**KEYNOTE REMARKS BY CE/CSA AT THE UNIDIR-CSIS WORKSHOP ON THE ROLE OF REGIONAL ORGANISATIONS IN STRENGTHENING CYBERSECURITY AND STABILITY, THURSDAY 24 JANUARY 2019, 2.00-2.30PM, ROOM XXII PALAIS DES NATIONS, UN OFFICE AT GENEVA**

- Good afternoon. I am honoured to have the opportunity to speak to all of you at this workshop today. We are gathered here at a time when international discussions on cyber policy issues, such as those on cyber norms, attribution and the applicability of international law to cyberspace at the UN have entered a decidedly new phase. In the coming months, we will see the potential establishment of an Open-Ended Working Group as well as a new UN Group of Governmental Experts to discuss these issues.

- Regional organisations have an immense, untapped potential to support and shape this wider international process, such as those at the United Nations. This does not mean that the work of regional organisations can replace those at the international level. Cyber is an international, or 'Olympics-level' problem. The continuation of strong international cyber discussions such as

those at the UN are crucial to tackling this problem in a holistic way. Rather, efforts undertaken at the regional level can instead complement established international dialogues on cyber by firstly, representing regional perspectives at the wider international discussions; and secondly, helping build awareness of these outcomes in the various regions and driving the implementation of internationally-agreed decisions in their respective regions. Unfortunately, inter-regional cybersecurity cooperation is also a topic that is not discussed enough.

***The Current State of Play***

- There has no doubt been good progress in cybersecurity made within our respective regions in the recent years. In this regard, there has been excellent work done within regional groupings such as the Organisation of American States (OAS), the Organisation for Security and Cooperation in Europe (OSCE), as well as the Association of Southeast Asian Nations (ASEAN) on areas such as cyber norms, confidence building measures (CBMs) and capacity building.

- In this regard, it may be worthwhile to note part of this success is due to the fact that regional groupings are better-placed to initiate and coordinate certain types of cybersecurity initiatives, as compared to individual States and even international fora like the UN. Regional groupings have a more intimate grasp of the cyber developmental needs, state of cyber readiness and on-the-ground policy and socio-historical issues in the countries belonging to their region. As such, regional groupings are able to bring value to areas such as the implementation of norms, CBMs and capacity building, by applying these in a timely and relevant manner across their respective regions. This is something that no individual State can hope to achieve by itself.
- Singapore has been privileged to work with our other ASEAN and ASEAN Dialogue Partner countries to move cybersecurity norms, Confidence Building Measures (CBMs) and capacity building discussions within our region. From the policy perspective, we have worked to draft a first-ever ASEAN Leaders' Statement on Cybersecurity Cooperation during Singapore's ASEAN Chairmanship in 2018.

- Through this Statement, Leaders' affirmed their support and commitment to a rules-based international order in cyberspace and tasked relevant Ministers to firstly, identify a suitable mechanism or platform for coordinating cybersecurity policy, diplomacy, cooperation, technical and capacity building efforts across ASEAN; and secondly, to identify a concrete list of voluntary, practical norms of State behavior in cyberspace that ASEAN can work towards adopting and implementing, taking reference from the 11 voluntary norms recommended in the 2015 UNGGE Report.

- At the 3rd ASEAN Ministerial Conference on Cybersecurity (AMCC) hosted by Singapore in September 2018, ASEAN ICT and Cybersecurity Ministers and Senior Officials acted on these instructions, expressing support for a Study to be conducted on the possible establishment of a separate mechanism for regional cybersecurity discussions. AMCC Participants also agreed to subscribe in-principle to the 11 voluntary, non-binding norms recommended in the 2015 UNGGE Report, as well as to focus on regional capacity building in implementing these norms.

- These decisions at the AMCC were noted in the ASEAN Summit Chairman's Statement of November 2018. Singapore has been given the mandate to lead the study on an appropriate regional mechanism for cybersecurity.

- Separately, Singapore has also decided to expand its ongoing ASEAN Cyber Capacity Programme (ACCP) with the set-up of a SGD 30 million ASEAN-Singapore Cybersecurity Centre of Excellence (ASCCE). The ASCCE, which will be fully functional later this year, will focus on working with a range of international and regional partners – including countries, regional organisations, industry and academic institutions – to build cybersecurity policy-making, strategy development as well as technical and operational capacity in ASEAN.

- Our Thai colleagues have also worked with Japan to set up a ASEAN-Japan Cybersecurity Capacity Building Centre (AJCCBC) in Bangkok. The Thai Centre will provide human resource training programmes for regional ICT officials.

- Singapore, Malaysia and Japan also co-chair the newly established ASEAN Regional Forum Inter-Sessional Meeting on ICTs Security (ARF ISM-ICTs), which has already in its first year worked towards identifying and implementing 5 cyber CBMs.

- Taken together, these initiatives will potentially allow ASEAN Member States including Singapore, to improve our collective capacity to implement a trusted and secure rules-based cyber environment in the regional ASEAN cyberspace, and also to participate effectively and contribute to international discussions, speaking as one region with one voice.

