Report of the Select Committee on Deliberate Online Falsehoods
Executive Summary

Background

1. The Select Committee was appointed by Parliament to examine and report on a serious challenge that many countries, including Singapore, face – the phenomenon of deliberate online falsehoods. The Committee deliberated extensively and went through numerous suggestions and formulations before agreeing on the final version of the report. Arising from this, all decisions made by the Committee were unanimous and consensual. It reflects the Members' shared understanding of the problem and of what Singapore needs to do to counter it.

2. The Committee invited written representations and held public hearings. The Committee considered 169 written representations and oral evidence from 65 individuals and organisations. Representors were from a broad cross-section of society. The Committee also considered other international and local research, and relevant international developments.

Overview

3. The Report addresses the various aspects of the phenomenon and the nature of its dangers for Singapore. It covers (i) the actors that use online falsehoods and their objectives, (ii) the use of digital technologies to spread online falsehoods; (iii) the impact of online falsehoods; and (iv) the difficulties of combatting online falsehoods. It gives specific attention to State-sponsored disinformation operations.

4. The Committee concluded that that the phenomenon is a real and serious problem for Singapore. With the Internet and digital technology, deliberate online falsehoods are more difficult to combat than before. Deliberate online falsehoods are stronger, and spread more widely and at greater speed than the facts. Given the strong effect falsehoods can have on people, and how malicious actors are using them, there is no reason why Singapore would be immune. The Committee received evidence to show that Singapore is a target of hostile disinformation operations, which both stronger and weaker States would find attractive to use against Singapore. At stake for Singapore are her national sovereignty and security, social cohesion, and democratic institutions, including the democratic contestation of ideas. The Report details the evidence that led to these findings.

5. The Committee identified the desired outcomes to guide Singapore's responses, namely, a public that is informed, a society that is cohesive and resilient, and a people whose sovereignty and freedom are safeguarded.

6. The Committee recommended a multi-pronged approach to tackle deliberate online falsehoods, comprising 22 specific recommendations to (i) nurture an informed public, (ii) reinforce social cohesion and trust, (iii) promote fact-checking, (iv)

disrupt online falsehoods, giving particular consideration to the role of technology companies, and (v) deal with threats to national security and sovereignty. These recommendations were addressed to the Government, as well as other actors such as technology companies, journalists, media organisations, and civic society.

7. The Committee found that Government intervention, including through legislation, is necessary to disrupt online falsehoods.

Findings on the Phenomenon of Deliberate Online Falsehoods

Actors Who Use Falsehoods and Their Objectives

8. The Committee found that the phenomenon was pervasive. The Report sets out examples from around the world, which showed that a wide range of actors, both States and civilians, use deliberate online falsehoods to achieve various objectives.

9. Motivated by geopolitical interests, foreign States use deliberate online falsehoods to discredit other governments, undermine their foreign policies, turn people against each other from within, and sow confusion over the truth to undermine public discourse in the target country. They even target their own citizens to motivate them to fight other countries.

10. Motivated by ideologies, politics and prejudices, citizens and others, in different countries use online falsehoods to illegitimately promote their causes. Elections around the world have seen domestic groups use disinformation to support their favoured politicians and denigrate the opposition. Extreme right-wing groups in the US, UK and France have used falsehoods to stoke anger against Muslims and migrants, and undermine trust in the government's ability to deal with these issues. Falsehoods by domestic groups in Indonesia have furthered racist and sectarian interests.

11. These causes can cut across national borders. For example, the US alt-right were reportedly involved in disinformation campaigns in the 2017 German Federal Election and the 2017 French Presidential Election, to support the election of alt-right politicians and undermine their opposition. In Singapore, user accounts that appeared to be foreign posted on local media's Facebook pages, denying the crisis faced by Muslims in Myanmar's Rakhine state and making Islamophobic comments. There are also online civilian "armies" that advance their governments' agendas against other countries. Terrorist organisations, such as ISIL, have used online disinformation to radicalise people around the world, including in Singapore.

12. Profit-driven actors may spread falsehoods as these tend to attract more "clicks," which in turn generates more digital advertising revenue. Relevant examples include falsehoods about the 2016 US Election spread by the Macedonian "fake news industry," and the false story by a dubious overseas website that Singapore's

Minister of Foreign Affairs had collapsed at an international event. Profit-seekers may also, intentionally or otherwise, advance political objectives.

