RSiS S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES
Nanyang Technological University, Singapore

For the 6th meeting of the OEWG

To: estatements@un.org
Cc: Katherine Prizeman, UNODA (prizeman@un.org) for posting to OEWG site
Cc: Allison Pytlak (allison.pytlak@wilpf.org) for WILPF

27 July 2022

Remarks by the Centre of Excellence for National Security (CENS), S Rajaratnam School of International Studies (RSIS) to the UN OEWG ICTs 2021-2025 Third Substantive Session - Wednesday, 27 July, 3 pm - 6pm EST

1. We thank the Chair for the opportunity to speak to the third substantive session of the open-ended working group. We further thank the chair for his efforts to include non-government stakeholders like us in the formal processes of the OEWG, as well as continuing the conversation informally, as he was able to include stakeholders who were not accredited for this formal session.

2. We also thank the chair for his guiding questions. We wish to respond to the first set of questions posed by the chair on capacity building.

3. Our contribution is based on what we have learned while conducting capacity building efforts in ASEAN and beyond. CENS is an independent national security policy research think tank from Singapore, based at the RSIS graduate school.

   We provide trainers for the UNSCP (UN Singapore Cyber Program) capacity building programme for ASEAN, and other initiatives for capacity building in ASEAN. These include workshops for ASEAN delegates on, among other things, the meaning of the Norms, and the development of the Norms Implementation Checklist, which we have expanded to other interested States.

   We also contributed content to the UN Cyber Diplomacy online course which is available to all interested States and stakeholders. We will also be providing trainers for the UN Singapore Cyber Fellowship.

4. We share three observations from our experience:

   (1) We observe that participants at our workshops have been very eager to engage the topic and learn from stakeholders. We recognise that every state is at different level of cyber maturity, but over the years, many delegates who participated in the programmes have taken what they have learnt back to their respective states, and when they return in the following years, are able to report progress both on a personal and institutional level. We therefore encourage all stakeholders who support capacity building to continue to do so.

   (2) We observe that participants benefit from a multi-stakeholder approach to capacity building, with academia providing frameworks, industry providing technical expertise, civil society providing perspectives, and state participants frankly sharing their experiences and challenges.

   This has been instrumental in delivering value and holistic capacity to participants and is much better than a siloed approach, because in a siloed approach, the proposed academic or policy frameworks may not be technically feasible, or technical proposals may be blind to public and private interests.

   We therefore urge all stakeholders to work across domains when conducting capacity building, combining academia, civil society, private sector, and public sector.

   (3) We observe that participants share the chair's desire for sustained and substantive capacity building that is inclusive and builds confidence among states. We look forward to proposals to develop neutral and inclusive capacity building programmes to avoid politicisation and improve access to these programmes.

5. In conclusion, we have observed a wide range of capacity building aspects that stakeholder groups can contribute to in a concrete and action-oriented way, including (1) the application of international law to the use of ICT, (2) CERT to CERT cooperation and confidence building measures, and (3) technological aspects of protecting critical infrastructure.

   We therefore encourage states to continue working with stakeholders, stakeholders to continue engaging with states, and stakeholders to work with other stakeholders, on capacity building and other issues relating to ICT security.

This can carry on regardless of whether the stakeholders are accredited to attend formal sessions or not, as capacity building is ongoing all the time. It is in the interest of the global community that we find ways to cooperate even when it is inconvenient to do so and look forward for ways to deepen capacity building measures to ensure security and stability in the use of ICT.

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