hostile intent, takes actions to deliberately, covertly and deceptively disrupt the politics and policies of the Defender state (the “Defender”). We then described the forms in which such foreign interference has been observed to take, and the respective tactics employed.

This paper continues this trajectory of analysis by proposing a framework of countermeasure responses to the identified tactics in the following order: understanding the Adversary’s objectives; assessing the Defender’s vulnerabilities; setting clear goals for the countermeasures; setting up a task force for strategic responses; and countering specific tactics where necessary.

We note that in the assessment phase, the Defender must be alert to multi-faceted attacks, but must also be careful not to confuse a foreign entity’s legitimate activity for foreign interference.

For each aspect of this framework response, we propose and discuss the relevant strategic factors that should be considered, and provide examples of countermeasures deployed by other states.

We conclude by observing that an effective response against the threat of foreign interference needs to take the form of an integrated and strategic approach of focusing on the strategic factors outlined, and the design and implementation of practical and active countermeasures.

1. Foreign Interference

In our prior report Cases of Foreign Interference in Asia, we proposed a framework (in Figure 1 below) for understanding the relationship between foreign interference, foreign influence, and hostile information campaigns below. This framework was proposed 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.

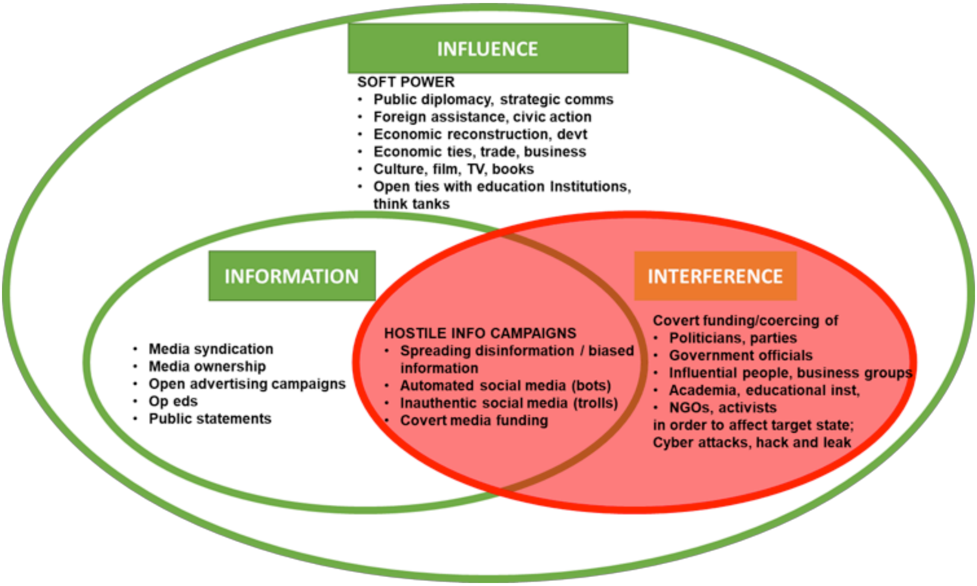
INFLUENCE
SOFT POWER
• Public diplomacy, strategic comms
• Foreign assistance, civic action
• Economic reconstruction, devt
• Economic ties, trade, business
• Culture, film, TV, books
• Open ties with education Institutions, think tanks
INFORMATION
• Media syndication
• Media ownership
• Open advertising campaigns
• Op eds
• Public statements
HOSTILE INFO CAMPAIGNS
• Spreading disinformation / biased information
• Automated social media (bots)
• Inauthentic social media (trolls)
• Covert media funding
INTERFERENCE
Covert funding/coercing of
• Politicians, parties
• Government officials
• Influential people, business groups
• Academia, educational inst,
• NGOs, activists
in order to affect target state;
Cyber attacks, hack and leak

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

We also defined foreign interference as occurring when a foreign entity (state or non-state actor, which we hereafter refer to as “**the Adversary**”), with **hostile intent**, **takes actions** to **deliberately**, **covertly** and **deceptively disrupt** the politics and policies of the Defender state (“the **Defender**”). This can be:

1. Covert funding or coercion, in order to negatively affect the Defender state, of
    1.1. Politicians and political parties, government officials
    1.2. Influential people and business groups
    1.3. NGOs and activists
    1.4. Academics and educational institutions
    1.5. Civil unrest

2. Cyberattacks (e.g., “hack and leak” campaigns)[1]

3. Hostile Information Campaigns, including
    3.1. Spreading disinformation or biased information in the Defender state
    3.2. Spreading narratives by traditional media (such as newspapers), through proxies, or under covert identities
    3.3. 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.

[1] 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.