Use of Digital Technologies to Spread Online Falsehoods

13. The Committee observed that the ease, speed, reach and impact of online falsehoods are unprecedented. Convincing falsehoods can be created through simple text. A basic splicing edit to a video of a speech by a former Jakarta governor made it seem like he had committed blasphemy, leading to massive protests. Fake videos and audio of real people saying or doing things they did not, also known as "deepfakes", can now be created relatively easily and cheaply.

14. Malicious actors are developing effective methods of using online falsehoods to influence people. The Report highlights several common methods. *First*, fake social media accounts have been used by foreign actors to infiltrate local communities and amass real local supporters, without spending a dollar on advertising. In the US, a foreign-linked fake Twitter account of a fictitious American woman called "Jenna Abrams" had over 70,000 followers, and was quoted by a slew of prominent media outlets, including the New York Times and The Washington Post. Another foreign-linked fake Twitter account impersonated the real Tennessee Republican Party. It had over 150,000 followers, far more than the real account, which had 14,000. The fake account was also re-tweeted by a US Presidential candidate and senior members of his campaign. These accounts spread divisive falsehoods and racist content, especially as the 2016 US Election neared.

15. *Second*, fake social media accounts run by human trolls or automated bots have been used to rapidly re-post online falsehoods, making them go viral. A 2018 Oxford University research report found evidence of trolls and bots spreading online disinformation in almost all of the 48 countries surveyed. During the #Macronleaks controversy in the 2017 French Presidential Election, a network of trolls and bots amplified the hashtag, which guided users to false claims that Macron was using offshore accounts to evade tax. The hashtag reached 47,000 tweets in just under 4 hours, and was pushed onto Twitter's trending lists.

16. *Third*, digital advertising tools have been used to target online falsehoods at susceptible audiences. This is easily and cheaply done on platforms such as Google and Facebook by selecting targeting options that are displayed, such as demographic, location and interests. During the 2016 US Election, foreign actors spent US$100,000 on Facebook advertisements, reaching 126 million US users. Targeting is effective – network theorists have shown that when falsehoods are targeted at those predisposed to believe them, they spread further.

17. *Fourth*, the algorithms of social media platforms have been exploited to make online falsehoods more visible to users. These algorithms control the content that users see, and generally increase the visibility of content that has received more user interactions. Malicious actors, including foreign disinformation agents, have

used bots, trolls and "click-bait" to drive up user interactions with disinformation, causing it to be "boosted" on the social media platform.

18. The Committee found it striking how these digital technologies used by foreign States are accessible to average civilians. It observed that the Internet has democratised information, and has also democratised its weaponisation.

Impact of Online Falsehoods

19. The Committee identified four overlapping dimensions of society impacted by online falsehoods: (i) national security, (ii) democratic institutions and free speech, (iii) individuals, and (iv) businesses. The first two, which are forms of public harm, are covered here.

20. *National security*. Disinformation operations by foreign States threaten national sovereignty and security. Foreign policies can be impacted. For example, false narratives discrediting the Ukraine government was said to have led to Dutch citizens voting against an EU-Ukraine trade agreement. Also, people can be galvanised to take up arms against another country. Russian citizens were reportedly motivated to fight against the Ukrainian army because of faked atrocities committed by Ukrainian soldiers.

21. Falsehoods can undermine social cohesion. Foreign disinformation has increased polarisation and turned groups against each other from within. For example, in the US, trolls linked to a foreign country used fake social media accounts to gain influence and use falsehoods to promote opposing sides of divisive issues such as race, LGBT rights, and political candidates. They would also organise rallies and protests. In one case, they used both a fake account promoting Muslim causes, and a fake anti-"Islamization" account, to organise a protest and a counter-protest about the setting up of an Islamic library – at the same time and place. Real Americans turned up, leading to a visible stand-off on the streets, with one protestor reportedly bringing a rifle. Organising this reportedly cost only US$200.

22. Similarly, falsehoods can provoke violence by preying on what people are afraid of or are angry about. Such falsehoods led an American to fire a gun in a pizza restaurant in Washington, DC. They provoked massive rallies during elections in Indonesia, and encouraged anti-immigrant demonstrations in Europe. They have had horrific consequences – such as instigating angry mobs to burn down temples and monasteries in Indonesia, and to murder amidst communal violence in India.

23. *Democratic institutions and free speech*. Online falsehoods can derail democratic contestation, and harm freedom of expression. In Germany, some representors said that anti-immigrant negativity on social media may have deterred those more sympathetic to immigrants from speaking up. In the US, false claims that the 2018 Florida school shooting was not real made the gun debate more toxic.

