Annexes for Minister's 2R Speech – Folder 1

The examples cited in the Annexes are based on open-source reports, or through testimonies provided at the Select Committee on Deliberate Online Falsehoods (which are then attributed to the representator), and are not MHA's comments.

Contents

Annex A: Foreign Interference Tactics

(1) Gerasimov Doctrine – Modern Warfare

1. The Russians have developed a military doctrine for the Internet age – the Gerasimov Doctrine, named after Russia's Chief of General Staff of the Armed Forces.

2. The Gerasimov doctrine took tactics developed by the Soviets, blended them with strategic military thinking about total war, and laid out a new theory of modern warfare.

3. It specifies that the objective is to achieve an environment of permanent unrest and conflict within an enemy state. This includes harnessing the "protest potential" of the population of a target country, deepening divisions, increasing hostility among the different groups, and getting them to distrust institutions.

4. With this doctrine, the "Rules of War" have changed. Non-military means of achieving political and strategic goals without using the force of weapons include utilizing a range of actors and tools, e.g. hackers, media, businessmen, information leaks and disinformation.

5. Several countries (Georgia, Syria, Ukraine, US) have complained of attacks mounted by the Russians under this doctrine.

   a. Russia has been deploying the Gerasimov Doctrine in Ukraine for the past several years. During the 2014 protests there, the Kremlin supported extremists on both sides of the fight (the pro-Russian groups and the Ukrainian ultra-nationalists) and fueled conflict that the Kremlin used as a pretext to seize Crimea and launch the war in eastern Ukraine.

      - The government was portrayed as a fascist junta, xenophobic, racist and anti-Semitic. Foreign Policy reported that in October 2014, a few weeks shy of the 109th anniversary of the 1905 Odessa pogrom, some foreign newspapers "wrote that members of the Right Sector were terrorizing the Jewish community of Odessa in Ukraine and had beaten more than 20 people. Local Jewish leaders were reported to be in the process of preparing an appeal to the World Jewish Congress, asking the international Jewish organisation to intercede on their behalf".

      - StopFake (a fact checking site launched in 2014 by Kyiv Mohyla Journalism School lecturers, graduates and students and the KMA Digital Future of Journalism project) highlighted that at the end of July 2018, there was proliferation of "a new fake… (that) Ukrainian children (were) forced to play with (a) stuffed Hitler toy." StopFake reported that this was then carried on various foreign, Bulgarian and Uzbek news sites.

      - Politico reported that "Three days before the presidential election in May 2014, hackers broke into Ukraine's Central Election Commission and disabled parts of the network using advanced cyberespionage malware, according to a report by the International Foundation of Electoral Systems funded by the US and UK and seen by Politico… Large-scale attacks followed the next year and again in 2016. The targets, this time, were companies running Ukraine's power grid… so-called KillDisk malware later destroyed parts of the grid."

- The attacks resulted in the Crimeans believing that their lives and freedoms were in danger and undermined the trust in the government's ability to provide protection. It also acerbated tensions between different communities. Foreign Policy reported that based on Israeli Interior Ministry's statistics, more than 32,000 people left Ukraine for Israel, and this exodus was overwhelmingly motivated by the instability and danger caused by Russian aggression rather than anti-Semitic attacks. A report by democrats on the US Senate Foreign Relation Committee also reported that it affected Ukraine's relations with other nations and potentially affected its ability to enter into international trade agreements.

b. More recently, on 6 Sep 2021, the German Foreign Ministry accused Russia of launching a disinformation and influence campaign, including cyber-attacks on German politicians and political candidates to gain access to their personal emails, as well as the spread of false information about specific candidates. These accusations came after a warning by the German domestic intelligence agency in Jul 2021 that a Russia-linked threat actor group, Ghostwriter, had been targeting private email addresses of German Members of Parliament and regional legislators dating back to at least Feb 2021. In another example, there was a false claim that the Green Party's candidate wanted to abolish Germany's widow's pension to fund support for refugees, and Correctiv revealed that the post was shared 2,800 times within a day. This campaign was aimed at undermining trust in public institutions and discrediting candidates who hold adversarial positions against Russia. Germany lodged a diplomatic protest to the Russian government in response to these attacks.

Note: The examples cited in the Annexes are based on open-source reports, or through testimonies provided at the Select Committee on Deliberate Online Falsehoods (which are then attributed to the representator), and are not MHA's comments.

(2) New Communication Tools

1. The online space has been used as a vector to conduct attacks. Social networks, bots and algorithms can flood the information space cheaply and quickly.

   a. Social networks are a major threat vector due to their reach, as well as their algorithms that are geared to maximise engagement.

   b. Bots (e.g. social bots, spam bots) can then further facilitate such proliferation of content on platforms by artificially inflating engagement. A bot can be as cheap as US$3000 for a small-size one (used for small business marketing on Facebook messenger). Coupled with algorithms, it allows one to automatically generate messages, mimic users on social media platforms (some can even directly communicate with real users), and massively boost follower levels or interactions with a post to create an artificial impression of popular opinion.

   c. Dr Kevin Limonier provided evidence to the Select Committee about a HIC perpetrated via Russian media outlets, social media platforms and bots. He identified four methods:

      i. Russian outlets spread grand narratives that cast the Western world as hegemonic and Russia as a champion of free-thinking and multi-polarity. It also included anti-Macron narratives, including rumors that Macron had a secret offshore account. This was supported by selective editorial content.
      ii. Use of social networks to target different groups.
      iii. Manipulation of social media to gain visibility of content, such as 'click-bait' articles.
      iv. Bots and trolls to relay or interact with the online content of Russian media outlets.

2. Brookings Institute reported that based on the US Department of Justice's Special Counsel Investigation, findings of the US Intelligence community and disclosures by tech companies at the Congressional testimony and investigative reports, Russia's influence campaign against the US during 2016 elections were as follows:

   a. Purchase of ads on Facebook at estimated cost of US$100,000,
   b. Ads on Google at US$4,700,
   c. Set up approximately 36,000 automated bot accounts on Twitter and
   d. Operated the IRA troll form at an estimated cost of US$3milion over the course of two years.

   Overall, including other methods such as cyber-attacks, the total known cost of Russia's most high-profile influence operation was reported to be around US$4 million, which helped Russian-linked content reach 125 million Americans.

3. Another example reported by various news outlets including BBC and the Economist - during the 2017 French Presidential Elections, fake documents were leaked hours before campaigning stopped for a "cooling off" period before voting. The leaked files were spread on 4Chan (an anonymous messaging board 4chan), then spread onto Twitter, and by political commentators and US alt-right and French far-right personalities. **Bots were used to retweet Twitter content (some accounts posted 150 tweets per hour).**

Note: The examples cited in the Annexes are based on open-source reports, or through testimonies provided at the Select Committee on Deliberate Online Falsehoods (which are then attributed to the representator), and are not MHA's comments.

(3) HIC Tactics

1. HIC tactics have become more sophisticated. The online space, which provides anonymity to users, makes it easier for foreign actors to escape detection and avoid attribution. Many social media platforms allow one to create multiple accounts, without verifying their identity or requiring the use of real particulars; accounts can also be sold or stolen.

2. In a recent report, Facebook said that of the over 150 influence operations taken down from 2017 to 2020, there has been a shift to smaller, more targeted operations that are harder to detect (e.g. instead of using bots, setting up troll farms in third countries). Facebook's 'The State of Influence Operations 2017-2020' report identifies the following evolving tactics, based on the "influence operations" removed by it during this period.

3. **Platforms have shifted from "wholesale" to "retail" influence operations, aimed at evading platforms' enhanced automated measures to block fake accounts.** Threat actors use fewer assets, focus on narrowly targeted audiences, and spend more time creating credible online personas that are less easily detected. These includes creating other supporting accounts so that when researchers or journalists attempt to verify identity, it will appear more legitimate. This means HICs are also harder to attribute definitively. Examples:

    a. **[Third country troll farms]** In Aug 2021, Facebook reported that it had removed a Russian network of fake accounts originating from account farms in Bangladesh and Pakistan, and which targeted audiences in India, Latin America and the US with disinformation about western-made COVID-19 vaccines. In India, these fake accounts first posted about innocent topics such as Indian food and Hollywood actors to gain followers, but when the Indian Government started discussing emergency authorization for the AstraZeneca vaccine, these accounts started to push false claims about the vaccines. Reuters reported that these networks included accounts on Instagram and Facebook, and the network organizer had attempted to pay influencers on YouTube and TikTok to amplify the messages. In addition, the Select Committee received testimony about troll farms in Macedonia which had created fabricated and highly partisan "news" stories during the US Presidential elections to earn money from advertising (although it is unclear if these farms were serving state-sponsored ends). **[Elaboration in Annex E]**

    b. **[Iran networks]** Facebook removed an Iranian network removed in May 2019 that used a small number of accounts that posed as journalists and other fake personas. Instead of broadcasting content, they sought to reach out directly to policymakers, reporters, academics etc. and submitted letters and columns to US newspapers. These accounts managed to get their work published in some legitimate publications.

    c. **[Russians posing as citizen journalists in Ukraine]** Facebook removed a network run by Russian military intelligence that targeted Ukraine and other neighbouring countries in early 2020. The network created fake personas that operated across blogging forums and multiple social media forums. Some posed as citizen journalists and tried to contact policymakers.

4. **Blurring the lines between authentic public debate and deception.** Sophisticated foreign actors co-opted unwitting but sympathetic domestic groups to amplify their narratives.

   a. **[Spamouflage Dragon]** In Feb 2021, social media analysis firm, Graphika, reported that it detected what it called “Spamouflage Dragon”, increasing in its sophistication and beginning to reach real social media users, including “heavyweight influencers”, with hundreds of videos that praise one country and criticise the US. Besides using clearly fake accounts, Spamouflage has begun to develop “persona accounts”, a mix of accounts created from scratch but with an attempt to build a seemingly real persona overtime, and accounts hacked or stolen from real people. Spamouflage’s content has been amplified by the Venezuelan foreign minister, a Pakistani Minister, and other influential social media users. Issues covered include Covid-19, the safety of the Pfizer-BioNTech vaccine, content portraying the US in a negative light (e.g. praising the US Capitol storming as “a beautiful sight”, calling the US the “greatest threat” to world peace).

   b. **[Russian IRA-linked network]** FB removed a Russian IRA-linked network looking to co-opt real people engaging on political issues, in Jul 2018. They would target events focused on hot-button issues and volunteer to amplify such events for local organisers. In addition, the Select Committee received testimony about the activities of IRA such as their targeting of the Black Lives Matter movement.

5. **Perception hacking**

   a. Give the impression that elections are compromised, without actually mounting the interference operation. The aim is to sow confusion and doubt.

   b. Facebook reported that in the 2018 US Mid-Terms, the Russian IRA claimed they were running thousands of fake accounts that threatened to sway the election, and created a website with an election countdown timer.