2. Framework for Countermeasures

Since the Adversary can engage in a coordinated campaign using any number of the tactics listed above, it would not be effective to deal with any of them piecemeal. We instead propose dealing with foreign interference campaigns strategically, using the following framework for countermeasures:

(1) Understand the Adversary's objectives
(2) Assess the Defender's vulnerabilities
(3) Set clear goals for the countermeasures
(4) Set up a task force for strategic response
(5) Counter specific tactics where needed

2.1. Understand the Adversary's objectives

To determine why the Adversary might want to interfere in the Defender's domestic affairs, it is necessary to appreciate how the Adversary perceives the world and wants to change it. External influences include shifts in the distribution of geopolitical power, and internal influences include domestic politics, public opinion, and agendas of interest groups (e.g., businesses). The Adversary's worldview also determines how it uses its national power — diplomatic, informational, military and economic — and takes risks to grow its influence and interfere overseas. For example, experts believe that prolonged economic stagnation drives Russia to prioritise the use of its military power to gain control over foreign lands, such as Crimea, in restoring what it views as its former sphere of influence, whereas China views the economy as the foundation for its global rise and therefore, prioritises the use of its economic power first — in the shape of the Belt and Road Initiative — to influence access to markets and natural resources.[2]

By appreciating the Adversary's worldview, the Defender can better determine what the foreign state regards as significant risks to be avoided and significant gains to be made. The Defender can use this to develop denial countermeasures to disrupt the foreign interference.[3]

[2] Huotari, Mikko, et al. "China's Emergence as a Global Security Actor." Mercator Institute for China Studies, https://www.merics.org/en/papers-on-china/chinas-emergence-global-security-actor-1.

[3] Muhammad Faizal Abdul Rahman. "Strategizing Countermeasures Against Foreign Interference in Singapore – Analysis." Eurasia Review, 5 October 2019, https://www.eurasiareview.com/05102019-strategizing-countermeasures-against-foreign-interference-in-singapore-analysis/.

The Defender will need to use its intelligence gathering apparatus internally, such as cultivating human intelligence assets (HUMINT) in critical public and private institutions, and social and business organisations where foreign involvement or interests are high. This will also help gather evidence if legal countermeasures are needed. The Defender may also need to invest resources externally in growing its influence in and collecting more intelligence on other states for forward defence.[4]

The Defender should then fuse internal and external intelligence for comprehensive threat assessment, including five important elements:[5]

(a) the interests and perceptions of the foreign state actor;
(b) the interests and vulnerabilities of the Defender;
(c) the interests and vulnerabilities of the intermediaries;
(d) how the domestic context of the Defender state features in the broader geopolitical environment; and
(e) the possible desired outcomes of the foreign state actor.[6]

During this phase, the framework that we propose in Figure 1 is particularly important: The Defender should be alert to the multi-faceted nature of the threat, but should also not mistake a foreign entity's legitimate activity for foreign interference. The risk of witch-hunting, or seeing foreign agents around every corner, is in creating a self-destructive national paranoia that can damage international relations and trade, to the detriment of the Defender's own economy and development.[7]

2.2. Assess the Defender's vulnerabilities and strengths

The Defender should also map the relationships between parties that have stakes or influence in its 4Is: Infrastructure and Information that constitute the foundations of national sovereignty, and Ideas and Individuals that define national identity and policies.[8] For example, one central idea for Singapore is multi-racial, multi-cultural, multi-religious harmony.

[4] Forward defence policy encompasses pre-empting external threats before they reach the borders of the state and building trust and friendships with foreign states. This policy requires the state having the capability to project its influence overseas.

[5] Muhammad Faizal Abdul Rahman. "Strategizing Countermeasures Against Foreign Interference in Singapore – Analysis." Eurasia Review, 5 October 2019, https://www.eurasiareview.com/05102019-strategizing-countermeasures-against-foreign-interference-in-singapore-analysis/.

[6] Manheim, Jarol B. *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, pp. 22 – 23 and 185

[7] Kofman, Michael. "Russian Hybrid Warfare and Other Dark Arts." *War on the Rocks*, 11 March 2016, https://warontherocks.com/2016/03/russian-hybrid-warfare-and-other-dark-arts/.

[8] Rahman, "Strategizing Countermeasures Against Foreign Interference in Singapore – Analysis."

One example of such mapping is the Vulnerability Index of Central European countries.[9] On the one hand, these parties — such as key personnel, suppliers, political and community figures — are in the right position to detect and defend the Defender state's 4Is from foreign interference. On the other hand, these parties are also in a position to act as agents of influence for a foreign state. These maps are therefore useful for (i) investigating the scope, scale, and sophistication of foreign interference when it happens, (ii) developing programmes to raise awareness in these parties of the potential risks of foreign interference, and (iii) cultivating partners, such as from community organisations and private sector, to counter foreign interference.

2.3. Set clear goals for the countermeasures

At the strategic level, the Defender should set clear goals for foreign interference countermeasures, which can include broad categories such as (i) deterrence by punishment, and/or (ii) deterrence by denial of goals.

Smaller states (like Singapore) have limited ability to deter larger / more powerful states by punishment through hard power — military, economic or cyber. The global interdependence of people, economies, and technologies, makes retaliation complicated and risky for smaller states. Smaller states can leverage their unique strengths instead, such as using strong laws to expel an agent of foreign influence, Singapore did to Professor Huang Jing in 2017.[10] His actions were classified by the Ministry of Home Affairs of Singapore[11] as "subversion and foreign interference".[12] Such expulsions would disrupt the relationships that the Adversary has invested time and resources to build, reduce the effectiveness of foreign interference, and hopefully send a deterrent message to the Adversary.

[9] Political Capital, Vulnerability Index, 11 April 2017, https://politicalcapital.hu/news.php?article_read=1&article_id=628

[10] Huang Jing leveraged his former position at the Lee Kuan Yew School of Public Policy to advance the agenda of a foreign country. He engaged with foreign intelligence operatives and recruited others as he sought to influence the Singapore government's foreign policy and public opinion in Singapore. See Leslie Schaffer, "Pro-Beijing professor expelled from Singapore for being 'agent' of foreign power", 7 August 2017, *CNBC*, https://www.cnbc.com/2017/08/07/pro-beijing-professor-expelled-from-singapore-for-being-agent-of-foreign-power.html.

