Ministry of Communications and Information
An Engaged and Connected Singapore

Keynote Address by Mrs Josephine Teo, Minister for Communications and Information, at ASEAN Ministerial Conference on Cybersecurity (6 Oct 2021)

Your Excellencies

Secretary General of ASEAN, Dato Lim Jock Hoi

Senior Officials

Ladies and Gentlemen

1. Welcome to the 6th ASEAN Ministerial Conference on Cybersecurity (or AMCC). This is my first AMCC since assuming my new portfolio as Minister responsible for cybersecurity in Singapore. I am pleased to meet my ASEAN colleagues virtually today, and hope to meet all of you in-person when the COVID-19 situation permits.

UN Discussions on Cyberspace to strengthen Rules-Based Multilateral Order

2. The digital domain is increasingly driving every aspect of our lives – be it work, study or just connecting with people. The outage of Facebook, WhatsApp and Instagram only two days ago – and the disruption it caused around the world – demonstrates our reliance on digital services, and the importance of safeguarding the resilience of our networks.

3. The attendance by all ASEAN Member States (or AMS) today highlights the importance we all place on one key aspect of resilience, which is cybersecurity. It is also a demonstration of our strong commitment to the ASEAN theme this year under Brunei's chairmanship – "We Care, We Prepare, We Prosper".

4. And strengthening our collective cybersecurity is more important now than ever. Over the past year, we have seen a step-change in the cyber threat landscape.

5. **Supply chain and ransomware attacks are increasing in frequency, scale, and impact**. Just to name a few: we saw how the SolarWinds breach affected close to 18,000 customers in December 2020; how the Colonial Pipeline attack in May had serious real-world consequences in the US; and how the Kaseya VSA breach in July forced Swedish Coop supermarkets to close, more than 800 of them.

6. **These examples show the importance of strengthening our cybersecurity. They also highlight the need for international cooperation to build consensus** on the rules, norms, principles and standards governing cyberspace. Such efforts will help to ensure that States behave responsibly in their use of Information and Communications Technologies (or ICTs), so we can achieve an open, secure, and interoperable ICT environment. In doing so, we can also strengthen the rules-based multilateral order.

7. Like other AMS, Singapore welcomes the successful conclusion of two UN processes this year – the Open-Ended Working Group (OEWG) and Group of Governmental Experts (GGE). The processes have contributed to the rules-based order, which we all benefit from. Many AMS participated actively. ASEAN played two critical roles in these UN discussions.

8. **First, ASEAN helped to bring the concerns of AMS to the UN**. One example is the issue of cross-border Critical Information Infrastructure (or CII). Such CII are owned by private companies and provide essential services to many countries across national borders. AMS collectively agreed at the AMCC last year that we needed to strengthen the protection of such CII. This topic was then

raised at the OEWG and GGE. Both have since recognised the importance of raising the cybersecurity posture of cross-border CII.

9. **Second, ASEAN has adapted UN's recommendations to our unique operating environment.** ASEAN is the first – and to date, only – regional organisation that has subscribed in-principle to the 11 voluntary, non-binding norms of responsible State behaviour in cyberspace. This is anchored by our belief in implementing the international cyber stability framework within our region.

10. We are making further progress through the development of the ASEAN Regional Action Plan, which will guide regional norms implementation. To this end, Malaysia and Singapore recently organised a workshop with our ASEAN colleagues.

11. I look forward to the endorsement of the Regional Action Plan at the ASEAN Digital Ministers' Meeting in December.[1]

Strengthening Partnerships among AMS through Cyber Strategy, Cyber Ops-Tech Collaboration and Cyber Capacity Building

12. However, malicious cyber threat actors continue to enhance their modus operandi to bypass our defences. We cannot afford to lose momentum.

13. This entails AMS working together on three tracks – **cyber strategy, cyber ops-tech collaboration, and cyber capacity building**.

14. First, cyber strategy. The first ASEAN Cybersecurity Cooperation Strategy from 2017-2020 provided a roadmap for regional cooperation to achieve a safe and secure ASEAN cyberspace.