6. **Rise of Influence Operations-for-hire.** Commercial actors – media, marketing and PR companies – have offered influence operations services, including to clients abroad, making information manipulation accessible to parties without the capabilities.

   a. **[Archimedes Group]** Facebook identified and removed accounts run by Israeli PR firm Archimedes Group, which ran campaigns on behalf of clients in Africa (e.g. Nigeria, Senegal, Togo), and with “some activity in Latin America and Southeast Asia”.

   b. **[Sepulveda]** Dr Shashi Jayakumar described to the Select Committee an active disinformation-for-hire industry, including one Andreas Sepulveda in Latin America whose methods included hacking, smear campaigns, disinformation and subversion.

7. **Improving ways to evade detection.** As governments and social media platforms improve their detection capabilities, threat actors are also improving their tactics, and avoiding automated detection by avoiding “inauthenticity clues” – e.g. by re-appropriating content rather than creating their own.

8. **Platform diversification.** Influence operations tended to target multiple platforms to increase chances of surviving enforcement.

    a. Targeted hyper-local platforms (e.g. local blogs and newspapers) to reach specific audiences, target public-facing spaces with less resourced security systems.

Note: The examples cited in the Annexes are based on open-source reports, or through testimonies provided at the Select Committee on Deliberate Online Falsehoods (which are then attributed to the representator), and are not MHA's comments.

Annex B: Examples of Foreign Interference in Ukraine, Czech Republic and Netherlands

(1) Foreign Interference in Ukraine

1. The Select Committee on Deliberate Online Falsehoods received various representations about Russian disinformation operations in Ukraine, which achieved considerable success. The tactics included targeting groups vulnerable to Russian influence, supporting overarching and emotive narratives, as well as fueling existing tensions between different communities. For example, Russian media outlets published news articles and commentaries that targeted sensitive local fault lines in order to falsely portray the Ukrainian government as a fascist, racist and xenophobic junta. They also pushed out communications targeted at soldiers in the Ukrainian Armed Forces to undermine their trust in the organisation and their will to defend their country.

2. Below illustrates the methods undertaken by foreign state actors following the 2014 Euromaidan revolution, based on representations to the Select Committee and News Reports.

3. Misinformation campaigns to undermine trust in the government and exploit sensitive fault lines.

   a. The government was portrayed as a fascist junta, xenophobic, racist and anti-Semitic.

      Foreign Policy reported that in October 2014, a few weeks shy of the 109th anniversary of the 1905 Odessa pogrom, some foreign newspapers wrote that members of the (for right group) Right Sector were terrorizing the Jewish community of Odessa in Ukraine and had beaten more than 20 people. Local Jewish leaders were reported to be in the process of preparing an appeal to the World Jewish Congress, asking the international Jewish organisation to intercede on their behalf.

      StopFake (a fact checking site launched in 2014 by Kyiv Mohyla Journalism School lecturers, graduates and students and the KMA Digital Future of Journalism project) highlighted that at the end of July 2018, there was proliferation of “a new fake… (that) Ukrainian children (were) forced to play with (a) stuffed Hitler toy.” StopFake reported that this was then carried on various foreign, Bulgarian and Uzbek news sites.

b. The campaign also sought to undermine trust in the Ukrainian army, and weaken the resolve of Ukrainians to defend their nation.

> *Ukraine Crisis Media Centre, Written Representation (No. 54), p 7 to the Select Committee on Deliberate Online Falsehoods*
>
> "Our analytical group was involved in Ukrainian military strategic communications in the period of 2015 – 2017. At the beginning of that period a foreign power used various tailored narratives against the Ukrainian Armed Forces. Here are some of them.
>
> - Leadership of your army is weak. It must be fired.
> - Conditions of service in your army are terrible.
> - Your President betrayed you in Minsk negotiations. He and his generals are traitors.
> - West doesn't care about you. You are doomed.
> - You can always escape from the army going to Russia or Donetsk
> - Don't let yourself be fooled by your illegal government."

4. Use of bots and inauthentic social media accounts.

c. Researchers analysed Twitter data and found a notable spike in tweets following the Malaysia Airlines MH17 crash. Dutch journalists, Robert van der Noordaa and Coen van de Ven studied the data, and found that many of these were driven by coordinated inauthentic activity. They reported in the Dutch weekly *De Groene Amsterdammer,* that in the 24 hours after the MH17 crash, there were at least 65,000 tweets blaming the Ukrainian government in Kiev for the disaster.

d. Moreover, VoxUkraine (an independent analytical platform founded in 2014 that conducts research on major economic and political processes and decisions in Ukraine) analysed the same set of tweets and found evidence that over 200 Twitter accounts were managed centrally and several accounts belonged to one owner.

5. Cyber-attacks against critical infrastructure.

a. Politico reported: three days before the presidential election in May 2014, hackers broke into Ukraine's Central Election Commission and disabled parts of the network using advanced cyberespionage malware, according to a report by the International Foundation of Electoral Systems funded by the US and UK and seen by Politico… Large-scale attacks followed the next year and again in 2016. The targets, this time, were companies running Ukraine's power grid… so-called KillDisk malware later destroyed parts of the grid."

6. The above led to the following consequences:

   a. Government lost support of some citizens. The BBC reported in March 2014 (after Russia took over Crimea) that “some 95.5% of voters in Crimea have supported joining Russia, officials say, after half the votes have been counted in a disputed referendum.”

   b. Exacerbated tensions between different communities. Foreign Policy reported that based on Israeli Interior Ministry statistics, more than 32,000 people left Ukraine for Israel, and this exodus was overwhelmingly motivated by the instability and danger caused by Russian aggression rather than anti-Semitic attacks.

   c. Affected Ukraine’s relations with other nations and potentially affected its ability to enter into international trade agreements. Mr Jakub Janda told the Select Committee that the foreign HIC discredited Ukraine’s standing in other EU countries (e.g. a forged official letter from Sweden’s Ministry of Justice was circulated online to suggest that Ukraine had sought to improperly influence a case before the Swedish Courts, which undermined support for Ukraine among the Swedish public), and loss of territorial sovereignty and lives.

7. More recent examples of interference in Ukraine are as follows:

   a. The New York Times reported in Mar 2019 that the Security Service of Ukraine (Sluzhba Bezpeky Ukrayiny, SBU) reported that it had countered a Russian attempt to use Facebook to undermine the vote in the 2019 Ukrainian elections. In an effort to circumvent Facebook’s new safeguards and interfere in the elections, instead of setting up fake accounts, Russian operatives sourced ‘people in Ukraine on Facebook who wanted to sell their accounts or temporarily rent them out’ and then used the accounts to manipulate voter attitudes through the dissemination of disinformation.

   b. Shortly before the elections, Facebook reported that it removed 107 Facebook pages, groups and accounts and 41 Instagram accounts operated by a network in Russia that operated in Ukraine. Facebook said there was “some technical overlap with Russia-based activity we saw prior to the US mid-term elections”, and that the behaviour “shared characteristics with previous the Internet Research Agency activity”.

   c. The EU External Action Service’s website EUvsDisinfo reported that following the first round of voting in 2019 Ukrainian Presidential Elections, Russian state-backed media outlets criticised the results, which placed candidate Volodymyr Zelenskiy ahead in the polls. Articles published by those outlets claimed that the election was ‘a rigged contest’ and falsely linked Zelenskiy to the 2019 Notre Dame fire in an effort to undermine his electability.

   .

(2) Foreign Interference in Czech Republic

1. The Select Committee on Deliberate Online Falsehoods received evidence from Jakub Janda, Head of the Kremlin Watch Program & Director of the European Values Think-Tank in Prague, Czech Republic, that Russia targeted extremists and fringe politicians to spread propaganda, and this was amplified by social media networks, resulting in public losing trust in the media and public institutions.

2. Based on research by the European Values Think-Tank in Prague, foreign disinformation campaigns had been successful in the Czech Republic. One-quarter to one-third of the Czech population believed that Ukraine is governed by a fascist government. This had resulted in Czech government not being able to support Ukraine with, for example, humanitarian aid. A quarter of Czechs also believed disinformation, which results in figures such as four in ten Czechs blaming the US for the crisis in Ukraine. Mr Janada said 53% of Czechs believed there is propaganda both for and against a foreign country in the Czech public space and that they cannot trust anything.

   Mr Jakub Janda told the Select Committee that if disinformation was not countered properly, it may result in the public losing trust in democratic institutions, in free media, and in democratic political parties.

3. Separately, the Guardian reported in Jan 2017 that the Czech Republic's Ministry of Foreign Affairs suffered a "sophisticated" data breach after hackers compromised dozens of email accounts belonging to senior diplomats. It was reported that thousands of files were downloaded from the ministry's external mailing system. Although the Czech Public made no public attribution, the Guardian said "another foreign ministry official – speaking anonymously – confirmed that fingers were being pointed at Russia". Vlado Bizik, a cybersecurity expert with the Prague-based European Values think tank, told the Guardian that the hack resembled another carried out against the Polish foreign ministry.

4. According to Balkan Insight, the 2018 Czech Republic presidential elections was also targeted. The report said there was a "Kremlin-linked disinformation campaign", in support of pro-Russia candidate Milos Zeman, who ultimately won his second term by "a slender majority" of around 150,000 votes. The report said Zeman's opponent Jiří Drahoš as a supporter of unrestricted immigration and a paedophile.

(3) Foreign Interference in Netherlands

1. According to the New York Times, Dutch left-wing politician Harry van Bommel's efforts to convince Dutch voters to reject the EU–Ukraine trade referendum in 2016 were likely supported by a group of Russians. The "Ukrainian team", whose most active members were from Russia, attended public meetings and appearances, and used social media to spread disinformation. This included a video that reportedly showed members of the Ukrainian National Guard burning the Dutch flag and threatening to carry out attacks against the Dutch if they voted against the trade agreement. The Russians also pretended to be Ukrainians and inflamed local debates. This was supported by online disinformation campaign involving fake stories about Ukraine. Eventually, Dutch voters voted against the trade agreement.

> *Minority Staff Report for the US Senate Foreign Relations Committee, p 113-114*
>
> "In April 2016, the Netherlands held a referendum on whether to approve a trade agreement between the EU and Ukraine. A left-wing member of the Dutch Parliament, Harry von Bommel, recruited a "Ukrainian team" to campaign against the agreement. The team used public meetings, television appearances, and social media to portray the Ukrainian government as a "bloodthirsty kleptocracy".
>
> Ultimately, the referendum saw a relatively low turnout of 32 percent of the Dutch population, with about two-thirds of those voting against the agreement. One Ukrainian foreign ministry official cited a poll which reported that 59 percent of those voting "no" said that their perception of Ukraine as corrupt was an important motivation for their vote; 19 percent believed that Ukraine was responsible for the shooting down of Malaysia Air Flight 17, which killed 298 people, including 193 Dutch citizens; and 34 percent thought that the agreement would guarantee Ukraine's accession to the EU (the latter two points are demonstrably false)."