[11] "In full: MHA's statement on revoking PR status of academic Huang Jing and wife", 4 August 2019, *TODAY*, https://www.todayonline.com/singapore/ministry-home-affairs-full-statement-huang-jing

[12] Leslie Schaffer, "Pro-Beijing professor expelled from Singapore for being 'agent' of foreign power", 7 August 2019, *CNBC*, https://www.cnbc.com/2017/08/07/pro-beijing-professor-expelled-from-singapore-for-being-agent-of-foreign-power.html

“Small, frontline states do not, however, lack options in the face of coercion. To the contrary, they could pursue a number of competitive strategies in an effort to make coercion less attractive. These include strategies of denial, which seek to harden a state against coercion; cost-imposing strategies, which seek to force an adversary to bear burdens sufficient to cause a reconsideration of coercion; efforts to attack and render ineffective the adversary’s coercive strategy; and strategies that seek to exploit divisions within the enemy’s political leadership to end the coercive campaign.”[13]

2.4. Set up a task force to respond strategically

Since this work crosses different sectors – intelligence, foreign affairs, home affairs, communications – several countries have established cross-cutting task forces or government divisions tasked with responding to different aspects of the problem. They have different focuses in different countries, including media monitoring, election safeguarding, and exploration of the broader threat framework.

- Australia founded the Electoral Integrity Assurance Taskforce to safeguard elections from cyberattacks and interference.[14]
- Denmark’s intergovernmental task force attends to election integrity as part of the broader framework of influence campaigns. The intergovernmental taskforce seeks to bolster the coordination and power of concerned authorities in fighting influence operations, including election interference.[15]
- Sweden’s efforts are coordinated by the Swedish Civil Contingencies Agency (MSB), which is regarded as one of the world’s most effective organisations in building public awareness about influence operations and responding to them. Sweden is also establishing a psychological defence unit to counter disinformation and maintain public morale in crisis periods.[16]

[13] Thomas G. Manken, “Small States Have Options Too: Competitive Strategies Against Aggressors”, 27 January 2016, *War On The Rocks*, https://warontherocks.com/2016/01/small-states-have-options-too-competitive-strategies-against-aggressors/

[14] “Electoral integrity: 2019 federal election,” *Australian Electoral Commission*, 12 April 2019, https://www.aec.gov.au/elections/electoral-advertising/electoral-integrity.htm. See Also Will Ziebell, “Australia forms task force to guard elections from cyber attacks,” *Reuters*, 9 June 2018, https://www.reuters.com/article/us-australia-security-elections/australia-forms-task-force-to-guard-elections-from-cyber-attacks-idUSKCN1J506D

[15] “Strengthened safeguards against foreign influence on Danish elections and democracy,” *Ministry of Foreign Affairs of Denmark*, https://um.dk/en/news/NewsDisplayPage/?newsID=1DF5ADBB-D1DF-402B-B9AC-57FD4485FFA4

[16] “What the United States Can Learn from Europe on Fighting Cyberattacks and Disinformation.” *Atlantic Council*, 10 December 2019, https://atlanticcouncil.org/blogs/new-atlanticist/what-the-united-states-can-learn-from-europe-on-fighting-cyberattacks-and-disinformation/.

Such task forces or agencies are needed to coordinate a whole-of-government approach and comprehensive countermeasures across different government agencies. We have identified three good practices:

Firstly, the agency should embark on broad research to examine all government agencies for functional areas and issues that may be potential vulnerabilities that hostile foreign states can exploit, especially those that oversee critical national infrastructure as well as critical industries. Additionally, the coordination agency should also assess whether the various agencies have roles and capabilities that can contribute to the overall endeavour of countering foreign interference. The coordination body should have the capability to respond to ongoing potential threats and vulnerabilities, not just during election periods. This capability would include an integrated function of facilitating intelligence sharing and analysis. For example, the Czech Republic established the Centre Against Terrorism and Hybrid Threats in 2017 and "house[ed]" it under the Ministry of Interior. The organisation is concerned with a wide range of security threats, including terrorism, extremism, and foreign disinformation campaigns.[17] Since its inauguration, the organisation has attracted criticism for allegedly "duplicat[ing] [the] work [of] the Ministry of Interior and others," and insufficiency of its output.[18]

Secondly, the agency should identify and monitor foreign states and actors that may be involved in foreign influence and interference operation. This requires a fusion of analysis in international relations, geostrategic ambitions, strategic coercion and internal security. The agency should then (i) identify its intelligence collection and analysis requirements, (ii) establish well-defined procedures for various agencies to report suspected attempts of foreign interference, (iii) and collaborate with local and international security research institutes. Countries who have enacted legislation to support this are the US' Foreign Agents Registration Act (FARA), and the Australian Foreign Influence Transparency Scheme (FITS) under the Foreign Influence Transparency Act 2018 (FITA).

Thirdly, the agency should embark on broad research to identify entities both in the private and non-governmental sectors that may become targets of foreign influence and foreign interference operations. The agency should then establish partnerships, information sharing and liaison channels with these entities, and enlist their support.