24. Falsehoods that undermine trust in public institutions can impede constructive policy-making, and the ability to respond to crises and threats effectively. For example, when German police de-bunked a false claim that immigrants had raped a girl, they were falsely accused of covering up crimes committed by immigrants. This contributed to street protests. A falsehood that a Syrian refugee in a photograph with German Chancellor Angela Merkel was an ISIS terrorist was intended to turn people against the German government. Such falsehoods are said to have made it more difficult for European governments to formulate constructive immigration policies.

25. Falsehoods can erode people's trust in authoritative sources of information, which provide a foundation of facts for rational discourse. Psychological research has shown that being exposed to large amounts of misinformation can make people stop believing facts altogether, and decrease their engagement in public discourse.

26. Online falsehoods have been increasingly prevalent in elections around the world. Falsehoods targeting elections can negate informed political participation. By casting doubt on the legitimacy of the outcome, they undermine people's assurance of a representative government. While the overall evidence is so far unclear, there is some evidence that falsehoods can also sway voting behaviour.

Difficulties of Combatting Deliberate Online Falsehoods

27. The Committee observed that deliberate online falsehoods are hard to combat, as falsehoods (which are designed to appeal to people in specific ways) often trump facts. *First*, falsehoods generally have a stronger psychological effect on people that is harder to correct. People tend to reject corrections that are inconsistent with their world views. These tendencies can affect people from all segments of the society.

28. *Second*, online falsehoods generally spread further, faster and deeper than the facts. A 2018 MIT study found that falsehoods were 70% more likely to be re-tweeted than the truth. A 2018 University of Buffalo study found that less than 20% of users who shared or liked a false tweet would correct it after it had been debunked.

29. *Third*, corrections tend not to reach those exposed to the falsehood. For example, based on a recent survey, respondents who read false articles shared during the 2016 US Election did not see the debunks. Similarly, there was almost no overlap between the audience for the rumour that then-French candidate Emmanuel Macron was funded by Saudi Arabia, and the audience of its debunk.

30. The Committee also observed that even as deliberate online falsehoods were becoming harder to combat, social resilience to them has tended to lessen. Online conditions worsen heuristic tendencies and cognitive biases. Social transformations in the digital age also play a role: (i) online echo chambers tend to heighten intolerance to differing views and are a primary driver of online misinformation, (ii) there is a proliferation of online news sources that do not apply standards of

professional journalism, and (iii) social media is increasingly being used for political discourse, even though it encourages discourse to be emotionally-driven and convenient, rather than reasoned and considered.

31. Adversaries are sophisticated and will improve. The techniques used in the 2016 US Election are again seen in the 2018 US Mid-Term Election; greater effort is now being made to avoid detection. Disinformation is becoming professionalised and commercialised. One can buy bot armies, click farms, and petition signatures, and hire people to manipulate votes or instigate a street protest.

Risks to Singapore

32. The Committee received evidence that State-sponsored information operations have been carried out against Singapore. Some of this evidence was received in private hearings. The series of cyber-attacks against Singapore, including the recent SingHealth hacking, are also indicative; both disinformation and cyber-attacks are part of the information warfare toolkit.

33. Both stronger and weaker States will find online disinformation an attractive option against Singapore, which has achieved strong deterrence in relation to conventional warfare. Examples elsewhere show how disinformation can achieve high impact at disproportionately low cost. With online anonymity, and the borderless Internet, it is harder to detect, and easier to disavow. It often exploits local concerns to disguise foreign interference as a local movement.

34. Online disinformation capabilities are developing in the region, which can be sharpened for the local context and turned against Singapore. These include for-profit syndicates, bot armies and "data-driven political consultants" with expertise in using data analytics to micro-target messages at susceptible people. The threat to Singapore is continuous. In the digital age, some States regard information warfare as continuous and permanent, to be used whether in war or peacetime.

35. The realities of Singapore's diverse social landscape create many opportunities for falsehoods to undermine Singapore's social cohesion. Survey findings presented to the Committee showed that Singapore is not a race-blind society and differences do matter. Any source of difference, including racial and ideological differences and social inequalities, can be exploited, turning cracks into chasms.

36. "Low level" everyday online falsehoods can gradually raise tensions, leading to more serious crises. In Singapore, online falsehoods about new immigrants have provoked xenophobic comments; communal and religious online falsehoods have stirred tensions within communities. Such falsehoods can, over time, corrode Singapore's social cohesion. Exposure over time to falsehoods and partisan views can skew worldviews.

