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

Centre of Excellence for National Security
www.rsis.edu.sg/research/cens

Ambassador Jürg Lauber

Chair

UN Open-Ended Working Group (OEWG) on
Developments in the field of information
and telecommunications (ICTs) in the
context of international security

30 November 2020

Your Excellency,

The Centre of Excellence for National Security (CENS) at the S Rajaratnam School of International Studies, Nanyang Technological University, Singapore, having participated at the December 2019 Informal Multi-Stakeholder Meeting, applauds the efforts of the OEWG to consistently engage and create opportunities for non-governmental organisations (NGOs) from academia, industry, and civil society groups to interact with the representatives of the UN member states on the issue of international security with regard to the developments in the field of ICTs, in line with the mandate of the OEWG.

We also would like to acknowledge Canada’s leadership in coordinating the various discussions at this informal event on rules, norms and principles of responsible state behaviour; international law; capacity building; confidence-building measures; existing and potential threats; and the future regular institutional dialogue. We also acknowledge the other UN member states and civil society organisations are facilitating the discussion sessions in the dialogue series.

We welcome this opportunity to build on the December 2019 meeting and would like to provide feedback on the OEWG pre-draft from a NGO standpoint and establishing the role NGOs can play in critical areas in cybersecurity and in implementing the recommendations in the eventual OEWG report. CENS will also provide written submissions to the questions asked by the chairs of the different discussion sessions in the dialogue series.

CENS recognises that due to the challenges brought on by the COVID-19 global pandemic, the secretariat the OEWG and the United Nations Office for Disarmament affairs have had to undertake new work modalities in both virtual and hybrid formats. While the pandemic has narrowed the potential physical interaction between states and NGOs, the continuation of consultations with NGOs at the OEWG is a heartening move to holistically consider all viewpoints for the betterment of governance in cyberspace.

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.

Comments on the second pre-draft of the OEWG report

Generally, we believe the second pre-draft of the OEWG report captures the essence of the comments made by states in the wake of the initial pre-draft, and leaves space for discussion. In preparation for the informal dialogue series, we would like to respectfully submit these comments as part of the on-going consultation process.

CENS believes that using the ongoing COVID-19 global pandemic to anchor the conversation on the importance of international security in cyberspace is a game-changer for states and organisations that have hitherto not been participative in discussions on the topic. (Art. 4) The addition of the ongoing pandemic allows all states to clearly quantify their benefits and risks arising from the use of ICTs.

Relatedly, we are also heartened to see the issue of the digital divide acknowledged in the OEWG draft report (Art. 12). This is a challenge for regions like Southeast Asia where the cyber maturity of states is asymmetric. There is a need to strengthen the language to call on all states to improve the cybersecurity standards and processes of developing states to for the security of all states.

As much as addressing the issue of the digital divide is important as a security problem, the digital divide is also a development problem (Art. 2). We believe that bridging the digital divide can tackle and fulfil the objectives set in the UN Developmental Goals and as a matter of capacity building. It is therefore regrettable that the report, having recognised the progress made on narrowing the gender digital divide (Art. 13), has chosen to regard these issues as outside its mandate when addressing the divides in communities can potentially solve both international security and development issues.

Future iterations of the OEWG can consider working with other UN agencies to create a less piecemeal approach to international security, and at the same time, regard the developmental aspect of ICTs as part of the capacity building initiatives that the previous GGE reports have suggested.

a. Existing and Potential Threats

CENS would like to thank Australia and Indonesia for co-hosting the discussion on existing and potential threats to international security. We would like to address the two questions that Australia and Indonesia have asked in the concept note.

- What cyber/ICT related activities do you assess to be the biggest threats to international peace and security?
- With respect to the draft “Existing and Emerging Threats” section of the OEWG the pre-draft report, are there any notable omissions, additions, or statements with which you support or disagree?

CENS supports the view that technology is inherently neutral, and that it is the malicious use of these technologies by state and non-state actors that creates threats in the ICT environment (Art. 21). The increased use of ICTs during the global pandemic for economic purposes has expanded the attack surface and amplified the vulnerabilities in all sectors.

The importance of the protection of all Critical Information Infrastructure (CII), be it on a national or supranational level, should have become more apparent as the pandemic rages on (Art. 22). We also support that the targeting of these critical infrastructure may potentially cause the loss of life and cause disruption to the provision of vital services.

We further agree with the draft report that every state has different interests and have classified their CII according to these interests (Art. 23). We applaud the draft report for recognising that inter-state cooperation or state cooperation with private entities is needed to ensure that CIIs remain well protected. While most CII are domestic in nature, some CII are supranational and span across many states with different levels of protection. We believe that this varying level of security among the different stakeholders in the CII creates a vulnerability that can easily be exploited by malicious actors.

