SINGAPORE'S WRITTEN COMMENT ON THE CHAIR'S PRE-DRAFT OF THE OEWG REPORT

1. Singapore supports the UN's role in developing rules, norms, and principles of responsible State behaviour in cyberspace. Singapore regards the OEWG as an important mechanism and process for inter-governmental and multi-stakeholder consultations on the issue of cyber security.

2. The Chair's pre-draft OEWG report is a useful summary of the key points and concerns raised by Member States during the OEWG discussions. In addition, we would like to highlight the following points:

Existing and Potential Threats

3. Singapore underscores the importance of maintaining a technology-neutral approach when implementing measures to promote responsible State behaviour in cyberspace. It is the malicious use of technology, and not the technology itself that is a threat. Nevertheless, we agree that while technological advances and their new applications provide substantial benefits, they may also expand the attack surface and amplify vulnerabilities in the ICT environment.

4. In addition to recognising potential threats in the Internet of Things, Singapore further proposes that the draft report note the threats to Operational Technology (OT) devices. We note in particular, threats to Industrial Control Systems which make up the majority of OT systems, as these would undermine and threaten the economic growth, security, and stability of the global community.

5. Singapore supports the points on critical infrastructure being defined differently in accordance with national prerogatives and priorities, as well as the risks faced by transborder, transnational, and supranational critical information infrastructure. More cooperation is necessary to protect and deal with threats to supranational critical information infrastructure (CII), which are owned by private companies, operate across national borders, and are not under any particular State's jurisdiction.

International Law

6. Singapore affirms the principle that international law, in particular the UN Charter, applies to cyberspace. A rules-based international order in cyberspace will provide greater predictability and stability in the way actors behave in cyberspace. Singapore strongly supports the need for greater capacity-building,

to help Member States understand how international law applies to cyberspace, and which can in turn help to advance such discussions at the UN.

Rules, Norm, and Principles for Responsible State Behaviour

7. Singapore agrees that Member States need to promote awareness of the existing norms and support their operationalisation. Regional organisations play an important role in norms implementation.

8. Singapore also supports the further elaboration of norms where needed, for example, in respect of supranational CIIs which could be considered a special category of critical infrastructure, whose protection is the shared responsibility of all Member States.

9. We also support the recommendations for the establishment of a global repository of national practices regarding international rules, norms, and principles of responsible behaviour of States, under the auspices of the UN, as well as voluntary submissions to the repository. We believe that the sharing of best practices in norms implementation between Member States would enhance mutual trust, understanding, and confidence.

Confidence-building Measures (CBMs)

10. Singapore supports the significant role of regional and sub-regional bodies in developing and adapting CBMs to their specific context, as well as the crucial awareness-raising and information-sharing role that cross-regional or inter-organisational exchanges have served. Some of the CBMs that have been developed at the regional level could serve as useful models for adaptation to wider contexts.

11. We recognise the roles and responsibilities that other actors, including the private sector, academia, and civil society can have in contributing to building trust and confidence in the use of ICTs.

12. We support the establishment of a global registry of national Points of Contact (POCs) at the diplomatic/policy, technical, legal, and law enforcement/military levels. Singapore believes that this will facilitate inter-governmental coordination and promote ease of communication between Member States in times of crisis. We further support the need to conduct regular exercises among the network of POCs to maintain readiness and ensure the directories remain updated.

13. Singapore also supports the establishment of a global repository of CBMs adopted at regional and sub-regional levels, to enable the exchange of information. The ASEAN Regional Forum (ARF) Intersessional Meeting on Security of and in the Use of ICTs (ISM on ICTs Security) has done some work in this regard. This is an example of work that could be submitted to such a repository.

Capacity-building

14. Singapore is committed to regional cyber capacity-building. This should be both a shared responsibility and reciprocal endeavour. Capacity-building should be sustainable and politically neutral, with national ownership of capacity-building initiatives. We also agree that there is no one-size-fits-all approach to capacity-building.

15. Singapore thus proposes to draw from the principles of the 2011 Busan Partnership for Effective Development Cooperation, namely ownership of development priorities by developing countries, focus on results, inclusive development partnerships, and transparency and accountability to each other.

16. We support the need for greater coordination in capacity-building efforts. We recognise that existing platforms within the UN and the global community could be used to strengthen coordination. The ASEAN-Singapore Cybersecurity Centre of Excellence can be used to support this coordination role.

Regular institutional dialogue

17. Singapore reiterates our commitment to the UN processes to discuss developments in the field of ICTs and advancing responsible State behaviour in cyberspace in the context of international security. We hope that any future processes discussing cybersecurity issues will continue to be open, inclusive, and consensus-driven.

18. Singapore's view is that the informal intersessional consultative meeting, chaired by Chief Executive of the Cyber Security Agency of Singapore Mr David Koh, was useful in facilitating an interactive exchange between Member States, the private sector, civil society, academia, and the technical community on a range of substantive issues. We believe that it would be useful for any future iterations of the OEWG to hold similar informal intersessional consultative meetings.

. . . . .