[17] "Centre Against Terrorism and Hybrid Threats," *Ministerstvo Vnitra Ceske Republiky*, https://www.mvcr.cz/cthh/clanek/centre-against-terrorism-and-hybrid-threats.aspx

[18] Michael Colborne, "The Brief Life, and Looming Death, of Europe's 'SWAT Team for Truth'," *Foreign Policy*, 20 September 2017, https://foreignpolicy.com/2017/09/20/the-brief-life-and-looming-death-of-europes-swat-team-for-truth-fake-news/

2.5. Counter specific tactics where needed

With all of the above in place, the Defender should be able to counter specific tactics where needed, in a strategic and holistic way.

2.5.1. Countering covert funding / coercion of politicians, political parties, government officials, influential people, business groups, academics

Public coverage: Attempts to penetrate foreign influence through covert funding of politicians, political parties, government officials, influential people, businesspeople, and academics have received attention in the media in recent years. The coverage of such incidents by mainstream outlets is essential not only for raising public awareness on the issue but also to publicly condemn such acts.

Legislation: Some states follow up by introducing legislation. For instance, amidst growing concerns about potential foreign interference and plans to hold elections late 2020, New Zealand announced its plan to ban "foreign donations to politicians and tighten disclosure rules for political advertising."[19] Australia, on the other hand, passed a bill on "electoral funding and disclosure" to prevent foreign donations and revise the threshold for disclosing political donations,[20] after Senator Sam Dastyari stepped down because of financial engagements that raised concerns about Chinese influence.[21] The espionage and foreign interference bill introduces new offences for spying, sabotage, and theft of trade secrets on behalf of a foreign government, while the foreign influence transparency scheme bill will create a register for individuals or entities undertaking activities on behalf of "foreign principals".[22] Including communications activities.

[19] Eleanor Ainge Roy, "New Zealand bans foreign political donations amid interference concerns," *The Guardian*, 3 December 2019, https://www.theguardian.com/world/2019/dec/03/new-zealand-bans-foreign-political-donations-amid-interference-concerns.

[20] Paul Karp, "Coalition bill to ban foreign political donations passes Senate," *The Guardian*, 15 November 2018, https://www.theguardian.com/australia-news/2018/nov/15/coalition-bill-to-ban-foreign-political-donations-passes-senate.

[21] "'Double agent' Australian lawmaker Sam Dastyari quits over Chinese political links," *South China Morning Post*, 12 December 2017, https://www.scmp.com/news/asia/australasia/article/2123917/double-agent-australian-lawmaker-sam-dastyari-quits-over.

[22] Hutchens, Gareth. "Sweeping Foreign Interference and Spying Laws Pass Senate." *The Guardian*, 28 June 2018, www.theguardian.com/australia-news/2018/jun/29/sweeping-foreign-interference-and-spying-laws-pass-senate.

Both laws are useful though they have their limitations. Larissa Waters from the Australian Greens' party argued that the Australian bill does not stop foreign companies from channelling donations through "Australian subsidiaries" and criticised the "exception allowing foreign residents of Australia to donate."[23] Similarly, critics of the New Zealand law said that it might fail to respond to more roundabout means of pumping foreign money into New Zealand politics.[24]

The Australian legislation has also been criticized for potentially covering political expression without presenting any proof of harm or illegitimate foreign interests.[25]

Taiwan has been trying to tackle the problem of Chinese funding and coercion of politicians, parties, businesspeople, and other influential people, for a long time. For instance, Taiwan has the Classified National Security Information Protection Act in place to safeguard classified information and among others, penalise the sharing of such information with a "foreign hostile power."[26] Taiwan also passed an anti-infiltration law before its 2020 presidential elections. The law – among others - seek to prevent the injection of foreign funding into lobbying endeavours and election campaigns.[27]

The means of funding and coercion, especially when they are covert, may be hard to pinpoint and trace. Hence, it is vital to study publicly available cases with particular attention to the vulnerabilities the foreign actors leverage and channels they use. The like-minded countries can learn from one another's experiences by exchanging information and intelligence and with that have a better view of the tactics hostile actors may employ.

[23] Paul Karp, "Coalition bill to ban foreign political donations passes Senate," The Guardian, 15 November 2018, https://www.theguardian.com/australia-news/2018/nov/15/coalition-bill-to-ban-foreign-political-donations-passes-senate.

[24] Eleanor Ainge Roy, "New Zealand bans foreign political donations amid interference concerns," *The Guardian*, 3 December 2019, https://www.theguardian.com/world/2019/dec/03/new-zealand-bans-foreign-political-donations-amid-interference-concerns.

[25] Douek, Evelyn. "What's in Australia's New Laws on Foreign Interference in Domestic Politics." Lawfare, 31 October 2019, www.lawfareblog.com/whats-australias-new-laws-foreign-interference-domestic-politics.

[26] "The Classified National Security Information Protection Act," *Ministry of Justice*, Amendment date 2019-05-10, https://law.moj.gov.tw/ENG/LawClass/LawAll.aspx?pcode=I0060003.

[27] Lawrance Chung, "Taiwan's anti-infiltration bill Is pased as opposition lawmakers protest," *South China Morning Post*, 31 December 2019, https://www.scmp.com/news/china/politics/article/3044145/taiwans-anti-infiltration-bill-passed-opposition-lawmakers. See Also Sean Lin, "Legislature passes Anti-infiltration Act," *Taipei Times*, 1 Jan 2020, http://www.taipeitimes.com/News/front/archives/2020/01/01/2003728512. See Also "Taiwan passes anti-infiltration law aimed at combatting Chinese influence," *The Straits Times*, 31 December 2019, https://www.straitstimes.com/asia/east-asia/taiwan-passes-anti-infiltration-law-aimed-at-combating-chinese-influence.

