Remarks by the Centre of Excellence for National Security (CENS), S Rajaratnam School of International Studies (RSIS) to the UN OEWG ICTs 2021-2025 Informal Inter-sessional Meetings on Capacity Building - Thursday, 9 March 2023, 3 pm – 6 pm EST

1. We thank the Chair for the opportunity to speak to this informal inter-sessional meeting of the Open-Ended Working Group on the theme – Capacity Building, and in particular, the role of public-private partnerships for capacity building. We further thank the chair for his efforts to continue including all stakeholders, in formal and informal and hybrid formats of the OEWG.

2. We wish to respond to your guiding questions from our perspective as an independent national security policy research think tank from Singapore, based on what we have observed while conducting cyber capacity building workshops and events in ASEAN and beyond.

3. **Are there good examples of public-private partnerships on capacity-building in the area of security of and in the use of ICTs?** We share examples that we have assisted in: The UN Singapore Cyber Programme and the UN Singapore Cyber Fellowship. In these programmes, non-government stakeholders provided an objective, textured and non-political approach to discussions on the topics relevant to this OEWG, such as the norms implementation checklist, and the applicability and scope of international law to the use of ICTs.

   Non-government stakeholders can therefore facilitate difficult discussions, such as state sovereignty, sovereign equality, and non-interference, definitions of what amounts to threat or use of force in cyber operations, the principle of due diligence, whether there is a need for a binding legal instrument, the operationalisation of the Points-of-Contact directory, and the surfacing of cyber threats.

   As part of capacity building activities, non-government stakeholders can bridge gaps in International Law, by convening in-depth discussions and study groups, for both Track 1 and Track 2, and assisting states in developing position papers for the OEWG to consider, even on topics that may be controversial.

   The OEWG can support non-government stakeholders to engage other regional stakeholders that are not yet engaged in the process but have relevant expertise, such as multinational companies or think tanks, to provide capacity building on transnational issues, such as protection of transnational critical infrastructure.

   The OEWG can also invite non-government stakeholders, who have assisted in these external capacity-building programmes, to present their lessons learned and best practices to the OEWG so that all member states can benefit. This can be done irrespective of their accreditation status to the substantive sessions.

4. **Are there lessons that can be gleaned from those examples?** We have found that participants learn best when no-government stakeholders present in-depth technical assessment case studies in an academic manner, without political finger pointing over the actions of any state.

5. We observe, from the public-private collaboration in the UN Singapore Cyber Programme, that states that pursue an approach of engaging non-government stakeholders engender systemic confidence through the mutual building of capacity between states and non-state stakeholders.

6. Public-private cooperation also helps threat intelligence sharing, when states and private sector have issued advisories over vulnerabilities in software being used by both public and private agencies. We see such joint disclosures by public and private agencies strengthen the corresponding norm of responsible state behaviour in managing vulnerabilities, and help confidence building in the international community.

7. We therefore sincerely hope that states can come to consensus in this OEWG on regulating the actions of state actors, and for states to live up to their commitments and obligations agreed to in the acquis in the OEWG and UNGGE processes.

8. For States to gain the most benefit, we encourage all states to take advantage of the programmes like the UN Singapore Cyber Fellowship, and actively engage stakeholders like us within and outside the framework of the OEWG. We are keen to share our research through briefings, workshops, and papers, and we hope that states are also open to receive.

9. Thank you Chair.

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

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