2. According to Dutch daily newspaper,de Volkskrant, two Russian-backed hacker groups (Fancy Bear and Cozy Bear) attempted to gain online access to a number of ministries in the Netherlands, including the Ministry of General Affairs, which includes the Prime Minister's office. The hacking attempts took place over six months in the lead-up to the Dutch general election, although they were ultimately unsuccessful in obtaining any confidential information or credentials. Rob Bertholee, head of the Dutch Intelligence service AVID and General Intelligence and Security Service of the Netherlands, confirmed that it was Russia that was "trying to penetrate secret government documents". According to the annual report of the Dutch Intelligence service AVID, Russia also tried to influence the 2017 Dutch election by spreading fake news. Journalists from NRC Handelsblad reported that voters had been encouraged to vote for far-right politician Geert Wilders and the far-right PVV party by social media accounts linked to the Russian Internet Research Agency (IRA). The report said Russia was not afraid of using Cold War methods to obtain political influence, and they were "using the freedom of open and democratic societies of the West".

Note: The examples cited in the Annexes are based on open-source reports, or through testimonies provided at the Select Committee on Deliberate Online Falsehoods (which are then attributed to the representator), and are not MHA's comments.

Annex C: Examples of Foreign Interference (Reports Identifying Iran as a Foreign State Actor)

1. **[Target: Israel]** In June 2021, the New York Times reported an Iranian influence operation in Israel. Iranian agents infiltrated many private messaging groups used by Israeli activists for private discussions. Once there, they spread polarising content to sow mistrust amongst the online communities. These "miniaturised" influence operations aimed to stay under the radar to avoid detection.

2. **[Target: US]** The US intelligence community assessed that Iran had carried out a "multi-pronged covert influence campaign" against Trump during the 2020 elections. Without directly promoting his rivals, they undermined public confidence in the electoral process and US institutions, and sowed division and exacerbated societal tensions in the US. The report cited:

    a. Iranian cyber actors sent threatening, spoofed emails purporting to be from the Proud Boys group to democratic voters in multiple US states, demanding that the individuals vote for Trump, and spread a video intending to demonstrate alleged voter fraud.
    b. Social media accounts published over 1000 pieces of online content, and number of inauthentic social media accounted to at least several thousand.

3. **[Target: US]** A small Iranian network was removed by Facebook in May 2019. The network posed as journalists and other fake personas. Instead of broadcasting content, it sought to reach out directly to policymakers, reporters, academics etc. and submitted letters and columns to US newspapers. These accounts managed to get their work published in some legitimate publications.

4. **[Target: UK]** According to The Telegraph, a network of Iranian internet trolls on Twitter attempted to divide public opinion by spreading divisive information on the day of Britain's EU membership referendum in 2016. More than 770 Iranian Twitter accounts were found to have been engaged in coordinated manipulation by spreading disinformation on British politicians Nigel Farage and Boris Johnson while praising the leader of Britain's opposition Labour Party, Jeremy Corbyn.

5. **[Target: UK]** According to The Herald, multiple Facebook pages were taken down ahead of the 2014 Scottish independence referendum after they were discovered to be fake Iranian-backed accounts. This included a pro-independence page called 'Free Scotland 2014', for example, which was involved in spreading fake news to more than 20,000 of its followers about Jeremy Corbyn, Boris Johnson, Donald Trump, and the British monarch. The page was also connected to a series of Iranian state-backed media outlets. Twitter confirmed that it shut down a further 284 fake accounts, most of which originated from Iran, for engaging in inauthentic coordinated manipulation. The motive behind the fake accounts was to promote left-wing and anti-Western opinions by targeting British voters.

Note: The examples cited in the Annexes are based on open-source reports, or through testimonies provided at the Select Committee on Deliberate Online Falsehoods (which are then attributed to the representator), and are not MHA's comments.

Annex D: Foreign Interference in the Online Space

(1) Highlights from Select Committee's Report on Low Cost and Ease of Disinformation Online

1. Ms Myla Pilao (Director, Core Technology Marketing, TrendMicro) gave evidence at the Select Committee on Deliberate Online Falsehoods of the services available on the market and how they can be exploited. One example is "click farms", which comprise a large number of low-paid workers who click on links or posts. "Click farms" allow "click farm masters" to sell things like video views, "likes" and even votes. One can buy one million Instagram "likes" for only US$18, 1,000 WeChat "likes" for US$0.19, and 500 re-tweets for US$2. There are also content marketing services, which offer fake news articles for as little as US$15 to US$30 for 500 to 1,500 words.

2. The Select Committee also identified several reasons for why online falsehoods, including falsehoods spread by foreign actions, are much easier to propagate and cost much less than on traditional media.

3. First, on social media, information is often shared amongst peers without verification of content or source. An online falsehood can be created simply by typing out some text online, or swapping the caption of a video or photograph. It could then easily find a believing audience on social media. Fabricated articles or misleading headlines may also take advantage of how information appears to Internet users. Even satire may be more difficult to identify when read off a social media feed, according to Dr Wardle. During the 2017 French Presidential Election, CrossCheck, a fact-checking project, found that people were disseminating falsehoods masquerading as satire to avoid fact-checks.

4. Second, consumer-friendly tools for creating audio-visual online content are readily available. Such tools have allowed relatively unskilled users to manipulate and distort visual media in ways that are very difficult to detect, according to various representors, including computer scientist Dr Hany Farid from the US (Professor & Chair, Computer Science, Dartmouth College).

5. For example, representors drew attention to free artificial intelligence tools that can convincingly simulate actual people to deliver messages that are not from the apparent sender, as well as easy-to-use software for editing and creating audio. There are already applications which allow users to feed a computer image and audio of a person to teach it to imitate that person's voice. There are video tutorials online to teach one how to use such applications. Such software can make it relatively easy to transpose a picture of one person on an existing video to create a fake video (known as a "deepfake"). A Financial Times article described how such "deepfakes" can be easily used to put words and expressions on the face and mouth of a politician and influence elections. One New York Times reporter said that creating a "deepfake" cost him less than US$100.

6. Third, online platforms such as websites and blogs can be created at relatively low cost. Purveyors of falsehoods can easily masquerade as genuine reporting outlets. For example, a website was created to mimic a genuine South African news site, and spread the false claim that South African President Jacob Zuma had resigned. This triggered a brief spike in the value of the South African rand. In Singapore, a student created a fake copy of a government website, and posted the fake announcement that Mr Lee Kuan Yew had passed away. Established international news outlets fell for the hoax and reported it to an international audience.

7. These low-cost and user-friendly methods can rival or exceed the influence of traditional media. A simple splicing edit to a video of then-incumbent Jakarta governor Basuki Tjahaja Purnama (popularly known as "Ahok") made it seem that he had committed blasphemy. This fuelled rallies involving hundreds of thousands of people, and protests that turned violent. In the US, doctored photographs were used to accuse the police of setting fire to a protestors' campsite, inflaming sentiments against the police.

(2) Hostile Information Campaigns Targeting Democratic Processes

1. Based on a survey of 2,948 US adults in March and April 2018, Stanford University researchers found that "foreign involvement provoked public disapproval, which increased with the level of intervention… voters who learned of foreign interference were much more likely to distrust the results of the election and lose faith in US democracy". Examples of elections that had been attacked by foreign state actors are as follows:

2. **2021 German Elections.** The German Foreign Ministry reported in Sep 2021 that Russia launched cyber-attacks on German politicians to gain access to their personal emails. These accusations came after a warning by the German domestic intelligence agency BfV in Jul 2021 that a Russia-linked threat actor group, Ghostwriter, had been targeting private email addresses of German Members of Parliament and regional legislators since at least Feb 2021. The German and Polish governments linked Ghostwriter to the Main Intelligence Directorate of the General Staff of the Armed Forces (GRU), who had been known to support influence operations by exfiltrating and leaking information from targeted political entities. Observed tactics used by Ghostwriter include leveraging compromised websites, predominantly news outlets, to disseminate fabricated content, such as fake news articles, quotes, correspondences and other documents.

3. **2020 US Presidential Elections.** The US Intelligence Community published a declassified report on foreign interference in the 2020 elections, revealing that Russia and Iran had conducted influence operations to sway votes. The report found that "a key element" of Russia's strategy was its use of proxies linked to Russian intelligence to push narratives – including "misleading or unsubstantiated allegations against President Biden" – to US media organisations, US officials, and prominent US individuals, including some close to former President Trump and his administration. Russian proxies advocated for formal investigations into alleged corrupt links between President Biden's family and Ukraine, and even released audio recordings to implicate President Biden. The report also said Iran carried out a "multi-pronged covert influence campaign" against Trump. Without directly promoting his rivals, it undermined public confidence in the electoral process and US institutions, and sowed division and exacerbated societal tensions in the US.

4. **2017 French Presidential elections.** A French Government report in Apr 2018 found an attempted Hostile Information Campaign (HIC) targeting then-candidate Macron, even though the report found that it did not succeed in interfering with the election or antagonising French society. The report highlighted American alternate-right trolls supporting Macron's far-right opponent Marine Le Pen, and a hack-and-leak campaign spreading a rumour that Macron had a secret offshore account, prior to the final televised debate between Macron and Le Pen. Phishing attacks were also carried out with email spoofing targeting Macron and his party members, and these documents were leaked hours before campaigning stopped for a "cooling off" period before voting. In addition, Dr Kevin Limonier provided evidence to the Select Committee about a HIC perpetrated via Russian media outlets, social media platforms and bots. He identified four methods: (1) Russian outlets spread grand narratives that cast the Western world as hegemonic and Russia as a champion of free-thinking and multi-polarity. This was supported by selectively edited content using information that could discredit the US, EU or NATO; (2) Use of social networks to target different groups; (3) Manipulation of social media to gain visibility of content, such as 'click-bait' articles; (4) Bots and trolls to relay or interact with the online content of Russian media outlets.

5. **2017 Federal German Elections.** A Political Data Science Team at the Technical University of Munich highlighted the presence of a disinformation campaign conducted by a foreign state and the alt-right from the US. Further, evidence provided by Mr Ben Nimmo at the Select Committee highlighted that a foreign 'Botnet' was active during the election campaign. Mr Nimmo noted that this botnet had formerly retweeted Russian-language commercial content (such as car advertisements and Bitcoin) and began retweeting posts supporting the anti-migrant AlternativeforGermany (AfD) close to the elections. Moreover, Buzzfeed news reported in 2017 that a foreign hacker linked to a network of Twitter bots revealed that he and thirty other people in his country "had been using bots to promote messages favourable to the AfD during the election" and they offered this service for free.

6. **2016 Brexit referendum and 2017 UK General Elections.** During Brexit, various studies found the use of fake social media accounts and mobilisation of online trolls to propagate messages in support of the Leave campaign. A study by Swansea University found evidence suggesting that more than 150,000 foreign-linked accounts tweeted over 45,000 pro-Brexit messages in the last 48 hours of the campaign. Researchers from the University of Edinburgh analysed Twitter data and found 3,485 tweets from 419 of the accounts listed as Internet Research Agency accounts, which specifically discussed Brexit and related topics such as the EU and migration. In addition, during the UK General Election in 2017, a false BBC article was spread, and it claimed that the elections would be held over two days, and instructed supporters of selected parties to vote on the real election day and supporters of other parties to vote on the fake election day.

Note: The examples cited in the Annexes are based on open-source reports, or through testimonies provided at the Select Committee on Deliberate Online Falsehoods (which are then attributed to the representator), and are not MHA's comments.