2.5.2. Countering covert funding of NGOs

Some states implement legislation to govern both foreign and domestic NGOs operating within the country. China, for example, has introduced two laws to administer domestic social organisations and overseas NGOs, to regulate interactions between foreign NGOs and local organisations. The Charity Law introduced in September 2016 prevented improperly registered NGOs from engaging in fundraising from Chinese donors.[28] The Foreign NGO Law which came into effect on 1 January 2017 compels foreign NGOs to register with the Ministry of Public Security or equivalent agencies on the provincial level prior to establishment of office in China.[29] It also works to limit funding sources available for Chinese NGOs by preventing unregistered Chinese NGOs from seeking funding and collaboration from foreign NGOs.[30]

2.5.3. Countering covert funding of educational institutions

Some states issue guidelines to identify possible cases of foreign interference or funding of educational institutions. For example, Australia's University Foreign Interference Taskforce provides guidelines that help relevant departments and programmes to identify possible cases of interference including funding. Australian universities are encouraged to consider: (i) the minimum level of due diligence is applied to foreign investments and partnerships at all levels; (ii) providing appropriate internal reporting for funding sources; (iii) Ensuring that donations from international or domestic companies with strong foreign links place no undue influence on academic program and are appropriately disclosed including through the Foreign Influence Transparency Scheme if required; and (iv) policies on international travel, staff appointments and engagements, bribery, foreign donations and gifts.

2.5.4. Countering covert funding of media

Covert funding of media efforts (as shown in the examples raised in the previous paper) has historically utilised mediums such as radio or print. However, the prevalent form of media consumption has shifted online towards social media and the internet. The popularity of websites, microblogs and social media platforms (e.g., Facebook, Twitter) creates potential for more covert funding opportunities.

[28] "2016 Charity Law", *China Law Translate*, 16 March 2016, https://www.chinalawtranslate.com/en/2016-charity-law/

[29] "Fact Sheet on China's Foreign NGO Law," *The China NGO Project*, 1 November 2017, http://www.chinafile.com/ngo/latest/fact-sheet-chinas-foreign-ngo-law

[30] Setsuko Matsuzawa, *Activating China: Local Actors, Foreign Influence, and State Response* (Oxon and New York: Routledge, 2019).

While many states have existing regulatory restrictions for foreign ownership of media entities, Defenders can tighten regulatory tools to limit potential covert funding, and media ownership restrictions for new forms of internet content providers. For example, the Broadcasting (Class Licence) Notification of Singapore requires internet content which propagate, promote or discuss political issues relating to Singapore to submit annual statutory declarations, including funding. Statutory declarations prevent against covert funding of media and mitigates foreign influence.

Defenders may want to create a public-access repository of media ownership, which would enable the public, journalists, and academics, to hold media entities or internet content providers to account. Increased public scrutiny can be beneficial to expose linkages between covertly funded entities or individuals. This can also strengthen media literacy of citizens, who can become more aware of where their media is coming from.

2.5.5. Building Resilience to Cyberattacks

The fundamental means of cyber deterrence are (i) deterrence through hardening-- making the cyberattack too difficult to execute, (ii) deterrence through punishment – imposing a cost on the attacker, and (iii) deterrence by resilience – mitigating or reducing the impact of the cyberattack. Deterrence by hardening has its limits, as few organisations can withstand a sustained assault by hackers who are state sponsored and well resourced. Deterrence by punishment also has limits, inter alia because of the difficulty of accurate attribution.[31] Taking into account that eventually some cyberattacks will be successful in breaching defences, states are advised to build resilience, i.e., what should be done upon detection of a breach. This resilience is built through creating greater awareness before incidents occur, and developing comprehensive backup and response plans

Estonia has a well-documented case of Russian political interference by major cyberattack, which aimed to disrupt Estonian society by focusing on media websites, online bank accounts, and email systems, followed by disinformation campaigns. From this experience, Estonian officials learned that resilience to cyberattacks require not only technical responses, but also political responses.[32]

[31] Ranger, Steve. "Can Russian Hackers Be Stopped? Here's Why It Might Take 20 Years." TechRepublic, *TechRepublic*, 26 January 2019, https://www.techrepublic.com/article/can-russian-hackers-be-stopped-heres-why-it-might-take-20-years/.

[32] "What the United States Can Learn from Europe on Fighting Cyberattacks and Disinformation." *Atlantic Council*, 10 December 2019, https://atlanticcouncil.org/blogs/new-atlanticist/what-the-united-states-can-learn-from-europe-on-fighting-cyberattacks-and-disinformation/.

France also showed resilience to disinformation campaigns and "hack and leak" operations conducted by hackers linked to Russian military intelligence during their 2017 presidential campaign. These were unsuccessful in swaying the French public, due in large part to French efforts to build awareness about information manipulation in both the government and among the public, strong central organisations put in place to counter disinformation, and a strategy to push counter-narratives to blunt the effects of disinformation, such as focusing public attention on the leakers rather than the leaks.[33]

2.5.6. Countering Hostile Information Campaigns

National institutions should enhance their capability to detect and disrupt information campaigns that target them. This could involve publicly exposing disinformation, designing relevant counter-messages for stakeholders, and planning strategies for delivering the counter-messages. National campaigns can educate the public be wary of messages that encourage social division or discord. **Governments** within the Asia Pacific region have increased media and digital literacy efforts to assist in countering foreign influence campaigns.[34] Australia's News and Media Research Centre (NMRC) has proposed that media literacy be the first line of defence against disinformation. Research from NMRC demonstrated that 76 per cent of social media news consumers recorded low/very low levels of literacy.[35] To combat this, all school and university students will be instructed in information literacy, including providing them an understanding of algorithms and artificial intelligence.[36] This initiative

[33] Ministère de l'Europe et des Affaires étrangères. "Joint Report by the CAPS/IRSEM – Information Manipulation: A Challenge for Our Democracies (04.09.18)." France Diplomatie :: Ministry for Europe and Foreign Affairs, https://www.diplomatie.gouv.fr/en/french-foreign-policy/manipulation-of-information/article/joint-report-by-the-caps-irsem-information-manipulation-a-challenge-for-our.

