Ministry of Communications and Information
An Engaged and Connected Singapore

Keynote Address by SMS Janil Puthucheary at International IOT Security Roundtable (6 Oct 2021)

The Internet of Things Beyond Borders

Ladies and gentlemen,

1. Good day and thank you for joining us at the International IoT Security Roundtable event of the 6th Singapore International Cyber Week (SICW).

2. Let me begin by thanking all our partners – governments, industry, and academia for being present here today to support our continued efforts to build a secure and trusted IoT ecosystem globally.

Securing the International IoT Landscape

3. COVID-19 has highlighted the importance of digital technology, especially the accelerated pace of digitalisation and advances to internet technologies. The pandemic has thrown up many uncertainties and issues, and has spurred governments and businesses to pick up the pace on their digital transformation. All over the world, dependence on IoT has increased as nations and cities are transforming into smart cities, with the need for connectivity and the harnessing of vast volumes of data deepening and accelerating. By some estimates, the number of connected devices globally will double in 2030, compared to 2018, up to 50 billion devices, and in slightly over a decade.

4. In my portfolios - Communications and Information, and Health, cybersecurity cuts across and remains a key priority. It is something my colleagues and I constantly grapple with and think about, especially the tradeoff of how to balance the need to ensure the safety, health and wellbeing of our fellow citizens during this period. The social distancing and travel restrictions have been inevitable to curb the spread of the COVID-19 virus. And we still, through that, want to encourage people to remain virtually connected to their families, friends and colleagues, and to their businesses. Doing so virtually has become essential and IoT has thus become an even more integral part of our daily lives as much of our work and social interactions are taking place online. And that digital transformation, which nations, governments and societies are engaged in, is also transforming our homes and personal lives.

5. Notwithstanding the opportunities that IoT and digitalisation bring, there are also downsides and risks that need to be addressed. Majority of consumer IoT devices are built and developed to optimise functionality and cost, usually at the expense of the security of the device. However, IoT security should not and cannot be an afterthought, but should be a key consideration and a design fundamental. Without the requisite security in place, it leaves end users exposed to malicious cyber threat actors seeking to compromise the devices and this results in the loss of data, but more importantly, privacy and trust. Just last year, it was reported that hacked footage from home cameras in Singapore were leaked online. Thus it is critical for us to upskill our security professionals, instill a sense of awareness and responsibility amongst end users, and build strong partnerships and trust with the international community and industry.

Singapore at the Forefront of IoT Security

6. This is the sixth edition of the International IoT Security Roundtable and it has served as an important platform that supports international collaboration and cooperation on how to better

secure IoT devices. The pandemic has indeed posed some challenges to the organisation of large-scale events like the SICW, but I am truly grateful and heartened to see many familiar faces today, albeit virtually. It is a testament to our collective commitment – as a community of practice of like-minded professionals across government, industry, and academia – to develop a trusted ecosystem to run our digital ecosystem.

7. These twin pillars of trust and partnership have always guided Singapore's efforts in IOT security. Last year, Singapore launched the Cybersecurity Labelling Scheme (CLS), the first multi-levelled scheme for IoT devices in the world. This initiative aims to empower consumers to make more informed decisions when purchasing IoT devices and to allow the companies producing them to distinguish their products. Taken together, this would help us to raise the level of cyber hygiene standards in Singapore. Although just launched last year, I was told that the scheme has received more than 100 applications and some labelled products can already be found in physical stores and online shops. I'm sure there are more to come.

    a. This year, trust and partnership continue to feature strongly, both internationally and within Singapore. **I am pleased to announce that Singapore will be signing a Memorandum of Understanding (MOU) with Finland to mutually recognise the cybersecurity labels issued by** the Cyber Security Agency of Singapore (CSA) and the Transport and Communications Agency of Finland (Traficom). The signing will be taking place live right after my speech and Mr David Koh, Chief Executive of CSA, will say more about the significance of this mutual recognition.

    b. **CSA has also published the CLS labelling standard – Technical Reference 91 – under the Singapore Standards Council**. This technical reference was developed through a public-private partnership between the government, industry, and academia. It aims to serve as a standard that can be adopted by manufacturers, developers, testing bodies and suppliers of consumer IoT devices globally, as well as a framework for the mutual recognition of cybersecurity labels with international partners. We hope that the TR 91 can encourage more IoT manufacturers to be proactive in building safe and secure consumer IoT devices. TR 91 is developed based on international standards and practices which help reduce testing and compliance costs while facilitating greater market access. CSA has also started to look into extending the CLS to additional products and services. We are further set to increase the number of service providers for CLS assessment, to meet growing demand.