Annex E: Example of Macedonian Troll Farm Cottage Industry

1. The Select Committee received testimony about troll farms in Macedonia having created fabricated and highly partisan "news" stories during the US Presidential elections to earn money from advertising (although it is unclear if these farms were serving state-sponsored ends).

2. Representors at the Select Committee shared that teenagers in a Macedonian town had created fake news, and one of the teenagers reportedly earned US$16,000 in ad-revenue from two pro-Trump websites, which is many times the average monthly salary in Macedonia (US$371).

3. Buzzfeed reported in Nov 2016 that in the final weeks of the 2016 US Presidential elections, over 140 "fake news" US politics websites were traced to Macedonia. Another Buzzfeed News Analysis article in Nov 2016 reported that based on the top 20 election stories in terms of Facebook engagement in the final 3 months of the elections, the fake news sites have more engagements than mainstream news. Two false election stories from Macedonian sites made it into the top-10 list of stories in terms of Facebook engagement.

4. CNN also reported in 2000 that there were dedicated classes training young Macedonians on how to set up and operate fake websites that targeted foreign users. Mirko Ceselkoski, whom CNN dubbed a "clickbait coach", was reported to have told his students that they would earn at least 1000 Euros a month (compared to an average monthly income of 480 Euros), and around 100 of his pupils were operating US political news sites.

Note: The examples cited in the Annexes are based on open-source reports, or through testimonies provided at the Select Committee on Deliberate Online Falsehoods (which are then attributed to the representator), and are not MHA's comments.

Annex F: Past Discussions and Publications on Foreign Interference over Last Three Years

(1) Testimonies by representators at Select Committee on Deliberate Online Falsehoods

The Report of the Select Committee and written representations can be found on www.parliament.gov.sg/sconlinefalsehoods.

Summary of testimony by Dr Gulizar Haciyakupoglu (Research Fellow, RSIS)

[Representations were given behind closed-doors due to sensitivity]

- Disinformation campaigns have become more sophisticated with disruptions in technology and media ecology and changes in news consumption habits.
- Said that states who mount campaigns have an unrestricted approach to warfare.
- Gave a specific example of a country who had taken efforts to infiltrate another through several methods, including disinformation campaigns, psychological weakening, manipulation of public opinion and tactical campaigns. The country had (a) manipulated the media and used media professionals and content creators, (b) spread influence with the help of businessmen, students, academics and other groups, and (c) carried out cyber-attacks with the help of civilians. As a result, the target had been thoroughly penetrated even though it had taken some countermeasures.
- Said there had been a number of occasions when Singapore had been subjected to cyber-attacks in the recent past, including attacks on sensitive ministries.
- Described indicators of information warfare carried out against Singapore.

Summary of testimony by Dr Michael Raska (Assistant Professor, RSIS)

- Observed that a sophisticated State actor can employ non-State actors as proxies in cyber space and information operations.
- Such non-state actors can include state-sponsored media of a foreign country, business or clan associations.
- Considering Singapore’s conventional military strength, foreign States who cannot challenge Singapore through conventional warfare will engage in subtle information campaigns that target the friction points in Singapore society, weakening Singapore and undermining Singapore’s will to defend itself. This form of asymmetric warfare may offset a foreign State’s military inferiority and achieve political aims similar to conventional warfare.
- Recommended for Singapore to study the nature of the evolving strategic competition in East Asia.
- Observed that more governments, intelligence agencies, military organisations as well as non-state actors were investing in cyber / information warfare capabilities; future conflicts – particularly in East Asia - will be increasingly linked with confrontations in cyber space such as cyber-attacks on physical systems and processes controlling critical information infrastructure, information operations, and various forms of cyber espionage. The resulting “cyber-kinetic conflicts” will evolve parallel with technological changes – e.g. the introduction of next generation robots, artificial intelligence, and remotely controlled systems will continue to alter the character of future warfare.
- Said that the character of hybrid conflicts in the regional “gray zones” may also reflect low-level intensity conflicts in “peripheral information/influence campaigns”, rather than high-level conflicts. Under this changing character of conflict, he said Singapore and the SAF will likely have to redefine its objectives necessary to achieve “victory”.

- Highlighted the strategic significance of the progressive complexity of cyber threats, which are increasingly blurring distinctions between civil and military domains, state and non-state actors, principal targets and weapons used. Online activities and behaviour will have increasingly offline consequences, and vice-versa.

Summary of testimonies by others

S/N	Representor	Summary of Representations
1.	Dr Shashi Jayakumar (Head, Centre of Excellence for National Security, RSIS)	• Cautioned it would be a mistake to assume that foreign state-led disinformation was not already happening here. • Highlighted that rumours and untruths carried by foreign-linked bots and fake ads had supported and inflamed all sides of the political spectrum in the US. • Shared that there was an online "army" of content creators based in an Asian country, whose role is to promote their government's policies and attack criticisms of those policies, both within and outside their own country. • Described how individual "consultants" and private sector entities specialised in hacking or interfering with elections with the aim of achieving the desired election result for the client, including one Andreas Sepulveda in Latin America whose methods included hacking, smear campaigns, disinformation and subversion.
2.	Assistant Professor Liew Kai Khiun (Wee Kim Wee School of Communication and Information, NTU)	• Shared that seemingly Myanmar-based social media accounts had posted about articles on the Rohingya issue written by Singapore's mainstream media, and suggested that Singapore's mainstream media is a "Muslim media" and that Rohingyas do not exist in Myanmar. Some of these comments had Islamophobic tones and incited backlash from Singapore Muslims. • Explained that foreign influences seek to exploit and magnify existing social divisions.
3.	Mr Benjamin Ang (Senior Fellow, RSIS)	• States can use non-state actors to spread falsehoods, and non-state actors can include state sponsored media of a foreign country, business or clan associations. NGOs that may be infiltrated by the foreign country, political parties that may have the same view or have been infiltrated by the foreign country, academics who may be agents of influence for the foreign country, as well as organised or volunteer groups of civilians. • Highlighted the limitations of other countries' legislation in responding to state-level attacks (e.g. they are more effective in taking post-hoc actions, can be circumvented).
4.	Dr Damien Cheong (then-Research Fellow, RSIS)	• Identified public institutions in Singapore as a potential target of disinformation operations. [Representations were given behind closed-doors due to sensitivity]

S/N	Representor	Summary of Representations
5.	Mr Ruslan Deynychenko (one of the founders of StopFake)	• Highlighted that foreign disinformation campaigns aim to weaken a country, reduce its ability to resist foreign aggression, change its foreign policy, and create conditions for its inclusion in a foreign country's sphere of influence. • Shared that in Ukraine, news sources from a foreign state spread disinformation targeting local divisions and motivating citizens of that foreign State to fight Ukrainian forces in Eastern Ukraine. • Shared about a foreign state's disinformation operations in Eastern Europe.
6.	Mr Nicholas Fang (Managing Director, Black Dot Pte Ltd)	• Highlighted that influence operations can be instigated by larger, more powerful nations who have at their disposal a full range of information tools. • They typically feed on a society's vulnerabilities and fragilities, seek to amplify areas of doubt and unhappiness, and perpetuate falsehoods voluminously and at great speed through the use of media and technology.
7.	Mr Jakub Janda (Head, Kremlin Watch Program; Director, European Values Think-Tank)	• Shared that a foreign state had influenced extremists and fringe politicians in the Czech Republic to share and spread propaganda and disinformation. There were also online networks that normalised fringe views among the Czech citizens. This resulted in the public losing trust in the media and public institutions, and forming skewed views of Ukraine that then undermined the Czech government's diplomatic relations with Ukraine.
8.	Associate Professor Kevin Limonier (French Institute of Geopolitics)	• Gave evidence of a HIC perpetrated via foreign media outlets, social media platforms and bots. This comprised four methods: (1) Foreign-owned news outlets spread grand narratives based on selective editorial content. (2) Use of social networks to target different groups. (3) Manipulation of social media to gain visibility of content. (4) Bots and trolls amplified online content of Russian media outlets.
9.	Mr Andrew Loh (self-investor)	• Raised concerns that deliberate online misinformation during the 2016 US Presidential Elections could give rise to concerns about the integrity of public institution and democratic processes. • Even powerful and resourceful countries are not immune.
10.	Assistant Professor Elmie Nekmat (Department of Communications and New Media, NUS)	• Noted that between 2015 and 2017, 9,097 posts linked to an agency with links to a foreign State, were found to have manipulated Americans' opinions about pipelines, fossil fuels, fracking, and climate change. • Observed that nearly 17 million Twitter posts were shared within 10 days of the 2017 French Presidential election, indicating the use of artificial methods of propagation such as Bots. In addition, the user accounts that engaged with "MacronLeaks" mostly belonged to foreigners with pre-existing interest in alt-right topics and alternative mews media.
11.	Mr Ben Nimmo (Senior Fellow, Information Defense Digital	• Shared how the Internet Research Agency (IRA) starting in 2014 sough to use the Black Lives Matter (BLM) movement to widen the divide between the African-American community and the police, as well as to undermine the institution of the police, and how the posts by the IRA sought to push both sides.

S/N	Representor	Summary of Representations
	Forensic Research Lab)	- Shared various incidents of foreign disinformation campaign during the 2016 US Presidential elections (e.g. 'Pizzagate' conspiracy, false US personas created by the IRA) - Shared about the increasing involvement of non-state foreign actors participating in foreign disinformation efforts, such as Macedonian teenagers who created fabricated and highly partisan "news" stories during the 2016 US Presidential elections for revenue. - Shared that a foreign 'Botnet' was active during Germany's election campaign, and this botnet had formerly retweeted Russian-language commercial content (such as car advertisements and Bitcoin) and began retweeting posts supporting the anti-immigration AfD close to the elections.
12.	Mr Septiaji Eko Nugroho (Founder, Mafindo/Indonesian Anti-Hoax Community)	- Cautioned that Singapore is particularly vulnerable to foreign disinformation operators as English is widely spoken.
13.	Ms Nataliia Popovych and Mr Oleksiy Makhuhin (Ukraine Crisis Media Centre)	- Described how disinformation from a foreign State had targeted the Ukrainian Armed Forces. - Explained that vulnerable groups (e.g. pensioners and people living in poverty in the Ukraine) were especially vulnerable to foreign disinformation.
14.	A/P Eugene Tan (SMU School of Law)	- Highlighted that foreign disinformation campaigns exploit existing societal fault lines (e.g. the alleged foreign meddling in the US could make headway due to the deep internal rifts and political alienation among Americans).
15.	Mr Thiruprakassh S/O Suppiah (Manufacturing Manager)	- Shared how, soon after the London terror attacks of 2017, social bots controlled by foreigners spread a post containing a picture of a Muslim woman, claiming that she was walking past a dying man. This carried the hashtag "BanIslam".
16.	Mr Norman Vasu (Senior Fellow, Centre of Excellence for National Security, RSIS)	- Shared about active disinformation-for-hire industry in Macedonia.
17.	Mr Carlos Nicholas Fernandez (Technology Entrepreneur)	- Shared that one of the Macedonian teenagers reportedly earned $16,000 in ad revenue from two pro-Trump websites.
18.	National Council of Churches of Singapore	- Submitted that "fake news" can be used by a foreign government to interfere with the domestic affairs or elections of another country.