[34] Singapore has placed high emphasis on media and digital literacy initiatives. These are seen as important anchors in the country's strategies against deliberate online falsehoods and influence efforts. These initiatives target a variety of population segments, including students, young adults and senior citizens. The "Better Internet Campaign", for instance, seeks to nurture students to become responsible and ethical users of the Internet. The National Library Board (NLB) of Singapore has a nationwide campaign which seeks to raise awareness of the dangers of fake news. The "Source. Understand. Research. Evaluate. (SURE)" programme attempts to train individuals to identify fake news. The programme was recently upgraded to comprise three main thrusts: "SURE for Life", "SURE for Work" and "SURE for School" – ensuring a comprehensive messaging to reach out to Singaporeans from different walks of life.

[35] News and Media Research Centre, "Response to selected issues regarding social media manipulation during the 2016 Australian federal election", Submission to the Joint Standing Committee on Electoral Matters, *University of Canberra*, *Australia*, https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Electoral_Matters/2016Election/Submissions

[36] An idea was proposed to fold in media and digital literacy efforts into civic education studies for Australian students, as students were more active online in activities such as political advocacy. This enables initiatives relevant for students, as current issues resonating with students are given a platform to be raised. Both political advocacy efforts and digital literacy initiatives can complement and reinforce the other.

is being conducted alongside Twitter.[37] Ahead of the Australian Federal elections, “Stop and Consider”, a nationwide digital literacy campaign, was rolled out on April 2019, to increase awareness of the potential risks hostile information campaigns and disinformation pose to electoral integrity.[38]

Legislators in some countries have implemented legislative measures to tackle disinformation. Germany’s Network Enforcement Act (Netzwerkdurchsetzungsgesetz or NetzDG) came into effect at the beginning of 2018, and is aimed primarily at online forms of hate speech inciting breaches of the public peace and public discourse, which might in some cases involve false information. It applies to social media network companies with more than two million registered users in the country. NetzDG requires these companies to implement procedures to review complaints regarding content about hosted hosting and remove anything that is illegal within 24 hours. Individuals may be fined up to €5m ($5.6m; £4.4m) and companies up to €50m for failing to comply with these requirements.[39] Since its implementation, criticism of the law has largely rounded on its chilling effect on freedom of speech, and an observation was made that most of the takedowns in the period after the law coming into force mostly took place as a result of enforcement of the key online platforms’ community guidelines, and not so much as a result of NetzDG.[40] There is no substantial evidence as yet to demonstrate the law’s effectiveness on online disinformation. In October 2018, France passed two anti-fake news laws to counter the spread of false information during election campaigns, in the wake of allegations of Russian meddling in the 2017 presidential elections. These laws enable a candidate or political party to obtain a court injunction preventing the dissemination of “false information” in the three months prior to a national election. They empower France’s broadcast authority to take any network that is “controlled by, or under the influence of a foreign power” off the air if it intentionally disseminates false information.[41] The next presidential elections are in 2022, and these laws have yet to be tested. In December 2018, Taiwanese legislators proposed amendments to their Social Order Maintenance Act, to criminalise the publication of misinformation.

[37] Ibid.

[38] “Stop and Consider”, *Australian Electoral Commission*, https://www.aec.gov.au/elections/electoral-advertising/stopandconsider.htm

[39] BBC News, “Social media: How can governments regulate it?”. Accessed 12 December 2019. https://www.bbc.com/news/technology-47135058,.

[40] Tworek, Heidi and PJ Leerssen. “An Analysis of Germany’s NetzDG Law” High Level Working Group on Content Moderation Online and Freedom of Expression, 15 April 2019, pp. 2 – 5. https://www.ivir.nl/publicaties/download/NetzDG_Tworek_Leerssen_April_2019.pdf.

[41] *The Straits Times*, “What countries around the world are doing to tackle fake news and violent content”. Accessed 12 December 2019. https://www.straitstimes.com/world/what-countries-around-the-world-are-doing-to-tackle-fake-news-and-violent-content

These chiefly involve increased fines for disseminating disinformation, and it is left to government agencies and the courts to decide if published information is false.[42] In the case of Singapore, the Protection from Online Falsehoods and Manipulation Act, which came into effect in early October 2019, is discussed below.