As many small states, like Singapore, rely on digital transformation to build their economies and seek to build smart cities, cyber threats to the Internet of Things and Operational Technology (OT) devices (in particular, threats to Industrial Control Systems) will undermine and threaten the economic growth, security, and stability of the global community.

b. International Law

CENS would like to thank Japan and Oxford University for co-hosting the discussion on international law.

We are pleased that the OEWG has chosen to reaffirm the principle that international law, in particular the UN Charter, applies to cyberspace (Art. 26). A rules-based international order in cyberspace will provide greater predictability and stability in the way actors behave in cyberspace.

We note that the report has not finalised a consensus opinion on the question of how International Law applies in cyberspace, and requires much discussion and understanding from both state and non-state actors. To this end, we strongly support the call 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 (Art. 37).

c. Rules, Norms and Principles for Responsible State Behaviour

CENS would like to thank Canada, Global Partners Digital (GPD), Microsoft, and Association for Progressive Communications (APC) for co-hosting the discussion on rules, norms, and principles for responsible state behaviour.

CENS notes that in the pre-draft report, states have in their discussions reaffirmed their support for the 11 voluntary, non-binding norms of responsible State behaviour of the 2015 UNGGE report, recalling that consensus resolution 70/237 calls upon States to be guided in their use of ICTs by the 2015 GGE report, which includes those norms (Art. 39). ASEAN, the regional organisation, prides itself as the first regional organisation that agreed in principle to be guided by the 2015 UNGGE norms as part of a rules-based international order.

We agree that in particular the need to promote awareness of the existing norms and support their operationalization (Art. 41). While having a set of norms articulate what actions States should or should not take in general, it is still unclear how states can put these norms into action. States need to be guided on the best way to implement the norms or correct misinterpretation of these norms.

We also recognise that regional organisations have a role to play in norms implementation (Art. 44). ASEAN has committed at the October 2020 ASEAN Ministerial Conference on Cybersecurity (AMCC) to have also agreed to develop a long-term regional cybersecurity action plan to implement the norms of responsible state behaviour in cyberspace, taking into account the national priorities and cyber capacities of individual ASEAN member states. This would allow a level of coordination and standards among member states to ensure cybersecurity in the region.

d. Confidence Building Measures

CENS would like to thank Hungary, Chile, and Dechores Digitales in co-hosting the discussion on confidence building measures. We would like to provide input for two of the three discussion questions posed by the co-hosts, namely:

- How do regional organizations approach the development in implementation of CBMs at the regional level? What are the fundamental similarities and differences?
    - With respect to the draft "CBM" section of the OEWG pre-draft report (points 45-52), are there any notable omissions, or statements with which you disagree?

We believe that the regional and sub-regional bodies can play a significant role of in developing and adapting Confidence Building Measures to their specific contexts, as well as serving as crucial awareness-raising and information-sharing roles in cross-regional or inter-organisational exchanges. Some of the CBMs that have been developed at the various regional levels could serve as useful roadmaps for other regions to emulate.

The continuation of dialogue among and between states and non-state actors at all levels – domestic, sub-regional, regional, inter-regional, and global – also serves to build confidence and trust among the various stakeholders in cyberspace. We are pleased that states find that the dialogues at the OEWG is a CBM (Art. 47), and hope that the spirit and usefulness of dialogue also extends to the sessions with NGOs.

We welcome the acknowledgement by states over the contributions of NGOs in building the trust and confidence among all stakeholders (Art. 52). We hope that the noted expanded network for exchange, collaboration, and cooperation that these multi-stakeholder initiatives create can be taken as part of future OEWG consultations between states and NGOs. This would create more interaction among the various stakeholders to understand and discuss the different views and limitations of states and non-state actors.

e. Capacity Building

CENS would like to thank the South Africa, EU Institute for Security Studies and Research ICT Africa for co-hosting the discussion on capacity building.

As previously mentioned, CENS believes that the development aspect of ICTs is closely tied to that of international security, and the concepts cannot be easily dissociated from each other. The chapeau paragraph of the section rightly mentions that that capacity building helps to develop the skills, define the policies and build the institutions that increase the resilience and security of States so they can fully enjoy the benefits of digital technologies and sustainable development. While the statement on cross-border benefits is true, the potential risk of vulnerabilities as part of an integrated ecosystem is equally alarming and should be reflected in the report.

We agree that capacity building should be undertaken to ensure an open, secure, stable, accessible, and peaceful ICT environment by utilising the principles of partnerships, people, and processes (Art. 57). We further agree that capacity building is a shared responsibility and reciprocal endeavour that all states and stakeholders should partake in (Art. 58).