15. Since its adoption, we have seen much progress in policy coordination and incident response as one ASEAN. It is timely to update the Strategy for the next bound to address evolving challenges.

16. Singapore is happy to take the lead and we will discuss this as one of the agenda items later. The updated Strategy places stronger focus on initiatives to support the establishment of the rules-based order in cyberspace and ASEAN's Digital Masterplan 2025.

17. This involves moving forward on five action-oriented aspects: advancing cyber readiness cooperation; strengthening regional cyber policy coordination; enhancing trust in cyberspace; enhancing regional capacity building; and strengthening international cooperation. We hope for AMS' support of the updated Strategy.

18. Second, let me talk about cyber ops-tech collaboration. The recent global supply chain attacks have shown that the compromise of trusted software can affect many users downstream. Swift sharing of threat information is essential so that we gain a headstart to mitigate cyber-attacks.

19. We are establishing the ASEAN CERT and the ASEAN CERT Information Exchange Mechanism for precisely this purpose. These build on our existing partnerships and trust accrued over the years. The initiatives will strengthen our region's resilience against cyber threats.

20. Another way to safeguard our systems and networks against cyber-attacks is through technical standards development and implementation. Often, we are forced into a *reactive* position when dealing with cyber incidents. In fact, we would rather be *proactive* on cybersecurity, by making our systems, networks, and devices secure-by-design.

[1] The ASEAN Regional Action Plan also supports the development of the Norms Implementation Checklist, under the UN-Singapore Cyber Programme with the UN Office of Disarmament Affairs.

21. This involves working with countries and the private sector to develop and implement technical, objective cybersecurity standards in technologies like 5G and IoT. For example, Singapore launched the Cybersecurity Labelling Scheme for IoT devices last year. The Scheme allows consumers to easily identify the level of cybersecurity of IoT devices and encourages them to buy devices that are labelled as more secure.

22. AMS can collectively raise the cyber hygiene level in our region, by working towards a *common* baseline cybersecurity standard for IoT devices. Singapore would be happy to facilitate this conversation.

23. Third, cyber capacity building. This is a priority for the region as capacity building is the bedrock supporting States toward the implementation of the norms of responsible State behaviour in cyberspace.

24. At the 4th AMCC in 2019, we launched the ASEAN-Singapore Cybersecurity Centre of Excellence (or ASCCE) to support cyber capacity building efforts in the region. I am pleased to announce today the official opening of the ASCCE campus, which we will have the pleasure of virtually opening later with my fellow ASEAN Ministers.

25. The ASCCE adopts a *coordinated* regional effort to deliver capacity building programmes for ASEAN senior officials, through a 4M approach: multi-disciplinary, multi-stakeholder, modular and measurable. I look forward to the support from AMS, our Dialogue Partners, industry, academia and international organisations, as we gradually resume in-person programmes.

26. A core focus of our capacity building efforts is to take a regional approach. We aim to share experiences most relevant to our region and to establish a strong network of cyber officials in ASEAN. To this end, we will launch the ASCCE LinkedIn account to facilitate better communication and information sharing among our ASCCE alumni and partners.

How ASEAN can contribute to OEWG 2.0

27. However, cybersecurity is not just a *regional* issue – it is a *global* issue.

28. Come December, the new five-year UN OEWG on Security of and in the Use of ICTs will commence. We are honoured that it will be chaired by Singapore's Permanent Representative to the UN, Ambassador Burhan Gafoor. I thank AMS for your support of the Chair's election earlier this year.

29. The OEWG will build on the strong foundation of the OEWG and GGE consensus reports, and work on deeper discussions of key cyber issues.

30. As we embark on the next tranche of UN cyber discussions, I encourage AMS to actively contribute to the cyber stability framework – and collectively identify key issues of regional interest to value-add to the UN conversation.

31. As Chair of the OEWG, Singapore looks forward to your support. We are keen to hear your candid views, and work with you to move the discussion toward our shared objective of a secure, resilient, and interoperable cyberspace, not just regionally, but also globally.

32. This is how we can continue to show the world the strength of ASEAN's unity, and that: "We Care, We Prepare, We Prosper". Thank you, and I look forward to your active participation at the AMCC.