Citizens can be educated to resist hostile information campaign efforts. Improving the psychological resilience in the citizens (and non-citizens) in a country is one of the strategies in the toolkit of policymakers to combat foreign interference. Risks posed by foreign influence and interference campaigns are not restricted to a single demographic. Ultimately, research must go into determining and understanding the behavioural characteristics and demographics of population segments.[43] Tailored messaging and communication strategies for various demographics is crucial in crafting media and digital literacy. Short, informational videos on the importance of resilience against hostile information campaigns online can provide brief explainers on foreign influence and interference. **Social media users** can flag malicious accounts and content to social media companies. A state-supported Netizens-On-Watch (NOW) scheme that is similar to Singapore's Riders-On-Watch (ROW) scheme could help. Positive online influencers who can amplify positive messages – relating to national cohesion and public peace – can help to neutralise negative messages. They can focus on (i) preventing disinformation from pulling in more people, (ii) pulling back people who were influenced by negative messages but can be persuaded, and (iii) encouraging healthier debates on social and political issues.

Social media companies should be encouraged or required by law to detect and remove postings and accounts containing harmful content promoting sedition, hate and public disorder. So far, the self-regulatory measures that social media companies have undertaken have been found to be inadequate.[44] They are reluctant to remove malicious accounts or content do not violate their "community standards", even if potentially threatening to national security. Several countries have passed legislation to enforce compliance, which

[42] Jane Rickards, "The Battle Against Disinformation", AmCham Taipei, accessed 12 December 2019. https://topics.amcham.com.tw/2019/08/battle-against-disinformation/

[43] For instance, Instagram has a high concentric usage amongst teenagers and young adults in Singapore, while youth usage of Facebook has declined and tapered over the years. Understanding and analysing context is also important as social media platforms usage differs across Asia Pacific countries.

[44] Zhang, Lim Min. "Parliament: Tech Firms Are Partners in Tackling Fake News but They Can't Be Left to Self-Regulate, Says Shanmugam." *The Straits Times*, 7 May 2019, https://www.straitstimes.com/politics/parliament-tech-firms-are-partners-in-tackling-fake-news-but-they-cant-be-left-to-self

we have noted above. Currently, the companies have their own guidelines to assess the content circulated on their platforms. For instance, Facebook takes an action against "coordinated inauthentic behaviour" on their platform. The term "coordinated inauthentic behaviour" is often used by Facebook and it is defined as "groups of pages or people work[ing] together to mislead others about what they are or what they are doing."[45] Accordingly, Facebook takedowns are not guided by the content of a post; they are practiced based on the identification of a "deceptive" behaviour in the platform.[46] The company leverages people and technological solutions in tackling coordinated inauthentic behaviour. While experts "manually" search for and "take down the most sophisticated networks," technological solutions help "automatically detect and remove the most common threats" such as "fake accounts."[47]

Facebook recently started "We Think Digital", an Asia Pacific digital literacy initiative, with the aim of developing the skills individuals need to enjoy digital technology safely, skills such as critical thinking and empathy.[48] Announced in March 2019, this initiative has Facebook collaborating with various local partners in countries from Singapore, Taiwan, the Philippines, Indonesia and the Asia Pacific region.[49] Resources are made available for local partner agencies to educate on critical thinking and digital literacy skills when using Facebook (e.g. educating teenagers and young adults in navigating Facebook safely and securely).[50] **Technical solutions** are being developed to uncover and monitor the usage of bots (coordinated and inauthentic automated accounts) for coordinated disinformation online campaigns (called "astroturfing"). Such tactics could reduce the bots' ability to exploit and manipulate public opinion. Technical platforms such as BotSlayer can be used during elections to identify, monitor and remove malicious accounts.[51]

[45] *Nathaniel Gleicher*, "Coordinated Inauthentic Behavior Explained" [Video], Facebook Newsroom, 6 December 2018, https://about.fb.com/news/2018/12/inside-feed-coordinated-inauthentic-behavior/.

[46] Ibid.

[47] Ibid.

[48] Clair Deevy, "Introducing We Think Digital: New Digital Literacy Resources to Reach 1 Million People in Asia Pacific by 2020", *Facebook*, 4 March 2019, https://about.fb.com/news/2019/03/introducing-we-think-digital-new-digital-literacy-resources-to-reach-1-million-people-in-asia-pacific-by-2020/

[49] Facebook plans to extend this initiative globally, including countries such as Argentina.

[50] "Facebook Youth Portal", *Facebook*, https://www.facebook.com/safety/youth

[51] "Tracking coordinated disinformation campaigns online made easier with new BotSlayer tool", *Indiana University*, 12 September 2019, https://news.iu.edu/stories/2019/09/iub/releases/12-botslayer-launch.html

Observations in respect of tackling coordinated inauthentic behaviour: Having outlined various countermeasures in respect of the online front, it must be emphasised that identification of the perpetrators of deceptive behaviour in online spaces is a difficult task. Strategising coordinated inauthentic behaviour may involve the mobilisation of intermediaries, including cyber troops. Cyber troops are "government or political party actors tasked with manipulating public opinion online."[52] Cyber troops are hard to locate in an online environment where ideologically driven groups, "fringe movements," "hacker collectives," social media influencers and other such groups co-exist, and sometimes work concurrently towards a mutual cause.[53] Domestic as well as external actors may leverage cyber troops in their online mission, and cyber troops may carry out various tactics including "micro-targeting," "trolling," managing "political bots," and others.[54] Here it should be noted that not all these tactics are unlawful.[55] However, the tactic becomes questionable when it is **deliberately, covertly** and/or **deceptively** used to **disrupt** or **sway** politics, policies, and opinions.

[52] 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

[53] Ibid, 9.

[54] Ibid, 1.

[55] For instance, a marketing company may use micro targeting when advertising a product to a defined audience group, or companies may use bots to provide rapid response to basic customer enquiries.

