24 March 2022

Representation to the Chair of the Open-Ended Working Group on security of and in the use of information and communications technologies 2021-2025 (OEWG), at the Virtual Informal Dialogue on 24 March 2022

Thank you Chair for the opportunity to speak. On behalf of the Centre of Excellence for National Security at the S Rajaratnam School of International Studies in Singapore, we commend the chair for taking extra time to continue the conversation with all stakeholders, even in an informal and virtual setting. We also thank Bart Hogeveen, Head of Cyber Capacity Building at the International Cyber Policy Centre, Australian Strategy Policy Institute, for his endorsement of this statement.

Drawing from our experience over the past years assisting in cyber capacity building programmes and confidence building measures, together with the ASEAN Singapore Cyber Centre of Excellence and the UN Singapore Cyber Programme, we suggest four ways that stakeholders can assist Member States pursuant to the agenda in the Chair’s invitation letter.

1. **Stakeholders can assist Member States in confidence building measures through non-official communication pathways** to convey political thinking and practical solutions of member states, and technical cooperation between CERTS, especially in times where official diplomacy is inconvenient. This can help member states and stakeholders to re-establish a level of trust and confidence that the rules-based international order is respected.

2. **Stakeholders can assist Member States by providing advice on how to implement the existing rules, norms, and principles of responsible state behaviour, especially for small and developing states.** These may include training, private sector assistance in implementing due diligence, and assisting in attribution of cyberattacks.

3. **Stakeholders can assist Member States in holding accountable other states for actions that violate the existing rules, norms, and principles of responsible state behaviour.** Stakeholders can publish statements, communicate issues, take private sector actions, and advise on escalation, especially for small and developing states.
4. Stakeholders can continue to assist Member States and the UN in supporting cyber capacity building for smaller and developing states, to help the smaller and developing states to better voice their concerns during the Substantial Meetings, and to better implement the existing rules, norms, and principles of responsible state behaviour.

Thank you Chair.

Benjamin Ang (Deputy Head) and Eugene EG Tan (Associate Research Fellow), Centre of Excellence for National Security, at the S Rajaratnam School of International Studies, Nanyang Technological University, Singapore

Bart Hogeveen (Head of Cyber Capacity Building), International Cyber Policy Centre, Australian Strategy Policy Institute
The Centre of Excellence for National Security (CENS) is a research unit of the S. Rajaratnam School of International Studies (RSIS) at Nanyang Technological University, Singapore. Established on 1 April 2006, CENS is devoted to rigorous policy-relevant analysis of a range of national security issues. The CENS team is multinational in composition, comprising both Singaporean and foreign analysts who are specialists in various aspects of national and homeland security affairs.