REMARKS BY MR DAVID KOH, CHIEF EXECUTIVE, CYBER SECURITY AGENCY OF SINGAPORE AT THE UNITED NATIONS SECURITY COUNCIL ARRIA FORMULA MEETING ON 22 MAY 2020

Mr President,

Under-Secretary-General and High Representative for Disarmament Affairs of the United Nations, Ms Izumi Nakamitsu,

Director for Technology Policy at the Centre for Strategic and International Studies, Dr James Lewis,

Excellencies,

I am honoured to have been invited by Estonia to speak at the UN Security Council today. I thank Estonia, Belgium, the Dominican Republic, Indonesia, and Kenya for convening this meeting on a very important topic to the global community, which has become more pressing with the current COVID-19 crisis. This crisis has shown how important digital capabilities are, to ensure that essential services, effective governance, and communications can continue even in a highly disrupted environment. And all of this is underpinned by cyber security.

2 Let me begin by laying out some fundamental parameters that guide Singapore's thinking.

3 ***First***, Singapore's perspective is shaped by our geography, demography, and economy. We are a tiny nation-state located in a rapidly developing region of the world. We are also one of the world's most digitally connected cities.

4 Singapore is a gateway to Southeast Asia and the larger Asia-Pacific region. We are a major banking, aviation and maritime hub; a significant proportion of the world's financial capital, air traffic, and freight flows through our borders.

5 We are a small but highly-connected country, and this will become more intense under our Smart Nation initiative. We do not claim to have the model answer for navigating this "wild, wild west" of cyberspace, but we are happy to share our experiences with UN Member States, and catalyse further ideas on how we can work together to deal with cyber threats.

6 Forced by the current crisis, the trend for more and more activities to go online looks irreversible. The more digitalised our world becomes, the more important cybersecurity is; we need a trusted, reliable digital space so that we can transact with confidence.

7 ***Second***, the financial cost of cyber attacks can be high, but indirect costs, such as the loss of public confidence and trust, can be even higher. Preserving public trust is especially critical as governments and international organisations manage the pandemic, and find ways

to rebuild. Preserving and increasing trust among States is equally important, to forge a united response to the current challenges and to prevent conflict.

8 ***Third***, the transboundary and continually evolving nature of cybersecurity challenges requires national, regional, and international responses. To complement national and regional approaches, it is necessary for the international community to develop principles, norms, and rules of responsible State behaviour in cyberspace and implement effective Confidence Building Measures (CBMs). These elements underpin the development of a stable multilateral framework or a rules-based international order in cyberspace.

The UN's Role in Cyber Discussions

9 With its universal membership, and guided by the principle of sovereign equality, the UN General Assembly has the legitimacy and credibility to host cyber discussions; to adopt and implement the international cyber stability and resilience framework, developed in an open, inclusive, and collaborative manner. It is here at the UN where we need to drive international cooperation to raise awareness of cyber challenges to international peace and security, and to make progress on advancing responsible State behaviour in cyberspace.

10 Let me propose three points as food for thought.

Cybersecurity as a Key Enabler of the Digital Future

11 First, cybersecurity is a key enabler and undergirds our modern way of life. As more of how we work, live, and play goes digital, the cyber-attack surface also increases exponentially. Attacks on our Critical Information Infrastructure (CIIs) will disrupt the provision of essential services to our citizens.

12 Singapore's priority is to ensure that our CIIs have the capabilities and measures in place to detect, respond, and recover from cyber threats in a prompt and expedient manner. However, the present crisis has also revealed new services which have now become essential to this new way of life. Examples include online grocery shopping or food delivery services – these were non-CII services which have become important virtually overnight. A safer cyberspace is important not just for CIIs, but also businesses and non-CII sectors.

13 At the same time, we must not forget about another class of CIIs which we have termed "supranational CIIs". The international community needs to look at ways to safeguard supranational CIIs such as banking, finance, communications and aviation – these are owned by private companies, and operate across national borders, and they are not under any one state's jurisdiction.

International Collaboration to Build Trust

14 Second, international cooperation is necessary to establish a stable, rules-based order in cyberspace.

15 In recent years, there has been significant progress on recognising the need for international dialogue and collaboration on cyber. Here at the UN, there have been substantive discussions at both the UN Group of Governmental Experts (GGE) and the newly-established Open-Ended Working Group (OEWG).

16 In particular, consistent engagement at the OEWG and GGE, and in other international fora builds networks of relationships and mutual trust. This is an important enabler as we seek to establish common norms, or "rules of the road" if you will, for responsible State behaviour in cyberspace.

17 In these dialogues, it is important to take the range of voices into account, especially the views of small and developing states. Our push for universal implementation needs to be underpinned by a sense of legitimacy that can only come about from wide, broad-based support.

18 It is also important to include voices of other stakeholders in these discussions. Governments do not have a monopoly on the solutions to cyber challenges. We need to forge more public-private partnerships, especially with industry. Some areas that merit greater attention include capacity building, threat assessment and information sharing.

A Continued Need for Capacity Building

19 Third, there remains an urgent need to build capacity among and within countries.

20 The diverse domestic organisational structures for cybersecurity in each country, the cross-cutting nature of the cyber domain where responsibility for cybersecurity does not fall on any one agency, and different capacities in each country, must be taken into account as we seek to build international and regional cyber security and resilience.

21 Regional organisations are ideally placed to undertake and lead in such efforts. The Association of Southeast Asian Nations, or ASEAN, has worked to coordinate regional cyber policy initiatives with robust capacity building. For example, during Singapore's ASEAN chairmanship in 2018, ASEAN Leaders issued the first ever ASEAN Leaders' Statement on Cybersecurity Cooperation calling for greater coordination of cybersecurity efforts within ASEAN on cyber policy, norms, CBMs, and capacity-building.

22 ASEAN Cybersecurity and Digital Ministers continue to discuss on practical ways to implement the guidance of Leaders. For example, ASEAN Ministers and Senior Officials meeting at the informal ASEAN Ministerial Conference on Cybersecurity subscribed in-principle to the 11 voluntary, non-binding norms recommended in the 2015 UNGGE Consensus Report. This made ASEAN the first and thus far, only regional grouping to do so.

23 These discussions are complemented at the practical level by discussions, workshops and drills undertaken by platforms such as the ASEAN Regional Forum Intersessional Meeting on the Security of and in the Use of Information and Communications Technologies.

24 Regional capacity-building continues to be a key priority for Singapore. We began with the S$10 million ASEAN Cyber Capacity Programme in 2016, which has now been extended to the S$30 million ASEAN-Singapore Cybersecurity Centre of Excellence.

25 Regional capacity building is a building block for better international cooperation. To this end, Singapore is also working with the UN and other international partners to conduct awareness building and workshops on various aspects of cyber diplomacy, including norms and CBMs.

Conclusion

26 In conclusion, from Singapore’s perspective, ensuring a resilient and secure cyberspace cannot be done alone. Collaboration among governments, businesses, academia, and individuals across multiple fronts will be crucial to our success. Especially during these times of the pandemic, the international community must come together to resist efforts to exploit fears, disrupt computer systems and networks, and to hamper our response.

27 Moving forward, it is important not just to build defences for the cyber-threats of today, but also to develop the infrastructure, capabilities, and relationships that will enable us, as an international community, to tackle the cyber challenges of tomorrow.

28 Thank you.