3. The role of legislation in countering foreign interference

Legislation is one of the important parts of countering foreign interference, and has to be integrated into a comprehensive approach which includes establishing a strategic task force, intelligence gathering, technology development (for prevention and detection), skills development for practitioners, identifying and cultivating key stakeholders and partners, building information sharing channels, public announcements, strategic use of communications and media, public education, building media literacy and critical thinking, supporting citizens, and building public resilience.

Some of the key areas that legislation can cover are

- Regulating foreign funding of politicians, political parties, NGOs, business groups, educational institutions, media, etc. – learning from the experiences of Australia and New Zealand above
- Regulating new media / social media platforms for content which would amount to foreign interference – learning from the experiences of Germany and France above
- Prohibiting the use of inauthentic online accounts (trolls) or automated online accounts (bots) for foreign interference
- Updating procedures for investigation into foreign interference activities

Any foreign interference legislation must be used carefully and strategically. Political parties all over the world have been accused of alleging foreign interference as an excuse to target their opponents; one example is the US Republican party's hostile response to investigations into Russian interference in the 2016 Presidential Elections. Allegations of foreign interference can also damage international relations and trade. Foreign interference laws should be used in cases which are clear and undeniable, and even then, they should be used in coordination with strategic communications to ensure that they do not cause the very division that they are aiming to prevent.

3.1 POFMA

Singapore passed the Protection From Online Falsehoods and Manipulation Act 2019 (hereafter "POFMA") to "prevent the electronic communication in Singapore of false statements of fact, to suppress support for and counteract the effects of such communication, to safeguard against the use of online accounts for such communication and for information manipulation, to enable measures to be taken to enhance transparency of online political advertisements, and for related matters."[56]

Although POFMA is not a legal tool that was enacted to counter foreign interference, it can complement national efforts to address the threat when it comes through the online information space. At the second reading of the POFMA Bill in May 2019, it was cited that sources of online falsehoods include "foreign countries using information warfare."[57] A noteworthy example is how Russia had interfered in the US 2016 Presidential Election through online political advertisements and social media. Investigations by the US Senate Select Committee on Intelligence uncovered that the Russian Internet Research Agency (IRA) had reportedly spent "$100,000 over two years on advertisements" in addition to the "61,500 Facebook posts, 116,000 Instagram posts, and 10.4 million tweets" that were created for influence operations.[58]

In January 2020, the Singapore government had invoked POFMA against the Malaysian NGO Lawyers for Liberty (LFL) after it made allegations about the capital punishment for drug trafficking in Singapore.[59] This episode follows earlier attempts by Malaysia to persuade Singapore not to send convicted Malaysian drug traffickers to the gallows.[60] Of note, LFL reportedly has links with Malaysian politicians and the People's Justice Party (PKR).[61] Although there is no information to suggest a foreign state's campaign against Singapore's use of capital punishment, these episodes do highlight attempts by ideologically dissimilar foreign elements to influence Singapore's crime-fighting and legal policies.

[56] Protection from Online Falsehoods and Manipulation Act (No 18 of 2019)

[57] MinLaw. "Second Reading Speech by Minister for Law, K Shanmugam on The Protection from Online Falsehoods and Manipulation Bill." *Parliamentary Speeches*, 7 May 2019. https://www.mlaw.gov.sg/news/parliamentary-speeches/second-reading-speech-by-minister-for-law-k-shanmugam-on-the-protection-from-online-falsehoods-and-manipulation-bill

[58] Select Committee on Intelligence. "Russian Active Measures Campaigns and Interference in the 2016 US Election, Volume: Russia's Use of Social Media." United States Senate, October 2019, p. 40. https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume2.pdf.

[59] CNA, "Singapore invokes online falsehoods law against Malaysian rights group's 'preposterous' claims on execution methods." *Channel NewsAsia*, 22 January 2020. https://www.channelnewsasia.com/news/singapore/pofma-malaysia-lawyers-for-liberty-drugs-execution-falsehoods-12299384

[60] Koh, Fabian. "Untenable to give special moratorium on execution of Malaysian death-row prisoners: Shanmugam." *The Straits Times*, 24 May 2019. https://www.straitstimes.com/singapore/courts-crime/not-tenable-to-give-special-moratorium-to-malaysian-drug-traffickers

[61] Goh, Melissa. "Malaysian MP calls for tighter gun control locally after Las Vegas shooting." *Channel NewsAsia*, 3 October 2017. https://www.channelnewsasia.com/news/asia/malaysian-mp-calls-for-tighter-gun-control-locally-after-las-9275970

4. Conclusion

In sum, mounting a response against the threat of foreign interference should be a combination of focusing on the strategic factors outlined above, and the design and implementation of practical and active countermeasures. The focus is necessary as the threat will persist as long as divergent foreign policies exist and as long as the domestic policies of one state have external effects on the interests of another state.

Singapore must play a long game against foreign states that rely on foreign interference as an instrument of political warfare. The manner of application of these countermeasures must be fair and necessary both in terms of process and perception, without perpetuating the image of an Orwellian state. Singapore must not appear to be taking sides in geopolitical rivalries or using foreign interference as a pretext to clamp down on local political discourse and responsible activism. Ultimately, Singapore’s survival depends on both its foreign policy’s principle of neutrality and reputation of openness to global trade, talent, investments and ideas.

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.

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.

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.

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 US, Dutch, and Australian university systems.

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.

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