Note: The examples cited in the Annexes are based on open-source reports, or through testimonies provided at the Select Committee on Deliberate Online Falsehoods (which are then attributed to the representator), and are not MHA's comments.

(2) Past Discussions in Parliament

S/N	Speech	Summary of Key Points
1.	PQ on Foreign Interference in Singapore Elections Reply by Minister (PMO) Chan Chun Sing *Sep 2017*	**Miss Cheng Li Hui** asked the Prime Minister (a) whether there is any risk assessment made by the Government on our vulnerability to foreign interference in our elections from both state and non-state actors; (b) what are the measures in place to safeguard Singapore from foreign interference in our elections; (c) what are the security guidelines on vigilance by political parties and candidates on this issue; and (d) how can the social media be kept free and open for political discussions whilst dealing with malicious/subversive content. <u>Reply</u> • Singapore's small size, openness and relative short history makes it challenging for us to mitigate the external influences on our systems. The advent of modern technologies, proliferation of various media platforms, rapid communication cycles and seamless information transmission channels combine to further complicate our task of defending ourselves. • Our consistent position has always been that politics in Singapore is meant only for Singaporeans. Measures include: ○ Prohibiting foreigners from taking part in election activities: ▪ PDA prohibits election candidates and political parties from accepting foreign funding. ▪ Under the Societies Act, only Singaporean citizens can be members of political associations, and these associations must not have affiliation or connection with any organisation outside of Singapore that is contrary to our national interest. ○ Protect Government networks and IT systems, so that they are not used by others to subvert our election process. ○ Prevent foreigners from manipulating our media platforms, to influence local politics (i.e. Newspaper and Printing Presses Act, Broadcasting Act). ○ Education programmes, such as Better Internet, and the Source, Understand, Research and Evaluate programme, or SURE.
2.	PQ on Proposal for Legislation to deal with Foreign Interference of Singapore's election and politics	**Miss Cheng Li Hui** asked the Prime Minister (a) what can Singapore learn from the various incidences of foreign interferences in the elections and politics of countries such as the US, Australia, France and Germany; and (b) whether there is a need to introduce new laws or further strengthen existing laws to deal with foreign interference and Singaporeans who work with foreign actors to influence Singapore's elections and politics.

S/N	Speech	Summary of Key Points
	Reply by SMS (Law) Edwin Tong *Feb 2019*	• The Internet and social media have created a new, vast and easy playing field for foreign interference. Clandestine and sophisticated tactics were used to fracture social cohesion and influence election outcomes, through the spread of disinformation and half-truths, and exploitation of sensitive issues. • Examples: o 2016 US Presidential Election ▪ A foreign organisation used fake social media account to create social media groups on controversial issues. ▪ Researched fault lines in American society and politics, and drove wedges along these lines ▪ Used bots and digital advertisements to amplify its reach and viewpoints rapidly, to give the impression that they were popular. ▪ Aim of this hostile information campaign included longer term objectives to undermine American democracy and institutions. o Brexit Referendum ▪ A steady stream of anti-immigration falsehoods by foreign-linked social media accounts made people feel threatened, and built a narrative of a British government that was failing to protect its citizens. o 2017 French Presidential Elections ▪ Hacked data from presidential candidate Emmanuel Macro's campaign were leaked online, shared and retweeted o Netherlands – HIC sought to undermine support for an EU-Ukraine trade agreement in 2016 o Germany – Lisa Case o Ukraine • Another form of interference involves influencing those involved in domestic political discourse through funding and donations. Examples: o Australian senator resigned after it was revealed that he had received donations from a foreign political donor, and advocated for the foreign state's position on a sensitive issue, contradicting his own party's official position o New Zealand – an opposition leader allegedly circumvented political donation laws by disguising a donation made by a businessman linked to a foreign government • Singapore is especially vulnerable, so we are developing a strategy on two fronts: (i) sensitise Singaporeans to the threat and nurture a discerning public; (ii) update and enhance our

S/N	Speech	Summary of Key Points
		legal framework. On the latter, the new legislation must enable us to act swiftly and effectively to disrupt and counter false, misleading and inauthentic information and narratives spread by foreign actors. It must also be able to pre-emptively expose clandestine foreign interference campaigns. **Supplementary question: (i) instances of foreign interference in Singapore, (ii) gaps in laws.** • Examples of foreign interference in Singapore: o Eastern Sun and The Singapore Herald. o Huang Jing. o SingHealth hacking. Cyber hackings are often deployed in concern with hostile information campaigns to search for information that can be weaponised. o Malaysia – "In December last year, when bilateral issues with our immediate neighbour were at the top of the news, we noticed that a curious spike in online comments on social media made from avatar accounts – essentially anonymous accounts with profile pictures that do not show the owner's face. Many of these comments were critical of Singapore. On one such issue, jams at land checkpoints. Around 40% of the comments on alternative media outlets' pages on social media came from avatar accounts. We do not know who these suspicious accounts belong to nor do we know if they are being coordinated by foreign actors. But it is clear that these accounts had sought to give and create an artificial impression to netizens of the opposition to Singapore's position, at a time of heightened bilateral difficulties." • On 2nd question, Select Committee recommended that Govt consider measures to address both deliberate online falsehoods and state-sponsored campaigns that threaten national security. Govt will consider legislation in both these areas.
3.	Minister for Home Affair's speech at COS 2019 *March 2019*	• The government has been studying how other countries have dealt with foreign interference. Several countries have passed laws to combat both falsehoods and foreign interference: o Germany – Network Enforcement Act o Australia – stiff penalties, complete ban on foreign donations, disclosure. • To combat the threat of foreign interference, our current thinking is that early detection and exposure is critical. • We must be able to act quickly and keep up with new digital-age tactics.

S/N	Speech	Summary of Key Points
		• Apart from strengthening our laws, we have to build up the ability of Singaporeans to understand what is happening, to discern, to respond appropriately, and to try and resist foreign interference. We must train people to spot it but it is a reality that many people will find it difficult. • Some of these steps require legislation.
4.	Speech by Minister for Law and Minister for Home Affairs, Second Reading of the Protection from Online Falsehoods and Manipulation Bill *May 2019*	• The use of falsehoods can come from several sources, including (i) foreign countries using information warfare, (ii) profit-driven actors, (iii) deliberate actors, for political ends, and (iv) people with prejudice, seeking to harm other groups. • Foreign countries may seek to conduct information operations to target and create internal opposition as a "permanently operating front" throughout the target country. These non-kinetic military measures, in many cases, can exceed the power of force and weapons (Gerasimov Doctrine). • Supported by evidence from Select Committee: o Dr Shashi Jayakumar – in modern information warfare, "seeding internal opposition within the target country is extremely important". o Dr Berzin (national security expert from Latvia) – notion of broken social contract is the main vulnerability exploited by foreign adversaries. • Singapore is a specific and vulnerable target for information warfare because of our military superiority in the region. This drives militarily weaker country to focus on other means to weaken Singapore, sap our will from inside, create deep internal divisions and keep us in a permanent state of internal dissension. o Select Committee has given evidence that this is already happening. o Government knows this is happening, even if we don't come out in public to say it openly. "It is happening to sap people's support for the SAF, for defense, to try and shift Singapore's foreign policy as well". • Overseas examples of information campaign conducted by foreign countries: o Ukraine – "a foreign country … exploited falsehoods to build a narrative that the Ukrainian government was fascist and corrupt. It spread online falsehoods about atrocities being carried out against a particular country in Ukraine". o Czech Republic – "disinformation operation by a foreign country was used to turn domestic sentiments in favour of a foreign State's geopolitical goals". Key message: US

S/N	Speech	Summary of Key Points
		was responsible for influx of Syrian refugees into Europe. o Germany – Lisa Case. Foreign media outlets reported widely on a fabricated claim by a girl that she had been assaulted by three Middle East migrants. o Sweden – Swedish defence agency said false information about subjects such as NATO, immigration, terrorist, are spread on a daily basis in Sweden. • Foreign actors may also seek to conduct information operations to create alternate realities. o During the Brexit referendum, fake foreign-linked accounts posted more than 45,000 fabricated messages about Brexit, in the 48 hours during the referendum. o A sophisticated foreign information campaign sought to influence the outcome of the 2016 US Presidential Election, undermine democratic institutions, and democratic ideals. Foreign agents infiltrated, exploited alt-right movements using fake social media accounts. They pretended to be real Americans and amplified the falsehoods that originated on these websites. • Tools to spread falsehood: (i) fake accounts, (ii) digital advertising, and (iii) algorithms used by platforms to rank content. o Fake accounts: ▪ 2016 US Presidential Elections – a foreign troll factory conducted a disinformation campaign using 50,000 bot accounts, over 3,800 fake Twitter accounts, and at least 470 fake Facebook accounts. o Digital advertising: ▪ In the US, foreign operatives used $100,000 to spread Facebook advertisements to 126 million Americans in the 2016 US Presidential Election
5.	Speech by Minister for Home Affairs - RSIS Conference on Foreign Interference Tactics and Countermeasures *Sep 2019*	• Foreign interference is age old. Examples include: Spread of rumours to undermine standing of a military leader in a rival state during the Warring State Period in China (300BC); Roman intervention in Archean League (200BC). • Interference is a given in international relations. It takes a variety of forms: o Diplomatic channels. Both legitimate and non-legitimate (e.g. Hendrickson Affair). "It's one thing to link up with politicians of all shapes and partisan views – diplomats are entitled to that. It's quite another to try and set up political organisations, encourage citizens to take part in political processes, compete in elections,

S/N	Speech	Summary of Key Points
		and offer funding and asylum. That, I think, crosses well beyond the bounds of normal diplomatic activity.” o Covert agents of influence under the control of intelligence agencies. Examples: Huang Jing, Australian senator. o Media – key node to exert influence over domestic public opinion, through funding and control of publications, or having agents use the cover of journalist themselves. Examples: (i) CIA funded Congress for Cultural Freedom during the Cold War while Soviets manipulated journalists and publications; (ii) newspapers in Australia, New Zealand. Local example – Singapore Herald and Eastern Sun. o NGOs. States have been known to target cause-based movements in other states – e.g. Soviets used this to boost anti-nuclear movement in Europe in the late 1970s and early 1980s. • Internet has turbo-charged and revolutionised foreign interference o Gerasimov Doctrine: “The ‘Rules of War” have been redefined, such as using non-kinetic measures such as Hostile Information Campaigns (HICs). What they can do is to identify what they call ‘protest potential’ of any population of a target country, then create protests, deepen divisions and increase hostility among the different groups, and get them to distrust institutions. In that country, trust in institutions and systems get damaged, and the people lose faith in democracy as a whole” o Tap on legitimate sentiments; convert disinformation into mainstream information. o Actors exploit fault-lines on hot-button issues. Example: “Blue Lives Matter” as a response to “Black Lives Matters” in the US, stirred by foreign agency o The internet has made HICs cheap, easy and effective to mount. • Example: Ukraine o Mr Ruslan Deynychenko gave evidence at the Select Committee that a foreign country had built a narrative against Ukraine that the Ukrainian government was fascist and corrupt. A combination of online and offline methods was used to distribute and amplify these narratives. • Local example of nascent attempts at foreign interference: o PJ Thum and a group of activists met Dr Mahathir (then Prime Minister) and urged him to bring democracy to Singapore. Thum and Kirsten Han set up New Naratif,