Recommendations for Responding to the Phenomenon

37. The Committee observed that countermeasures needed to address the asymmetry between the growing power of technology, and the capacity of societies and countries to deal with its consequences. The Committee recommended a multi-pronged and calibrated approach to doing so. The different aspects are mutually reinforcing, and each are equally important.

(1) Nurture an informed public

38. The Committee identified public education and quality journalism as key pillars of nurturing an informed public. Public education equips individuals to tell false from fact. Quality journalism informs the public, and helps them make sense of the world. The main issue is ensuring they are adequate and effective against the evolving challenges of online falsehoods.

39. **Public education.** The Committee commended ground-up groups, the media, technology companies and public agencies engaged in public education, and called on them to review existing efforts to ensure they were adequate.

40. The Committee recommended a national framework comprising (i) a broad-based school curriculum that would not only impart critical thinking, but also include the motivations, tools and techniques of disinformation agents, and equip students for active and constructive public discourse, and (ii) a research-driven framework of desired skills and outcomes for educating other segments of the public, and coordinating ministry actions to ensure outreach to all segments of society (***Rec. 1***). The Committee also made a recommendation to the Government to widen effective outreach by supporting ground-up initiatives (***Rec. 2***).

41. **Quality journalism.** The Committee made recommendations to news organisations, journalists, technology companies, institutes of higher learning and the Government on ensuring that news providers are equipped with the skills to report with accuracy in a more challenging digital news environment, and that both online and alternative media maintain the same professional standards of journalism (***Recs. 3 to 6***).

(2) Reinforce social cohesion and trust

42. The Committee observed that trust holds a country and society together in the face of attempts to divide. The Committee considered ways to strengthen trust, to reduce opportunities for deliberate online falsehoods to exploit Singapore's fault-lines.

43. **Trust among people and communities.** The Committee commended existing initiatives that seek to foster understanding among different communities, and respond quickly to racial and religious tensions. The Committee observed that existing efforts would need to evolve to address the phenomenon of deliberate

online falsehoods. The Committee called for individuals to be equipped to overcome perceived barriers and raise sensitive issues relating to different groups.

44. The Committee recommended that organisations promoting social cohesion help clarify and dispel divisive falsehoods, and encouraged them to create "safe spaces" for discussing sensitive issues, and reach into and across "echo chambers." (***Rec. 7***) The Committee also emphasised responding early to how xenophobia, hate and other new vulnerabilities manifest in Singapore, and recommended that the Government consider supporting or conducting research to understand society's vulnerabilities (***Rec. 8***).

45. **Trust in public institutions.** Without public trust, public institutions would be unable to respond effectively to threats and crises, and serve as an authoritative source of information for society. Foreign disinformation campaigns have often sought to erode trust in public institutions, as this increases their chances of success.

46. The Committee made recommendations to public institutions that emphasised the timely communication of information to both pre-empt and respond to online falsehoods, and recognised the role of participation, transparency and accountability in ensuring public trust in how public institutions respond to online falsehoods (***Recs. 9 and 10***).

(3) Promote Fact-Checking

47. Fact-checkers can help spread corrections and encourage people to value and pursue accuracy and veracity. The Committee found fact-checking important, while acknowledging the evidence of its limitations, such as how they may fail to reach those exposed to the falsehood, or fail to persuade those with opposing world views.

48. The Committee considered diverse recommendations for different types of fact-checking initiatives, including divergent views on the role of the Government in fact-checking. The Committee recommended that media organisations and their industry partners consider establishing a fact-checking coalition. The role that the Government can play needs to be further considered, in the light of the different viewpoints (***Rec. 11***).

(4) Disrupt Online Falsehoods

49. The Committee found that Government intervention to disrupt online falsehoods is necessary. The Committee observed that the phenomenon of deliberate online falsehoods is gaining strength faster than laws and norms can keep up. The foregoing measures, which did not directly target falsehoods and those responsible, were shown by the evidence to be necessary but insufficient.

50. The Committee observed that falsehoods can appear in a broad spectrum of circumstances, from deliberately fabricated content to satire and parodies. They can

also have varying degrees of impact, causing minor confusion to threatening national security and dividing societies. The Committee emphasised that Government intervention should be calibrated in a manner that takes these factors into consideration, especially the potential for real-world impact and consequences. Also, there should be careful calibration to prevent the public interest from being harmed, and to at the same time respect communications that are personal, private, and of limited circulation.

