Ministry of Communications and Information
An Engaged and Connected Singapore

SPEECH BY MRS JOSEPHINE TEO, MINISTER FOR COMMUNICATIONS AND INFORMATION, AT THE ASEAN MINISTERIAL CONFERENCE ON CYBERSECURITY ON 20 OCTOBER 2022, 8.45AM

CREATING A SUSTAINABLE DIGITAL FUTURE TOGETHER

Your Excellencies

Deputy Secretary General for the ASEAN Economic Community, Mr Satvinder Singh

Senior Officials

Colleagues and friends

Introduction

1. Good morning. Welcome to the 7th ASEAN Ministerial Conference on Cybersecurity (or AMCC). I am very pleased to finally meet all our ASEAN colleagues in person today as a group after two years where the AMCC was conducted virtually. I also want to greet all of our dialogue partners today, and thank you for making the time and effort to interact with all of us.

Digital Security Underpins a Sustainable Digital Future

2. Last week, I attended the Tallinn Digital Summit and was posed during the dialogue discussion a question about how the digital landscape has changed over the past 15 years. The Estonian colleagues used 15 years, because in 2007, they suffered a major cyberattack that was permanently seared in their minds, and a constant reminder of how important it was to take cybersecurity seriously. So, the question was centred on the 15 years since 2007. In those 15 years, we have moved from 3G to 4G, and now many of us are getting ready for, or have already moved on to 5G.

3. In ASEAN, with a population of about 660 million, we have around 340 or 350 million of our people, who are already digital users. 60 million of them were added during the pandemic alone. So, the extent of digitalisation in our region is happening very quickly and shows no signs of slowing down. Bloomberg estimates a 25% growth in Southeast Asia's digital economy in 2022. It is an exciting time for ASEAN to tap on the opportunities that digitalisation brings.

4. But we all are also keenly aware that where there are opportunities, there are also threats and risks. Just this year alone, we've seen several crippling cyberattacks, such as those in Costa Rica and Albania. Globally, it is estimated that almost US$950 billion was lost to cybercrime in 2020. As digitalisation becomes pervasive, we will be exposed to a wide range of cyberattacks, cybercrime, and other online harms.

5. A safe and secure cyberspace is the foundation of a sustainable digital future. It allows us to trust the technologies that we use and gives us the confidence to continue on our digitalisation journeys.

6. This year's ASEAN chairmanship theme, "Addressing Challenges Together", is an apt rallying call. In the area of cybersecurity, we must act and address challenges in unity, to build a sustainable digital future together.

Implementation of the ASEAN Cyber Cooperation Strategy is Key

7. ASEAN has certainly made significant strides in strengthening our collective cybersecurity. In January this year, the second ASEAN Cybersecurity Cooperation Strategy was adopted during the 2nd ASEAN Digital Ministers' Meeting (ADGMIN).

8. Together with other initiatives undertaken at various ASEAN meetings, the Strategy will help advance cooperation among our countries and strengthen our regional cybersecurity posture. Singapore looks forward to working with our ASEAN partners to implement this Strategy over the next few years.

9. One key initiative in the Strategy is the establishment of an ASEAN Regional Computer Emergency Response Team (or CERT). We have conducted the ASEAN CERT Incident Drill (ACID) annually since 2006, to strengthen the preparedness of our countries' CERTs. Given the growing sophistication of cyberattacks, ASEAN Member States recognise that we need to be even more intentional in strengthening regional CERT-to-CERT collaboration. ASEAN Member States therefore agreed to establish an ASEAN Regional CERT as part of the Strategy adopted.

10. This is an important step in building regional cyber resilience. Now, the next step is to continue our good momentum to operationalise the ASEAN Regional CERT. What are we seeking to achieve? We envision the regional CERT to be a virtual centre comprising analysts and incident responders from across ASEAN. They will work closely to ensure timely information sharing during an incident. For example, if a supply-chain attack were to occur in any of our countries, regional CERT analysts would rapidly share information from their own countries and jointly develop advisories when needed. In other words, we are weaving a tighter net that will hopefully help to prevent cyber attackers from getting through too easily.

11. Singapore has circulated a draft Operational Framework and we look forward to your inputs.

Strengthening the Rules-Based Multilateral Order in Cyberspace is our Collective Responsibility

12. Having strong operational capabilities is just one aspect of our cyber resilience. A safe and secure cyberspace is also supported by the adoption and effective implementation of rules, norms and principles of responsible State behaviour in cyberspace.

13. All of us in ASEAN appreciate the importance of an open, secure, stable and interoperable cyberspace, based on mutual trust and confidence. We have the distinction of being the first and the only regional grouping to have subscribed in-principle to the eleven voluntary, non-binding norms of responsible State behaviour in the use of ICTs.

14. Capacity building is the bedrock supporting States in improving our collective cyber resilience. Since the launch of the ASEAN Cyber Capacity Programme in 2016, Singapore has hosted over 40 programmes and trained close to 1,500 officials from around the region. We will strengthen capacity building efforts within and beyond the region. For example, we had recently launched the UN-Singapore Cyber Fellowship to facilitate cross-regional learning with other UN Member States.

15. Developing the "rules of the road" for cyberspace requires deliberate and consistent effort. We need to actively implement the eleven voluntary and non-binding norms. I am therefore pleased to note that the ASEAN Regional Plan of Action on the Implementation of

Norms of Responsible State Behaviour in Cyberspace was endorsed last year when we met virtually. We had agreed at the time that subscribing to the principles was a good first step, but it needs to be supported by a concrete Plan of Action in order to put those principles into practice. The Plan of Action therefore outlines concrete steps that states could take, and also identifies specific areas that countries can focus on for capacity building.

16. At the UN, the ongoing five-year Open Ended Working Group (OEWG) continues to build on the work of previous international cyber norms discussions. As Chair of the OEWG, we thank our ASEAN partners for your continued support and participation.

Conclusion

17. In closing, I want to reaffirm the significant progress that ASEAN has made towards a secure and resilient cyberspace. We have accomplished all these because we stand by the principle of “Addressing Challenges Together” to build a sustainable digital future for all our peoples.

18. I look forward to our discussions at the AMCC and I wish all of you a pleasant and fruitful time in Singapore. Thank you once again.

+++