Having been part of capacity building efforts in Southeast Asia, CENS believes that a multi-stakeholder approach to capacity building is important (Art. 59). On any given issue arising from the use of ICTs, the perspectives and problem solving approach from professionals from different sectors are different and sometimes want entirely contradictory outcomes. Capacity building efforts can help in creating a unified, cross-sectoral, and holistic problem solving mechanism by creating the institutions or processes. These can be combined with confidence building mechanisms with other states to create an iterated regional mechanism for multi-national, inter-agency cooperation.

f. Regular Institutional Dialogue

CENS will like to thank France, Egypt, Kaspersky, and the Women's International League for Peace and Freedom for co-hosting the discussion on regular institutional dialogue.

For most states and NGOs, the OEWG was the first opportunity to be involved in matters regarding international security in cyberspace under the auspices of the United Nations (Art. 63). As previously mentioned, CENS actively participated in the OEWG Informal Intersessional Consultative Meeting held in December 2019, and stands ready to support states in its objective to ensure an open, secure, stable, accessible, and peaceful ICT environment. We believe 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 and should be included in the report from the OEWG.

While we understand that states have primary responsibility for national security, public safety, and the rule of law (Art. 71), dialogue with NGOs such as academia, civil society, private sector organisations, and the technical community should continue because the state does not own, control, or operate all ICTs in their territory or lay claim to having the best expertise to address threats from the use of ICTs.

As for the issues that future iterations of the OEWG should address, we believe that it is unavoidable that littoral issues such development and ICT governance will show up in discussions on international peace and security (Art. 70). For example, the issues of human rights, cybercrime, and terrorism are contained among the 11 voluntary, non-binding norms of responsible State behaviour of the 2015 UNGGE report, a recommendation reaffirmed by this very report.

We agree that existing efforts and activities at the other UN General Assembly committees should not be duplicated by the OEWG, but collaboration efforts with other committees should be considered as input into improving the international security outlook with regard to ICTs, especially in the issue areas of cybercrime, human rights, and cyber terrorism – areas that were previously identified by this committee.

g. Recommendations

CENS would like to thank the chair for his comprehensive list of recommendations arising from the discussions at the OEWG. We would like to make comments on the following:

i. International Law

We support the call for states to submit national views and practice on how international law applies to state use of ICTs to the Cyber Policy Portal of the United Nations Institute for Disarmament Research. The portal may be used by states as a repository of national views and practice on how international law applies.

We also encourage the International Law Commission to be called upon by the General Assembly to provide guidance on how international law applies in in the use of ICTs by states in the context of international security. The ILC, as body under the auspices of the UN, is well placed to provide such guidance to UN member states, of which some may have limited understanding or capacity to interpret international law with regard to cyberspace.

ii. Rules, norms and principles of responsible state behaviour by states

CENS welcomes the move from the chair to focus on the implementation of the 11 voluntary, non-binding norms of responsible State behaviour of the 2015 UNGGE report rather than creating new norms. We find that most states in Southeast Asia have only just begun their implementation roadmap, and the results on how these norms are implemented may take some time.

iii. Confidence building measures (CBMs)

CENS supports the call for the secretary general to establish a global registry of national Points of Contacts at a policy or diplomatic level. This is something the ASEAN regional forum has been calling for a Points of Contact directory since 2014, and has had minimal success.

iv. Capacity building

We believe that while it is right to encourage member states cooperate to identify and protect national and transnational critical infrastructure, they should be further encouraged to work on a cross-border, inter-agency, multi-disciplinary basis with both state and non-state actors.

v. Regular institutional dialogue

While some states may have reservations on the current format of a group of governmental experts running alongside the OEWG owing to the fears of duplication and repetition of the process, the current iteration of the two processes seem to be dealing with their mandates well. We believe that having a well-coordinated effort between two efficient chairpersons can lead to deeper and more meaningful discussions on issues arising from ICTs.

We would however like to caution against the encouragement of states establishing sponsorship programmes or support mechanisms for broader participation at the UN because beneficiaries from such sponsorship may be beholden to the interests of the sponsoring state and the discussion may be unfairly biased in favour of the states that are able to sponsor such individuals.

Thank you for considering our submission and we hope that these comments will be helpful to you and the organisers of the dialogue series. We stand ready to assist and support you in any way we can.

Yours Sincerely,

Benjamin Ang
Deputy Head and Senior Fellow, CENS
S Rajaratnam School of International Studies
Nanyang Technological University, Singapore

Eugene EG Tan
Associate Research Fellow, CENS
S Rajaratnam School of International Studies
Nanyang Technological University, Singapore