51. **Counter and deter online falsehoods.** To swiftly disrupt the spread of online falsehoods, the Committee recommended that the Government have powers, through new legislation, to implement a range of measures with different objectives, from increasing exposure to corrections, to limiting exposure to the falsehood, to preventing the falsehood from being amplified by bots, trolls and digital advertising. These measures should be able to break virality by being effective in a matter of hours. They should apply to both open and closed platforms. Adequate safeguards should be in place to ensure due process and the proper exercise of power. (***Rec. 12***).

52. The Committee observed that Facebook, Twitter and Google (and YouTube) have confirmed that they generally will not, as a matter of policy, and absent legislation, remove content on the basis that it is false. This also showed the need for legislation.

53. The Committee expressed concern as to whether electoral laws were fit for purpose in the digital age. The Committee recommended that the Government identify additional measures to safeguard election integrity, and implement the necessary measures, including legislation (***Rec. 13***). The Committee also made a general recommendation on monitoring and early warning mechanisms (***Rec. 14***).

54. To deter and dis-incentivise deliberate online falsehoods, the Committee recommended that the Government:

    a. Establish a de-monetisation regime, through legislation, against purveyors of online falsehoods, that would cut off digital advertising revenue and require the disgorgement of financial benefits. (***Rec. 15***)
    b. Impose criminal sanctions. The Committee emphasised that this should be applied only when certain criteria was met, such as the requisite degree of criminal culpability, and threshold of harm. The sanctions should cover the deliberate use of inauthentic accounts or bots and the provision of tools and services to publish falsehoods. (***Rec. 16***)

55. The Committee considered concerns that legislation was limited by national borders and may not keep up with technology. The Committee agreed that there were real challenges to be dealt with. These challenges should be dealt with through iterative improvements, rather than waiting for a perfect solution.

56. The Committee considered some viewpoints that legislation would harm free speech. The Committee found that online falsehoods undermine democracy and harm the democratic contestation of ideas, which freedom of speech serves to protect. Measures to combat deliberate online falsehoods and the right to free speech in fact served the same democratic ideals. On concerns that falsehoods were difficult to define, the Committee observed that the law has historically defined falsehoods, and the Courts regularly do so.

57. The Committee considered the view that the problem should be left to the contestation of ideas in a "free marketplace." The Committee found this to be contradicted by the real and serious consequences that online falsehoods have had. It was also discredited by rigorous analyses provided by representors, who noted that even free trade and market competition required regulation. The Committee highlighted how the free marketplace view wrongly assumes that the playing field is equal.

58. The Committee considered the argument that voluntary action by technology companies would be adequate to counter online falsehoods. Having examined the research and evidence in detail, the Committee found that: (i) the measures taken by technology companies to combat the phenomenon (Annex F) were a positive step; however, they were far from being adequate, (ii) they have a track record of not always responding adequately to the harm that their platforms have contributed to, even in times of serious crises, such as in Sri Lanka and Myanmar, and being slow to accept responsibility for their negative societal impacts, such as in the Cambridge Analytica case; (iii) due to a fundamental conflict of interest, technology companies are not best-placed to make decisions in the public interest.

59. **Adapt online platforms.** The Committee found that technology companies have a social responsibility to contribute to a clean Internet information ecosystem, and should bear responsibility for preventing their platforms and products from being abused to create and spread online falsehoods. The Committee considered in detail the various ways in which they have played a significant role in the spread of online falsehoods.

60. To prevent and mitigate the abuse of online platforms to spread online falsehoods, the Committee recommended that technology companies take certain measures concerning how their platforms prioritised content, inauthentic accounts, digital advertising tools, the collection and use of user data, and online anonymity and accountability (***Rec. 17***).

61. To foster an informed public, the Committee recommended that technology companies take certain measures, including enabling users to assess on their own the credibility of the information they receive, sharing information with researchers and experts to illuminate disinformation tactics and techniques, and helping develop technologies to advance the integrity of online information (***Rec. 18***).

62. The Committee considered ways of holding technology companies accountable for taking adequate measures to fulfil their responsibilities to society. The Committee recommended that technology companies undertake voluntary reporting and independent audits (***Rec. 19***). The Committee also recommended that the Government consider legislation and complementary forms of regulation to achieve the objectives in Recommendations 17 to 19 (***Rec. 20***).

(5) Deal with Threats to National Security and Sovereignty

63. Drawing on evidence from experts and researchers in the field of national security, the Committee observed that the "visible hand" of the State was crucial to counter threats to national sovereignty or security. The Committee recommended that the Government study the recommendations of expert representors, and formulate a national level strategy and coordinated approach for countering State-sponsored disinformation operations (***Rec. 22***).