S/N	Speech	Summary of Key Points
		which is significantly funded by a foreign foundation and received other foreign contributions. o The Online Citizen (TOC) uses foreigners to write exclusively negative articles on Singaporean social and political matters. Only five of the 14 admins are located within Singapore. • The State cannot take a hands-off approach. The serious impact of HICs on the social fabric, on political sovereignty, on peace, on stability, and on national security has to be addressed by states, working with tech companies. o Every country has the sovereign right to decide for itself how it will protect our national security interests o Tech companies cannot be left to self-regulate. Their business model does not incentivise self-regulation. The more users, the more content there is on their platform, the more user attention they can sell to advertisers, the more their profits. Regulating will involve costs. • Other countries have introduced new legislation: o France – Information Manipulation Law o Germany – Network Enforcement Act o Australia – Restrictions on political donations, stronger espionage laws, tougher penalties, and a requirement that agents or lobbyists who represent foreign nations or entities must register their interests o Israel – transparency requirements for NGOs receiving more than half their funding from foreign sources • We need legislation to deal with HICs. POFMA does not deal with HICs, because HICs don't just depend on falsehoods.
6.	PQ on Assessment of Security Risk faced by Singaporean individuals, firms and media organisations Reply by Minister for Home Affairs *Sep 2019*	**Ms Anthea Ong** asked the Minister for Home Affairs (a) what are the criteria used to determine whether Singaporean individuals, firms, or media organisations are at risk of being compromised by foreign influence for national security reasons; (b) whether a list of such individuals or organisations at risk, and the reasons for these risks, will be published; and (c) whether positions that involve media, communications, or outreach, that address issues of social or political concern should be staffed exclusively by Singaporeans due to the risks of foreign influence. **Assoc Prof Walter Theseira** asked the Minister for Home Affairs (a) what are the facts behind the concerns expressed at the recent Foreign Interference Tactics and Countermeasures Conference that certain activists and media persons are potential agents of foreign influence; and (b) how can Singaporeans protect themselves against foreign influence given that association with and receiving income from foreign sources is common amongst globalised Singapore firms and individuals.

S/N	Speech	Summary of Key Points
		• We are unable to identify a specific criteria for individuals, firms and organisations that are at risk of being compromised by foreign influence. It really depends on what is actually done, what actually happens. We have not published a list of individuals and organisations that are deemed at risk. Not possible to make a comprehensive list. • On whether some positions should be staffed exclusively by Singaporeans, there are specific jobs that already have requirements for security clearance.
7.	**Speech by the Second Minister for Home Affairs, Committee of Supply Debates 2021** *March 2021*	• The threat of foreign interference has always been present. But in recent times, it has risen in potential and severity because of the increasing ease to carry out such operations. o Globally, cases of cyber-enabled foreign interference in elections increased from seven between 2011 and 2015, to 41 between 2016 and 2020. o We have also seen reports from Australia and other countries that foreign powers and their agents attempted to influence their politics by buying off political parties and politicians. • Singapore needs to be open to the world to make a living. But our diversity and openness also present opportunities for foreign actors. Example of local foreign interference operations: Eastern Sun and Singapore Herald in 1970s; spike in online comments critical of Singapore during the bilateral issues with our immediate neighbour in 2018 and 2019. “Many of these comments came from anonymous accounts, which sought to give an artificial impression that there were significant and fundamental objections to Singapore's position”. o No signs of foreign interference at the 2020 Parliamentary Elections • To address the threat of foreign interference, we must build up Singaporean’s ability to discern legitimate and artificial online discourse, and respond appropriately. Legislative levers are also necessary, as it is not enough to have a discerning public. • We need legislative levers to obtain information to investigate hostile information campaigns to determine if they are of foreign provenance or artificial, to break the virality of such campaigns, and carry counter-messaging to alert Singaporeans. We also need to consider further measures to guard against foreign subversion of politically significant individuals and entities.

(3) Media Coverage on Foreign Interference

S/N	Date	Event	Headlines and Key Points (Articles are in respective folios)
2019			
1.	Feb 2019	SMS Edwin Tong's PQ reply on Foreign Interference (FI) (Feb 2019)	• **Spike in online talk critical of S'pore during spat with KL (Straits Times)** • **Laws to be introduced this year to give Government greater power to stop falsehoods (ZB)** • **Steps taken to counter online threats (TNP)** • **Curious critics on social media is one of the ways foreigners influence Singaporeans (BH)** • **Singapore to set legislation to stop fake information (WB)** Various news outlets provided a factual report of SMS Edwin Tong's PQ reply, and captured the key point that the government was looking at introducing new laws to counter the threat posed by foregin interference and falsehoods.
2.	Feb 2019	Commentary on FI following PQ reply by CNA	• **Commentary: What next as the Government looks beyond disinformation in targeting foreign influence in Singapore (CNA)** This article mentioned that government needed to identify ways to deal with foreign agents, foreign funding and hacks.
3.	March 2019	Minister for Home Affair's COS Speech	• **Stronger laws planned to combat foreign interference (ST)** • **Singapore to have legislation to combat increased risk of foreign interference (ZB)** • **Early detection exposure key to tackling foreign interference in digital era (BH)** • **Laws to be strengthened (TM)** • **Early detection, exposure key to tackling foreign interference in domestic politics: Shanmugam (CNA)** Various news outlets provided a factual report of Minister's COS speech, which highlighted the need to combat foreign interference by introducing new laws.
4.	March 2019	Commentary on FI following COS Speech by CNA	• **CNA feature on tackling foreign interference in domestic politics (10pm, Broadcast)** CNA interviewed security experts and SPS Sun Xue Ling on foreign interference. SPS Sun said that foreign

S/N	Date	Event	Headlines and Key Points (Articles are in respective folios)
			actors masked their identities, and made use of socially and politically divisive issues to create social divide.
5.	June 2019	Interview with Fabrice Pothier, French political analyst and co-founder of the Transatlantic Commission on Election Integrity	• **Singapore vulnerable to foreign election influence: Expert (ST)** Article summarised an interview with Fabrice Pothier, who said that Singapore's multi-ethnic society and global dependency can be exploited by foreign actors to influence election results and policies.
6.	June 2019	ZB feature on FI	**Three articles on FI in ZB and WB** on what is foreign interference and measures undertaken by other countries to combat foreign interference.
7.	Sep 2019	Commentary on FI by Today	• **Defending Singapore against foreign interference (TODAY)** Article provided an overview on the threat of FI and why Singapore might be vulnerable. Written by Muhammad Faizal Abdul Rahman, a Research Fellow with the Centre of Excellence for National Security at RSIS.
8.	Sep 2019	RSIS Conference on Foreign Interference	• **Singapore needs laws to tackle foreign meddling in its affairs: Shanmugam (ST)** • **Minister cites past examples of foreign meddling (ST)** • **TOC hired foreigners to pen negative articles, says Shanmugam (ST)** • **Call to guard against threats by bridging societal divides (ST)** • **Tech can be used by govts to exert control, says experts (ST)** • **Experts look at measures to fend off foreign interference (ST)** • **Laws needed to counter foreign interference: Shanmugam (TNP)** • **TOC using foreign writers for negative articles: Shanmugam (TNP)** • **Shanmugam warns of foreign interference in Singapore; questions agenda, funding of The Online Citizen (CNA)** • **Government must lead fight against foreign interference, cannot rely on tech firms: Shanmugam (TODAY)** • **Shanmugam questions funding sources behind TOC, reiterates need for laws to curb foreign interference (TODAY)**

S/N	Date	Event	Headlines and Key Points (Articles are in respective folios)
			Various news outlets (including venular news outlets) provided a factual report of Min's speech and various discussions at the RSIS Conference on Foreign Interference.
9.	Sep 2019	Follow-up articles after the RSIS Conference	• **Be vigilant about foreign interference: Jayakumar (ST)** – Professor Jayakumar highlighted how social media has magnified the threat of foreign interference during the launch of his book, "Diplomacy" • **Be ready to counter foreign meddling (ST Editorial)** – ST editorial highlighted the threat of hostile information campaigns, why it is difficult to get tech companies to self-regulate, and how Singapore can counter this threat. ZB also published an editorial and commentary.
10.	Oct 2019	Follow-up articles after RSIS Conference	• **Singapore to look at 'entry points' of foreign interference when crafting policy: Sun Xueling (CNA)** – Reported on SPS Sun's points at a panel discussion after a CNA screening of their documentary on fighting FI. SPS mentioned that there were two types of foreign interference that we were concerned about: HICs and local proxies. • **Disinformation? Fight with openness and transparency** – Editorial by Han Fook Kwang ZB published a commentary, which received two replies, and a feature on FI.
11.	Nov 2019	PQ Reply on Assessing FI risks	• **Politics in Singapore should be for Singaporeans: Shanmugam (ST)** • **Bar foreigners from some jobs to prevent foreign influence? Look from the broader perspective: Shanmugam (TODAY)** Factual reporting of PQ. ZB and BH also reported on the PQ.
2020			
12.	Apr 2020	Joint Statement by MHA, CSA and Elections Department on	• **Trolls, bots and fake accounts among methods used to sway votes (ST)** • **Risk of foreign and cyber threats in next GE highlighted (ST)**

S/N	Date	Event	Headlines and Key Points (Articles are in respective folios)
		foreign interference for GE 2020	• **Parties advised to review and strengthen cybersecurity measures (ST)** • **Political parties urged to guard against foreign interference (TNP)** • **Political parties in Singapore advised about threat of foreign interference in elections, cybersecurity risks (CNA)** • **Political parties advised to protect against cyber threats and foreign interference ahead of GE (TODAY)** • **Similar articles in ZB, TM, and BH**
13.	June 2020	Commentaries on GE (mentions of FI)	• **What navigating a largely virtual GE entails (TODAY)** – highlighted threats in the digital realm • **Organising a fair and safe elections (ZB)**
14.	Aug 2020	MHA's Reply to TNP's query on FI during GE 2020	• **No foreign interference in recent General Election, but laws under review: MHA (TNP).** MHA added the risk of foreign interference will only increase in the future.
15.	Oct 2020	MHA's reply to ZB's query on the Registry for Foreign Disclosures	• **Religious associations must disclose foreign linkages (ZB)**
16.	Dec 2020	Meltwater report on foreign interference during GE 2020	• **Most foreign social media accounts commenting on GE2020 were not Internet bots: Analytics firm (ST)** • Similar report in TM
2021			
17.	March 2021	Second Minister for Home Affairs' speech at COS	• **Legislation to counter foreign interference in politics (ST)** • **Laws being considered to address harmful online content (ST)** • **Laws needed to counter foreign interference: Minister (TNP)** • **Legislative 'levers' may be needed to deal with hostile information campaigns, says Josephine Teo (CNA)** • **Government considering new laws against harmful online content; 'not every platform puts society's interests first', says Josephine Teo (TODAY)** • Similar reports in ZB and BH