- ASEAN is not alone in this. The Organisation for Security and Cooperation in Europe (OSCE) has also moved forward to implement initiatives in the areas such as cyber CBMs. As of 2016, the OSCE now has a total of 16 CBMs, many of which are designed to facilitate communication and information sharing among member States, so as to reduce the risk of conflict arising from the use of ICTs.

- Likewise, the Organisation of American States (OAS) has built up a considerable arsenal of resources through the implementation of various initiatives. This includes a handbook on best practices for establishing a national CSIRT as well as various online courses on cybersecurity topics to raise awareness on developing trends and tools, all targeted at helping Member States strengthen their domestic cyber capabilities.

***The Cooperation Game – Levelling Up Regional Cooperation on Cybersecurity***

- As significant as these regional initiatives have been, more can be done. From our ASEAN perspective, regional organisations can play a key role in supporting international cyber discussions in three specific areas: (a) raising awareness on international cyber policy issues; (b) the implementation of robust CBMs; and (c) coordinating effective capacity building.

- Let me cover each of these areas in turn:
    - <u>Raising Awareness</u>

- As cybersecurity is a nascent area for most countries, it is not uncommon for States to be faced with a fragmented domestic cyber landscape where one part of the Government does not know what the other is doing. As such, there is often a lack of awareness in some Ministries on cyber issues because the 'news does not trickle down'. For instance, we not infrequently encounter participants in our capacity building programmes and workshops wondering about the exact nature of the UNGGE, what the norms means, or even what the Tallinn process is! Sometimes, our discussions start from the perspective that everyone knows that we are talking about – but this is not so. The lack of awareness can sometimes lead to a delay or even a stopping of cooperation and adoption of norms and CBMs. Regional organisations can therefore play a key role in fostering dialogue and raising awareness.

- Implementation of Robust CBMs
    - CBMs can be very effective tools in reducing the risk of cyber conflict and increasing trust and confidence in cyberspace. CBMs such as the sharing of strategies and legislation, exchanging of points of contact also reduce misperceptions. Sadly, CBMs have not received the same attention as norms. Regional organisations can play a crucial role in advancing the discussion and implementation of meaningful CBMs in their regions, because they know their region best.

- Coordinated Cybersecurity Capacity Building
    - Singapore believes that cyber stability consists of 3 sides of a mutually self-enforcing triangle: i) raising awareness on norms of responsible State behaviour in cyberspace, (ii) coordinated capacity building, and (iii) CBMs. States can only effectively implement rules norms and CBMs when they have the capacity to do so. To be truly effective cap building must be coordinated, so as to ensure the best use of resources,

and also to ensure that the capacity building is meaningful. To be meaningful, the programmes must identify the individual country's needs in a systematic fashion, tailor programmes to address these needs, have appropriate mechanics to measure success and ensure that follow-on workshops are held to deepen the learning.

- Regional organisations can play a vital role in supporting discussions in this area. Singapore has worked with our ASEAN partners to address this through the **ASEAN Cybersecurity Cooperation Strategy**, which aims to provide a roadmap for regional cooperation through a framework that enables Member States to identify areas of collaboration and subsequently assess the progress made in various areas including cybersecurity incident response and CERT policy and coordination.

***The Need for Cooperation Between Regions***

- A key distinctive of these ASEAN regional initiatives is that we constantly align and take reference to international efforts in framing regional cooperation. Given the transboundary nature of cyber, it would not make sense for each region to develop its own unique set of rules, norms and CBMs. Regions have to work together.

- Such cooperation between regions would allow us to align regional efforts as well as identify areas where can do joint capacity building. A key contribution that such cooperation between regions can make is the development of a common vocabulary or glossary of cybersecurity terms that will allow dialogue to be more effectively carried out at the international level.
- Dialogue between regions can also be an effective way of exchanging common perspectives on the implementation of norms and CBMs – and in time to come, may even give rise to the standardisation of norms and CBMs adopted in individual

regions, taking reference from decisions made at the international discussions such as those at the UNGGE and OEWG.

- Singapore has taken the first step to contribute to such inter-regional dialogue and cooperation. As a start, Singapore and the UK have, in September 2018, embarked on a 2-year **Commonwealth Cyber Capacity Programme** comprising various capacity building initiatives in areas such as cyber incident response. We are also working with the UN Office of Disarmament Affairs (UNODA) to implement a **Joint United Nations-Singapore Cyber Programme (UNSCP)**, to be run out of the new ASCCE. This programme encompasses two workshops to raise awareness on cyber norms and cyber policy, and will be run annually over a period of three years for senior ASEAN government officials.

***Singapore can help foster inter-regional dialogue***

- In sum, organisations like UNIDIR can play a key role in fostering such discussions between regions. Singapore would

therefore be happy to be part of the nucleus responsible for initiating such inter-regional exchanges.

- We would be most willing to host such discussions at our annual Singapore International Cyber Week, and hope to have the opportunity to work together with UNIDR and other regional groupings in this effort. Having said that, I would like to reiterate that it is important that our work in this area should be done in support of wider international processes, especially those taking place at the UN.

***Conclusion***

- This conference is a good first step in exploring the many possibilities for inter-regional cooperation. I look forward to participating in the discussions this afternoon. Thank you.

***