Johanna Weaver

Special Adviser to Ambassador for Cyber Affairs
Head of Delegation to Open Ended Working Group on Cyber
Representative to UN Group of Experts on Cyber
Department of Foreign Affairs and Trade,
Australia

30 November 2020

Dear Johanna,

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.

CENS further hopes that the threats emanating from Operational Technology be also captured in the discussion. 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 OT devices (in particular, threats to Industrial Control Systems) will undermine and threaten the economic growth, security, and stability of the global community.

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