Opening Keynote Address by Dr Janil Puthucheary, Senior Minister of State, Ministry of Communications and Information and SMS-in-Charge of Cybersecurity at International IoT Security Roundtable 2020 on 8 Oct 2020

Securing Our "Internet of Everything": Singapore's IoT Journey

Ladies and gentlemen,

1. Good afternoon. Thank you for joining us at the International IoT Roundtable event as part of the 5th Singapore International Cyber Week (SICW).

Securing Our IoT Landscape

2. In the wake of COVID-19, digitalisation is both an imperative and an opportunity. It has been described as the "Great Reset". It has torn up the script for how the global order operates, accelerated the pace of digitalisation, and catalysed new trends. This has all been made possible by advances in computing, and by "Internet of Things" (IoT) devices that blur the divide between physical and cyberspace, powering smart cities, harness big data, and keeping us connected in an age of physical lockdowns and safe distancing. These devices have become ubiquitous and people have taken to calling it the "Internet of Everything".

3. Studies estimate that there are 31 billion IoT devices today, with 127 new devices added every second. This will more than double to 75 billion connected devices by 2025. We are also beginning to see the convergence of IoT with emerging technologies such as Artificial Intelligence (AI), heralding new use cases such as hyper-automation.

4. In Singapore, digital solutions have been instrumental in helping us to progressively reopen our economy and emerge from our eight-week "Circuit Breaker" from April to June, which we undertook to arrest the spread of the pandemic. *TraceTogether* and *SafeEntry* – our two national digital contact tracing and digital check-in tools – have helped to raise the speed and effectiveness of our public health professionals' contact tracing operations, and have contributed to at least a semblance of normality. We will continue to leverage technology to push the boundaries in how we do business, and how we go about our lives. For example, we have set up the SG Digital Office, which coordinates the work of 1,000 Digital Ambassadors, helping almost 30,000 seniors to adopt digital solutions. Singapore will continue investing in digital inclusion initiatives, to help our citizens reap the benefits of technology.

5. But greater connectivity also brings greater risks. The "Internet of Everything" represents a vulnerable conduit that expands our attack surface, and can impact our broader cyber landscape. The vast majority of IoT devices – baby monitors, home routers, even our fridges and cars – are optimised for functionality and cost, rather than security. This is not just a technical problem. It is also about building trust and partnerships – such as partnerships on the need for internationally recognised IoT standards and protocols. Mutual trust and confidence between stakeholders are fundamental requirement for a hyperconnected digital society.

Singapore's IoT Journey

6. In this fifth edition of the International IoT Security Roundtable, which has been held since the inaugural SICW in 2016, I am happy to see so many of our partners - government, industry and academia here - supporting our triple helix efforts to develop a secure and trusted IoT ecosystem.

7. Singapore will continue to forge partnerships with like-minded stakeholders towards establishing industry standards, and cultivating a secure IoT ecosystem. Over the years, our Roundtable conversations have borne fruit. Last year, we published our **IoT Security Landscape Report** in collaboration with The Netherlands. The study called on public and private sector stakeholders to adopt security initiatives, to address security challenges in the IoT sphere, to drive standards, and innovate towards a safe and secure IoT space. **Singapore and the UK also affirmed our mutual commitment** towards the adoption of best practices to secure IoT devices. Such efforts are crucial in driving greater innovation and greater security. We hope that this Roundtable can continue to play a role in engaging and galvanising global communities to harness these powerful technologies in meaningful and responsible ways.

8. Much good can come from the public and private sector coming together, to mitigate potential harms arising from the use of digital products and services. Yesterday, Minister Iswaran announced the launch of the new Cybersecurity Labelling Scheme, an initiative under the Safer Cyberspace Masterplan – the first of its kind in the Asia Pacific region. This will help enable consumers to make informed decisions, help companies that produce secure IoT devices to distinguish themselves, and raise our overall cyber hygiene here in Singapore. Given the borderless and interconnected nature of cyberspace, a global approach is necessary. The scheme will be aligned to international security standards for consumer IoT products. And it would be continuously improved, to nudge businesses to embrace higher security standards, based on market interests, as well as the industry's acceptance and readiness. Through this, we hope to strike a balance between raising cyber hygiene, and encouraging the advent of new and innovative products. Singapore will also explore opportunities for mutual recognition with like-minded partners from around the world.

Securing Emerging Technologies

9. Even as we tackle the cyber challenges of today, it is important to prepare for the cyber threats of tomorrow. With emerging technologies such as quantum computing, research and innovation are pivotal in extending our cybersecurity capabilities in areas of strategic importance. It also creates numerous good career opportunities in this fast-growing ecosystem.

10. We will continue to seed strong long-lasting ties between our researchers and a wide range of partners to benchmark our research capabilities against the best in the world, and tap on a broad pool of global expertise. In the past, we have issued joint grant calls with international partners such as the UK. **CSA is working with Tel Aviv University to launch a second joint grant call in late 2020, under the ambit of our National Cybersecurity R&D programme.** The call will seed research collaboration efforts on challenging areas in cybersecurity, including the Security of Smart Cities and the Internet of Things.

11. As part of Singapore's continual efforts to develop and grow Research and Development (R&D) capabilities, I am pleased to announce that the **National Cybersecurity R&D Programme (NCRP) will be transferred from the National Research Foundation to the Cyber Security Agency of Singapore** by March 2021.The transfer of this research programme to CSA will allow the Programme to harness the networks that Cyber Security Agency of Singapore has built over the years, and achieve better synergies between Government agencies, industry, and research partners.

Conclusion

12. Let me leave you with two parting thoughts. First, cybersecurity - and IoT security – is a prerequisite for our common digital future. We cannot be a digital society if our systems are not trusted and resilient. Second, the need for IoT security is a collective challenge that requires trust and strong partnerships between stakeholders. In these most unusual times, it is more important than ever for governments, the industry, and academia – locally, regionally and internationally – to come together in enabling a trusted, secure and rules-based cyberspace.

13. I am glad to see strong support for the International IoT Security Roundtable, even in this new hybrid format. We have an exciting and diverse line-up of speakers today. Thank you for joining us, and I hope that you will find the conversations in this Roundtable useful and enriching.