Opening Speech by S Iswaran, Minister for Communications and Information, Minister-in-Charge of Cybersecurity, at the 5th ASEAN Ministerial Conference on Cybersecurity on 7 Oct 2020 (live virtual broadcast)

"Regional Cyber Cooperation For A Secure And Vibrant Digital Future"

Your Excellencies
Secretary General of ASEAN, Dato Lim Jock Hoi
Senior Officials
Ladies and Gentlemen

1. A very warm welcome to the 5th ASEAN Ministerial Conference on Cybersecurity (AMCC). I want to thank all ASEAN Member States (AMS) for your attendance today, especially amidst this COVID-19 pandemic. We are not able to meet in person, but I am heartened that we can come together virtually, to convene this meeting as we have done every year over the past four years.

2. As we all know, COVID-19 has disrupted global trade and supply chains, it has reshaped how we live, we work and we play. Perhaps more significantly for our discussions today, it has reinforced the digital imperative. Though it was born of necessity, the push towards digitalisation has also sparked innovation and accelerated the growth of the digital economy. Despite the economic toll of COVID-19 on our region and the global economy, Southeast Asia remains well-positioned to capitalise on this digital trajectory. Yet, as our digital economy grows, so too does the cyber threat attack surface. Today, we face an unprecedented level of exposure to cyber threats. A safe and secure digital infrastructure must undergird our digital economy ambitions for the region. It is more important than ever for ASEAN to tackle the challenge of cybersecurity together, in a sustained, holistic and coordinated manner.

3. Since its inception, the AMCC has made significant progress in advancing cross-cutting and wide-ranging discussions on possible areas for ASEAN regional cybersecurity cooperation. This afternoon, I look forward to deepening our cybersecurity cooperation as we discuss two important topics. First, **building a rules-based cyberspace**, focusing on our regional norms implementation workplan. Second, **strengthening our regional cyber resilience through Critical Information Infrastructure (CII) protection.**

<u>Building a Rules-Based Cyberspace: Regional Norms and Implementation Workplan and Capacity Building</u>

4. For a cyberspace that is open, secure, stable, accessible, and peaceful, we must maintain a rules-based international order. To do so will be increasingly challenging, against the backdrop of a volatile and fractious global landscape caused by growing geopolitical tensions as well as rising protectionism. Therefore, we have to double down on efforts to create robust rules and engender international collaboration for greater cyber resilience and stability.

5. ASEAN's shared commitment to foster a rules-based cyberspace has enabled us to successfully advance discussions on cybersecurity policy and regional coordination.

a. At the 3rd AMCC in 2018, AMS Ministers agreed to consider a formal regional mechanism to coordinate cybersecurity matters, and to study the adoption and implementation of the 11 norms of responsible state behaviour in cyberspace from the 2015 UN Group of Governmental Experts (UNGGE) Consensus report. It is noteworthy that ASEAN was the first regional body to subscribe in-principle to these norms.

b. At the 4th AMCC last year, we went one step further to discuss how to implement the norms and the capacities required, taking into account the different considerations of the ASEAN Member States. We established a working-level committee chaired by Malaysia to develop a long-term **regional action plan**, to ensure the effective and practical implementation of norms. I, and all of us, look forward to hearing updates from our Malaysian colleagues later, as we advance into identifying specific areas of focus for the AMS.

6. ASEAN also shares a common focus on capacity building. We have made significant progress in regional cyber capacity building through initiatives such as the ASEAN-Japan Cybersecurity Capacity Building Centre in Bangkok, and the ASEAN-Singapore Cybersecurity Centre of Excellence in Singapore. Singapore is committed to step up our efforts, with a view to working with our partners to roll out more capacity building programmes in the coming months.

<u>Strengthening Regional Cyber Resilience Through CII Protection</u>

7. Like many other ASEAN States, we are concerned also with safeguarding Critical Information Infrastructure within our jurisdiction. CIIs constitute national assets which form the backbone of our societies' most vital functions, services and activities. Many cities within ASEAN serve as key hubs for services spanning the banking and finance, telecommunications, aviation and maritime sectors. Thus, the impact of a cyberattack on a national CII may not be confined to that country alone, but also felt in other parts of the region and even the world. Many member states recognise the risks and are

taking proactive steps to protect their national CIIs. These efforts are in line with the UNGGE norms that we have agreed upon.

8. Beyond protecting national CIIs, ASEAN can do more to strengthen regional cyber resilience by safeguarding CIIs with cross-border impact, such as common cloud and banking systems. In fact, the significance of the Cloud has been heightened because of the pandemic and the response from industry. The need to secure these CIIs cannot be overstated. A cyberattack on any of these might cause wide-ranging disruptions to multiple states in essential services, including those related to international trade, transport, and communications. AMS must find ways to cooperate closely with CII owners to prevent and mitigate the impact of such disruptions. To this end, I look forward to the sharing by our colleagues from Thailand on CII protection.

<u>Enhancing Security for Operational Technology and Internet of Things</u>

9. Apart from cross-border CIIs, Singapore continues to ramp up our cybersecurity in the areas of Operational Technology (OT), and the Internet of Things (IoT). The OT and IoT landscapes are fast-evolving and pose distinctive threats and risks. A successful cyberattack on an OT system may manifest as a severe disruption in the physical world. For IoT, the challenge is defending at scale, as the proliferation of smart devices gives rise to a potentially huge attack surface. Singapore recognises that we cannot address these threats alone. We will work with regional and international partners whom we have already been collaborating with, including the industry, to catalyse the development of local capabilities and competencies in Operational Technology and IoT cybersecurity.

a. OT systems, including those in the energy, water and transport sectors, are vital to deliver essential services and support the economy. To augment our OT Cybersecurity Masterplan that was launched last year, I am pleased to announce that the Cyber Security Agency of Singapore (CSA) will establish an **OT Cybersecurity Expert Panel (OTCEP)** comprising internationally renowned practitioners, to advise government agencies and stakeholders on strategies to enhance the resilience of our OT systems. As we noted last year and our Senior Minister made the point, we often focus in our cybersecurity effort on the ICT side, but the OT aspect is one that is equally important and that deserves the kind of attention that we are giving it today at the national level and at the regional level.

b. To strengthen our IoT cybersecurity, I am also happy to announce the launch of the **Cybersecurity Labelling Scheme (CLS)** by CSA. The scheme is the first of its kind in the Asia-Pacific. It establishes cybersecurity rating levels for registered smart devices, such as home routers and smart home hubs.

Manufacturers of IoT devices can voluntarily apply for the CLS. With the labels, consumers can easily assess the level of security of each device and make informed purchasing choices. CSA plans to work with ASEAN member states and other international partners to establish mutual recognition arrangements for the CLS to enhance security standards of the global IoT device market. This takes on added significance when we consider the potential of 5G and the proliferation of IoT devices.

Conclusion

10. In closing, I would like to once again thank the ASEAN Member States for your steadfast commitment to strengthen cybersecurity, at home and in collaboration with regional and international partners. As our region's digital economy and society continues to grow, ASEAN's collective efforts to secure our digital infrastructure and safeguard our cyberspace will be crucial. Let me assure you that Singapore stands ready to work with all our ASEAN partners in this regard, so that our people and businesses can thrive in a safe digital future.

11. I look forward to building on the progress we have achieved in past AMCCs, also to a fruitful and stimulating discussion with all of you this afternoon. Thank you for joining us today in this virtual format.