(4) Online Publications on Foreign Interference

1. **Brookings Institute.** The Brookings Institute has a series of posts on 'Cybersecurity and Election Interference' which explores digital threats to American democracy, cybersecurity risks in elections, and ways to mitigate possible problems.
   https://www.brookings.edu/series/cybersecurity-and-election-interference/

2. **RAND Institute.** RAND Institute publishes a series on information efforts by foreign actors, and has an archive of publicly available and attributed data from known online information operations from public attributed to Russian and Iranian actors. Reports published include a report on foreign interference in the 2020 US Elections and the tools for detecting online election interference.
   https://www.rand.org/research/projects/truth-decay/fighting-disinformation/search/items/information-operations-archive.html

3. **Council for Foreign Relations (CFR).** The CFR publishes various articles and reports on the topic of influence campaigns and disinformation and maintains a quarterly Cyber Operations Tracker.
   https://www.cfr.org/influence-campaigns-and-disinformation

4. **Australian Strategic Policy Institute.** Based on a study by the Australian Strategic Policy Institute, there has been a significant uptick in foreign interference worldwide. Between 2015 and 2020, at least 38 elections and 6 referendums were impacted.
   https://www.aspi.org.au/report/cyber-enabled-foreign-interference-elections-and-referendums

5. **Oxford Internet Institute.** In Jan 2021, the Oxford Internet Institute (OII) released its 2020 report, which highlighted that in 2020:
   a. 81 countries used social media to spread computational propaganda and disinformation (note: this includes Governments spreading to its domestic audience)
   b. Between Jan 2019 to Nov 2020, Facebook and Twitter removed more than 317,000 accounts and pages, and almost US $10 million spent on political advertisements by cyber troops
   c. Private firms increasingly provide disinformation campaigns, such firms were found operating in 48 countries.
   d. In its 2019 report, OII identified 7 states that carried out foreign influence operations.

   https://www.oii.ox.ac.uk/news/releases/social-media-manipulation-by-political-actors-now-an-industrial-scale-problem-prevalent-in-over-80-countries-annual-oxford-report/

6. **RSIS's publication on Cases of Foreign Interference in Asia.** RSIS proposed a 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.
   https://www.rsis.edu.sg/rsis-publication/cens/cases-of-foreign-interference-in-asia/#.YVSab5pBw2w

Annex G: Examples of Foreign Agencies Using Legitimate-looking Fronts

1. **Funding 'legitimate' news channels**. A CNN Television report found that Russia's efforts to meddle in the 2016 US election was similar to its disinformation back in 1983. During the Cold War, the Soviets and the CIA secretly funded and controlled magazines and writers to sway public opinion. An example was the Congress for Cultural freedom – a covert propaganda front. The Soviets also launched secret influence campaign where they spread massive amounts of propaganda and disinformation through newspapers, magazines, television, radio, posters and other media forms. One of the most notorious examples was the AIDS disinformation campaign where the Russian intelligence service, KGB, spread news that AIDS was a product of secret US military research – playing into distrust in US institutions and rumours of biological warfare programmes in the US.

2. **Use of news and media outlets as a front**. At the Select Committee on Deliberate Online Falsehood, Mr Ben Nimmo cited the case where the First Russian TV reported the case of Lisa, a 13-year old Russian-German girl, who had gone missing and was raped by Arab migrants. The story turned out to be fake (the German police had established her whereabouts), but the Russian foreign media (including RT and Sputnik) continued to intensively report the case and alleged that the German police were part of a cover-up. These falsehoods accompanied with anti-immigration narrative in Germany then prompted protests on the streets by ethnic Russian Germans.

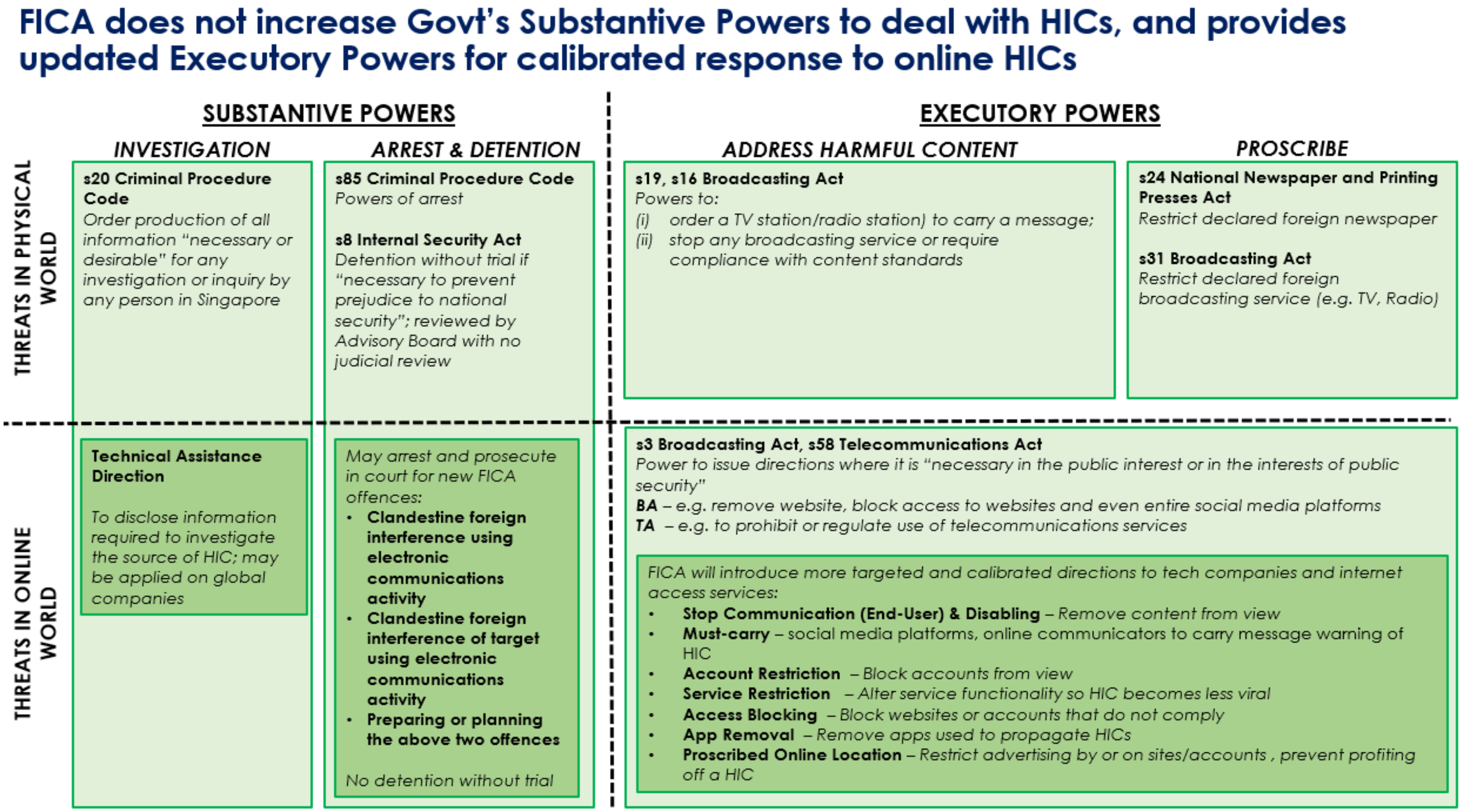
3. **Black Lives Matter movement – blending in with authentic content to increase legitimacy.** The Senate Intelligence Committee came out in Jun 2020 to warn Americans to be wary of state-sponsored and state-directed media platforms such as RT and Sputnik, as these Russian state-sponsored outlets heavily covered content that was intended to intensify social divisions on the issue of race after the death of African American George Floyd. For instance, African Americans were targeted with content highlighting incidents of Police brutality or racism by white Americans, using the hashtags such as #blacklivesmatter, #policebrutality – such content **blended in with authentic content from real Americans and represented an attempt to exploit on existing tensions within American society.** In addition, Mr Ben Nimmo had also given evidence to the Select Committee about the Russian-linked Internet Research Agency's efforts starting in 2014 to use the BLM movement to widen the divide between the African-American community and the Police, as well as to undermine the institution of the Police.

4. **2020 US Presidential Elections - using local proxies to advocate formal investigations, releasing convincing materials to convince the public.** The US Intelligence Community published a declassified report on foreign interference in the 2020 elections, revealing that Russia and Iran had conducted influence operations to sway votes. The report found that "a key element" of Russia's strategy **was its use of proxies linked to Russian intelligence to push narratives** – including "misleading or unsubstantiated allegations against President Biden" – to US media organisations, US officials, and prominent US individuals, including some close to former President Trump and his administration. **Russian proxies advocated for formal investigations into alleged corrupt links between President Biden's family and Ukraine, and even released audio recordings to implicate President Biden.**

Note: The examples cited in the Annexes are based on open-source reports, or through testimonies provided at the Select Committee on Deliberate Online Falsehoods (which are then attributed to the representator), and are not MHA's comments.

Annex H: Charts on Existing Powers and Updated Powers under FICA

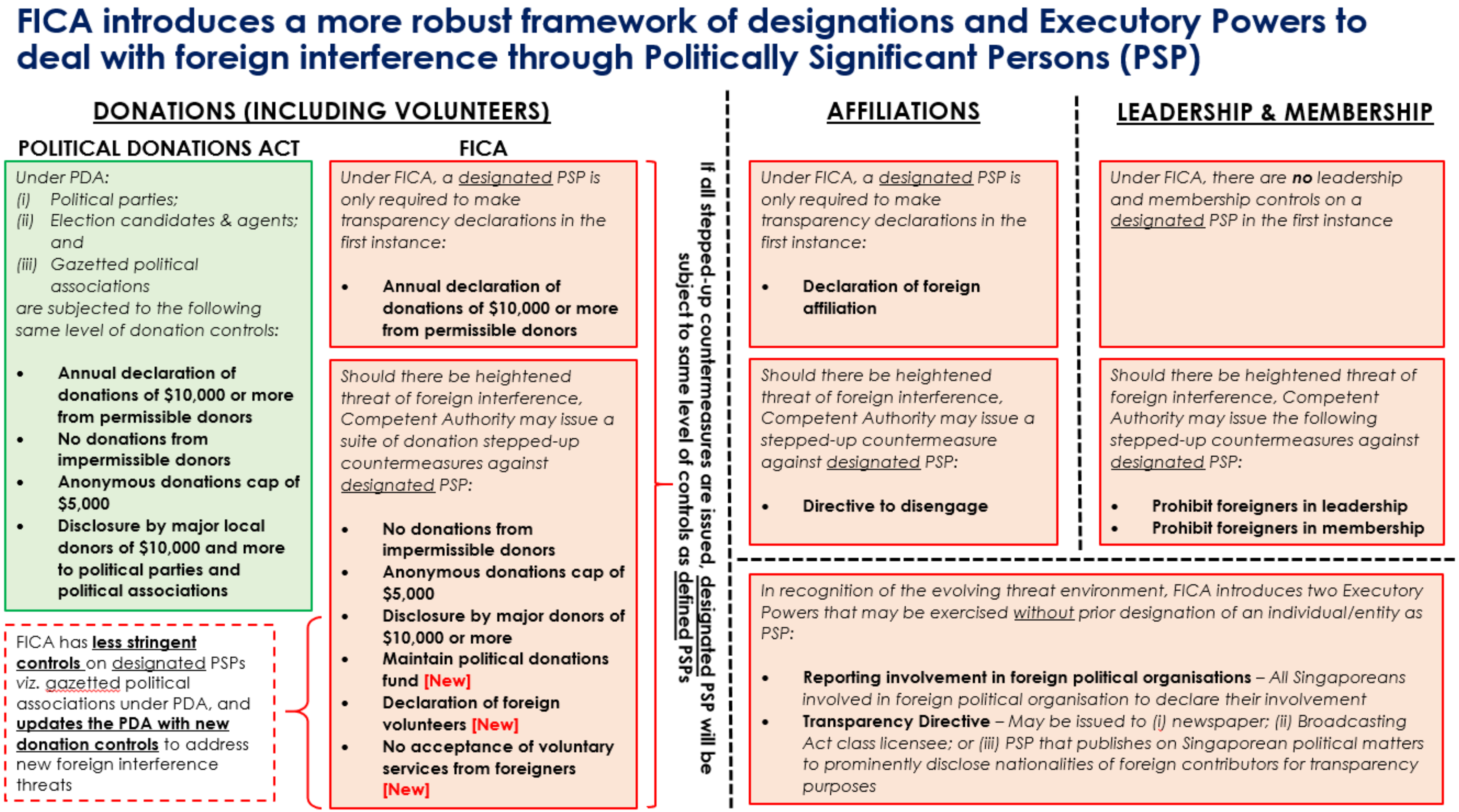
(1) Chart 1 - Substantive and Executory powers in Existing Legislation and FICA (HIC)



