Remarks by the Centre of Excellence for National Security (CENS), S Rajaratnam School of International Studies (RSIS) to the UN OEWG ICTs 2021-2025 7th Substantive Session - Wednesday, 5 March 2024, 3 pm – 6 pm EST

1. We thank the Chair for the opportunity to speak to the 7th Substantive Session of the Open-Ended Working Group. We thank the chair for continuing to hear input from all stakeholders, including those that have not been accredited at your Virtual Informal Dialogue last week. We hope that the useful stakeholder views that have been shared with the chair at the Virtual Informal Dialogue can be shared with the wider OEWG as a Chair's paper.

2. We make the following points based on the ongoing discussions this week, our experiences in capacity building in the ASEAN region with the UN Singapore Cyber Fellowship, and our other projects as a policy research think tank in Singapore.

3. We agree that Confidence Building Measures are more important than ever. We agree with the Chair that these meetings are a form of CBM because of information sharing and greater transparency. We observe from the discussions these past 3 days that there are two areas where greater confidence needs to be built: **(1) critical information infrastructure (CII) protection and (2) artificial intelligence (AI) threats vis-à-vis the use of ICTs.**

4. **First, for CII protection, we recommend engaging stakeholders like CII operators and practitioners.** Compared to our work in assisting the review of Singapore's Operational Technology Cybersecurity Masterplan, we observe a paucity of CII protection practitioners or CII operators at the OEWG formal and informal sessions. Some states do engage their CII operators or practitioners domestically, but we recommend engaging them at a global level, so the OEWG can concretely understand the threats they are facing, and then develop relevant and actionable responses.

   Academic stakeholders like us are ready to help to facilitate a study group or panel for states and CII operators on CI and CII protection. The objectives can include capacity building for both technical and policy experts; exchanging information on existing and potential threats to CI and CII and possible cooperative measures; creating learning opportunities from global experts and practitioners; and building understanding the fundamental principles behind national policies and strategies for CII protection. We believe this will be relevant to the agreements in the 2nd Annual Progress Report, specifically Paragraphs 12, 13, 17, and 23(c).

   We also call on states to involve their CII operators and practitioners in the ongoing discussions at the OEWG, the Global Roundtable on Capacity Building, and the inter-sessional meetings in May, as this will benefit the wider OEWG.

5. **Secondly, for Artificial Intelligence, we recommend engaging relevant experts.** We agree with Switzerland's assessment that AI should be viewed in a balanced manner and brings many more opportunities for development and improvements in security than there are threats arising from the use of AI. We echo Argentina's call for a multi-stakeholder study group, as this can help better understand the threat and opportunities in a balanced manner.

   Academic stakeholders like us are ready to help to facilitate a study group or panel for states and AI experts on the role of responsible state behaviour in responding to artificial intelligence and other emerging technologies. From our experience working with AI experts in AI Governance projects in Singapore, and in AI Standards Setting with ISO, we suggest that there are 3 aspects where experts can help with capacity building for smaller states:

   a. Cyber threats to AI systems

   b. Cyber and information threats enabled or enhanced by AI, and

   c. What may constitute responsible state behaviour in respect of these threats.

6. In conclusion, we, as the stakeholder community, reiterate that we are ready to collaborate with interested states and stakeholders, regardless of accreditation status, to help the OEWG deepen understandings and make informed decisions on the rapidly evolving threat landscape. We call on states and stakeholders to work together as a matter of priority.

7. We thank you chair.

Benjamin Ang
Head and Senior Fellow
Centre of Excellence for National Security

Eugene EG Tan
Associate Research Fellow
Centre of Excellence for National Security