Statement by the Centre for International Law (CIL), National University of Singapore, to the UN Open-Ended Working Group on Information and Communication Technologies 2021-2025 Seventh Substantive Session

Dedicated Stakeholder Segment, Wed 6 March 2024, 3 pm EST

On behalf of the Centre for International Law, National University of Singapore (CIL), we thank the Chair for this opportunity to engage in the discussions of the OEWG.

The application of international law to the use of ICTs by states and understanding how existing international law applies to cyberspace is critical in moving towards a shared understanding and ultimately, to maintaining peace, security and stability in the ICT environment. Converging on a common understanding of how international law applies will also illuminate any gaps in the existing legal frameworks and how they may be addressed. The increasing number of statements of national positions and interventions on international law in the OEWG sessions thus far have reflected areas of consensus eg applicability of the UN Charter, and reaffirmation of the application of certain international law principles and rules in cyberspace such as the prohibition of the use of force; principle of non-intervention; state sovereignty and sovereignty equality; and the peaceful settlement of disputes. These statements as well as statements on how international law applies to the use of ICTs in cyberspace have been valuable in scoping the legal landscape both for what they say as well as what they do not say and signposting where more dialogue is needed.

Turning to the question of emerging technologies like AI, it is unsurprising that AI has featured so predominantly in the discussions this week given its transformative and disruptive nature with both positive and negative effects. What does international law say about the deployment of AI in ICTs in cyberspace? International law is technology neutral, and as such, already applies to scenarios involving the use of AI technologies by states. States are already bound by existing treaties, customary international law as well as general principles of law. For instance, the principle of non-intervention requires States not to interfere in the internal or external affairs of other States. This broad principle is applicable regardless of the means and methods used including via the use of AI to launch malicious cyber operations.

While international rules and principles are sufficiently general and flexible to respond to new technological developments, are there nonetheless unique features which require distinctions in how international law applies? How does the nature of AI technologies particularly autonomous and generative AI affect evidence collection, evidence analysis and attribution? How does the nature of AI technologies affect the expected conduct of States to prevent or mitigate AI enabled malicious cyber operations? This analysis requires a thorough appreciation of the unique features of AI technology and necessarily requires multidisciplinary and multi-stakeholder engagement in

order to better appreciate the application of existing rules of international law, and gaps if any. A scenario-based discussion would be particularly beneficial in this regard.

In the discussions this week on existing and potential threats, several delegations have cited misinformation and disinformation cyber operations, whether AI enabled/generated or otherwise, and the undermining of national electoral processes. Stakeholders can play an important role in catalysing, facilitating and engaging in discussions of such emergent concerns. In this regard, the CIL is supporting the American University Washington College of Law, in partnership with other institutions, in convening the 3rd Annual Symposium on Cyber and International Law in Washington DC in Sept 24 with the theme of "Cyber and Information Conflict: The International Law Implications of Convergence". Recent history has demonstrated that the advent of cyberspace has enabled and evolved the realm of information conflict, with an attendant convergence of cyber and information operations. The symposium seeks to explore the implications of this trend, which raises critical questions across the spectrum of war and peace including, among others, the law of state responsibility and international human rights.

Chair, in our previous statement at the OEWG in Dec 2023, we shared certain observations from our experience convening capacity building workshops and dialogues on the application of international law to cyberspace, such as:-

(a) the convening of closed door discussions and a safe place that can engender frank, non – adversarial exchange of views and perspectives;
(b) engaging with policy makers, experts and stakeholders across different sectors and disciplines in a cohesive integrated manner to identify and priorities and interlinkages;
(c) engaging officials and experts from across diverse geographical regions and legal traditions;
(d) the value of drawing on case studies that engender more focused and practical discussions.

In the lead up to the Global Roundtable on ICT Capacity Building and the dedicated intersessional meetings in June, we wish to reiterate these observations, in particular the value of contextualizing, applying and analyzing how international law applies to the use of ICTs against specific fact scenarios and via table-top exercises. We look forward to engaging with States and other stakeholders and contributing to these sessions.

Thank you Chair.

Danielle Yeow P L
Lead, Cyber Law and Policy
Adjunct Senior Research Fellow