FICA does not increase Govt's Substantive Powers to deal with HICs, and provides updated Executory Powers for calibrated response to online HICs

	SUBSTANTIVE POWERS		EXECUTORY POWERS	
	INVESTIGATION	*ARREST & DETENTION*	*ADDRESS HARMFUL CONTENT*	*PROSCRIBE*
THREATS IN PHYSICAL WORLD	**s20 Criminal Procedure Code** *Order production of all information "necessary or desirable" for any investigation or inquiry by any person in Singapore*	**s85 Criminal Procedure Code** *Powers of arrest* **s8 Internal Security Act** *Detention without trial if "necessary to prevent prejudice to national security"; reviewed by Advisory Board with no judicial review*	**s19, s16 Broadcasting Act** *Powers to:* *(i) order a TV station/radio station) to carry a message;* *(ii) stop any broadcasting service or require compliance with content standards*	**s24 National Newspaper and Printing Presses Act** *Restrict declared foreign newspaper* **s31 Broadcasting Act** *Restrict declared foreign broadcasting service (e.g. TV, Radio)*
THREATS IN ONLINE WORLD	**Technical Assistance Direction** *To disclose information required to investigate the source of HIC; may be applied on global companies*	*May arrest and prosecute in court for new FICA offences:* • **Clandestine foreign interference using electronic communications activity** • **Clandestine foreign interference of target using electronic communications activity** • **Preparing or planning the above two offences** *No detention without trial*	**s3 Broadcasting Act, s58 Telecommunications Act** *Power to issue directions where it is "necessary in the public interest or in the interests of public security"* **BA** – *e.g. remove website, block access to websites and even entire social media platforms* **TA** – *e.g. to prohibit or regulate use of telecommunications services* *FICA will introduce more targeted and calibrated directions to tech companies and internet access services:* • **Stop Communication (End-User) & Disabling** – *Remove content from view* • **Must-carry** – social media platforms, online communicators to carry message warning of HIC • **Account Restriction** – *Block accounts from view* • **Service Restriction** – *Alter service functionality so HIC becomes less viral* • **Access Blocking** – *Block websites or accounts that do not comply* • **App Removal** – *Remove apps used to propagate HICs* • **Proscribed Online Location** – *Restrict advertising by or on sites/accounts , prevent profiting off a HIC*	

(2) Chart 2: Substantive and Executory powers in Existing Legislation and FICA (PSP)



FICA introduces a more robust framework of designations and Executory Powers to deal with foreign interference through Politically Significant Persons (PSP)

DONATIONS (INCLUDING VOLUNTEERS)

POLITICAL DONATIONS ACT

Under PDA:
(i) Political parties;
(ii) Election candidates & agents; and
(iii) Gazetted political associations
are subjected to the following same level of donation controls:

- **Annual declaration of donations of $10,000 or more from permissible donors**
- **No donations from impermissible donors**
- **Anonymous donations cap of $5,000**
- **Disclosure by major local donors of $10,000 and more to political parties and political associations**

FICA has **less stringent controls** on designated PSPs viz. gazetted political associations under PDA, and **updates the PDA with new donation controls** to address new foreign interference threats

FICA

Under FICA, a designated PSP is only required to make transparency declarations in the first instance:

- **Annual declaration of donations of $10,000 or more from permissible donors**

Should there be heightened threat of foreign interference, Competent Authority may issue a suite of donation stepped-up countermeasures against designated PSP:

- **No donations from impermissible donors**
- **Anonymous donations cap of $5,000**
- **Disclosure by major donors of $10,000 or more**
- **Maintain political donations fund [New]**
- **Declaration of foreign volunteers [New]**
- **No acceptance of voluntary services from foreigners [New]**

If all stepped-up countermeasures are issued, designated PSP will be subject to same level of controls as defined PSPs

AFFILIATIONS

Under FICA, a designated PSP is only required to make transparency declarations in the first instance:

- **Declaration of foreign affiliation**

Should there be heightened threat of foreign interference, Competent Authority may issue a stepped-up countermeasure against designated PSP:

- **Directive to disengage**

LEADERSHIP & MEMBERSHIP

*Under FICA, there are **no** leadership and membership controls on a designated PSP in the first instance*

Should there be heightened threat of foreign interference, Competent Authority may issue the following stepped-up countermeasures against designated PSP:

- **Prohibit foreigners in leadership**
- **Prohibit foreigners in membership**

In recognition of the evolving threat environment, FICA introduces two Executory Powers that may be exercised without prior designation of an individual/entity as PSP:

- **Reporting involvement in foreign political organisations** – *All Singaporeans involved in foreign political organisation to declare their involvement*
- **Transparency Directive** – *May be issued to (i) newspaper; (ii) Broadcasting Act class licensee; or (iii) PSP that publishes on Singaporean political matters to prominently disclose nationalities of foreign contributors for transparency purposes*

Annex I: Scenarios Raised by Commentators and Application of FICA

Hostile Information Campaigns (HICs)

A Part 3 direction to counter HICs can be issued if all the following conditions are met:

a. There is **online communications activity** taking place, or has already taken place;

b. The online communications activity is conducted **by** or **on behalf of a foreign principal**;

c. Information or material is **published in Singapore** as a result of the communications activity; and

d. After having regard to the circumstances of the case, the Minister assesses that it is in the **public interest** to authorise the giving of these directions.

The Technical Assistance Direction and Account Restriction Direction can be issued on an anticipatory basis, that is when the Minister has suspects or has reason to believe:

a. That **online communications activity** is being prepared or planned, **by** or **on behalf of a foreign principal**;

b. Information or material is likely to be **published in Singapore** as a result; and

c. It is in the **public interest** to give one or more directions.

Politically Significant Persons (PSPs)

A Competent Authority can designate individuals and non-individuals as PSPs if:

a. Their activities are **directed towards a political end**; and

b. The Competent Authority assesses that it is in the **public interest** that countermeasures be applied.

The key is that it must be in the public interest for any direction or designation to be issued.

Under Clause 7, on the definition of "in the public interest", the action taken must be "necessary or expedient".

1. **<u>Interactions raised in the media and other articles</u>**

S/N	Interactions Raised
1.	"The Bill defines 'foreign interference' and 'public interest' so broadly that legitimate online activity undertaken by Singaporeans to influence our laws and public policies potentially risks being the subject of a Part 3 direction by the minister, even in the absence of any manipulation or influence by a foreign government or its agents."
2.	"..even open, non-clandestine 'collaboration' between a Singaporean and any ordinary, private foreign citizen to improve any aspect of our laws and public policies constitutes 'foreign interference', notwithstanding the absence of any foreign state manipulation or foreign funding." "One can easily imagine a wide range of public policy issues that are currently, or which may in the future become, the subject of political debates in Singapore where there is legitimate reason for concerned Singaporeans to 'collaborate' with international experts, researchers and NGOs." Examples include: climate change (including review of laws and policies), trade policy and movement of persons, social issues such as women's rights and gender equality, treatment of foreign workers within Singapore, treatment of business and tax policy.
3.	<u>Local academic conducting research with foreign connections</u>: "presenting research at overseas conferences; writing for international journals and multi-author book projects; publishing in and reviewing for prestigious academic presses; participating in international collaborative research projects; partaking of fellowships, visiting appointments, and training programmes; and participation in international funding opportunities. Any of these may be subsidised or fully funded by foreign universities, foundations, and states."
4.	<u>Academic research on sensitive issues like race, religion, foreign policy, etc., published in foreign journals or co-authored by foreign academics</u> "Below are a few examples of recent works that involve foreign collaborations and online disseminations to the Singapore public and also have some risk of becoming points of social and political contestations locally: • A PhD student challenges the criminalisation of gay sex under the controversial Section 377A, in a special issue of an online, open access cultural studies journal published by the International Academic Forum, a think tank and research centre based at Osaka University. • A journal article in Asia Bioethics Review spotlights the 'multiple barriers to access' to healthcare faced by migrant workers in Singapore. It argues that 'Singapore's boundaries of solidarity must be redrawn to include migrant workers'. One of the co-authors is employed by a university overseas. • A Singaporean political scientist presents a webinar on current political issues in Singapore as part of a series sponsored by the Southeast Asian studies centre of the University of Sydney. The webinar is freely accessible to the Singapore public."

5.	“This [referring to the definition of ‘directed towards a political end’] is incredibly broad and can apply to a wide range of activities, including legitimate advocacy work undertaken by civil society organisations and activists, as well as journalistic reporting and analysis or opinion pieces”
6.	“A local NGO co-hosting an event with a foreign embassy or company could also be deemed to be acting on behalf of a foreign principal, regardless of whether any money has changed hands.”
7.	“Universities and researchers in Singapore sometimes receive foreign funding from private foundations such as Ford Foundation, MacArthur Foundation, Konrad Adenauer Stiftung, the Friedrich Ebert Stiftung, the Korea Foundation, or the Japan Foundation, to conduct research on local issues. They could include policies and the effects of policies on such issues as migrant labour, climate change, environment regulation and the haze, heritage protection, conservation, abortion, religious freedom and extremism, or aspects or internet and media regulation.”
8.	“A church or some religious organisation that has foreign links, such as training or funding, and has a position on an issue, such as abortion or other rights issues, could be affected by this law.”