8. Beyond protecting individual IoT devices, we also need to put in place measures to protect the network of IoT devices. The vast majority of Distributed Denial of Service (DDoS) botnets are typically built from consumer IoT devices; yet the potential damage from DDoS attacks goes far beyond individual users. This was the case in 2016, when the Mirai malware took advantage of insecure IoT devices to build a botnet, which caused a massive DDoS attack that left much of the internet inaccessible in the US. The work of building a safe, resilient, and secure IoT ecosystem is thus very important and spans across various stakeholders. To this end, **CSA has partnered with the Global Cyber Alliance (GCA) – an international organisation, to leverage on their Automated IoT Defence Ecosystem (AIDE), a growing network of partners for IoT threat sharing worldwide**. This partnership is a milestone that GCA can build upon to expand AIDE's reach to other smart cities globally. Our local industry partner Ensign Infosecurity (Ensign)'s advanced threat analytics insights will provide CSA with early warning of the latest IoT attacks and allow Singapore to develop and put in place appropriate policies and technical measures to safeguard against threat vectors. We hope that the result of this partnership will be a better prepared and safer IoT cyberspace that can safeguard our digital economy and our digital way of life.

Building up the TIC (Cyber) ecosystem in Singapore

9. Singapore is a globally trusted trade hub, and we aspire to continually provide high quality, reliable and secure digital products and services to our consumers and customers. To do so, we must adhere to and enforce stringent standards and a robust regime of testing, inspection, and certification (TIC). Singapore has the largest market share in ASEAN in the TIC industry and we are pushing on both the domestic and international fronts, to uplift the standards and technical capabilities of the growing talent pool to support the changing needs and requirements of the digital economy. One of the four key focal sectors for the local TIC industry is digitalisation and cybersecurity, which has also been identified as one of the fastest growing sectors requiring support in ASEAN. We will partner with trade associations and chambers, the industry, academia, and government agencies to further our efforts in this sector, and to expand the scope for TICs in Singapore.

10. One of CSA's key initiatives is our collaboration **with Nanyang Technological University to launch a Graduate Certificate for Hardware Security Evaluation and Certification**. This programme will commence in 2022 and will cover a range of topics that will enhance the existing cybersecurity curriculum for students and equip security practitioners and professionals with the skills to undertake roles for evaluation and certification, forensic investigation and vulnerability assessment. This will provide a competitive edge to our local cybersecurity workforce and lower the barriers of entry into this field. Students who enrol in this programme can also tap on SkillsFuture funding, our Singaporean adult learning initiative.

11. The Graduate Certificate programme will leverage on the state-of-the-art facilities in the National Integrated Centre for Evaluation (NICE). NICE is a partnership between CSA and NTU that will serve as a one-stop facility for security evaluation and certification, including research in security techniques, and is scheduled to open officially in early-2022.

Conclusion

12. We have made much progress since the inaugural International IoT Security Roundtable. Yet, with the constantly changing technology landscape and the accelerated pace of digitalisation, there is an urgency to our efforts. We must be able to work together to identify the risks to our digital ecosystem, and contain and transform them into opportunities. To this end, I am immensely grateful to the friends and partners from governments and industry who have lent their unwavering support and commitment to our joint cause.

13. Given the challenges confronting us and the opportunities awaiting us, we have every reason to keep pushing limits to enhance the resilience and security of our IoT ecosystem, and build trust that transcends geographical boundaries. I am glad to see such strong support and participation for the Roundtable today, despite the ongoing global pandemic. We have a diverse line-up of speakers today, and I wish you all enriching conversations and discussions at this Roundtable. Thank you.