

**Intervention by Mr. Md. Rafiqul Alam Molla, Counsellor at the intersessional session of the Open-Ended Working Group on security of and in the use of information and communications technologies 2021-2025 (OEWG)**

**International Law**

24 May 2023 at CR-2

Thank you, Mr. Chair.

Bangladesh believes that international law, and in particular the Charter of the United Nations in its entirety, is applicable to maintain peace, stability and promoting an open, secure, stable, accessible and peaceful ICT environment.

Previous OEWG and the GGEs recognized that “a number of States are developing ICT capabilities for military purposes” and that “the use of ICTs in future conflicts between States is becoming more likely”. This truth is further amplified by the rapid development of AI including generative AI and emerging technologies.

We believe that OEWG process can expedite clarity and enhance common understanding of how international law and International Humanitarian Law apply to state conduct in cyberspace. It also has the potential to contribute to the development of customary international law that is applicable to the unique challenges of the cyber domain.

In this regard, we are of the view that the group should leverage the expertise of all relevant bodies and stakeholders, including International Law

Commission as South Africa proposed and supported by many other states, on how and when international law, including IHL, applies to cyber operations.

**Mr. Chair,**

We reiterate that principles of international law, including principles of the UN Charter, encompass respect for sovereign equality, the settlement of international disputes by peaceful means, non-aggression, the prohibition of the threat or use of force in any manner inconsistent with the purposes of the UN, respect for human rights and fundamental freedoms as well as non-intervention and non-interference in the internal affairs of States apply in the cyber domain.

We emphasize the existence of legal gaps in the applicability of international law to the cyber domain, such as the lack of a clear understanding of the attribution of cyber-attacks, State Responsibility Threshold, and the use of force in cyberspace, among others. Consequently, we recognize the merit of developing a dedicated international legal framework tailored to the distinct characteristics of the ICT environment. It is imperative that any such framework addressing ICT-related issues be universal, inclusive, and non-discriminatory in nature.

We look forward to further discussion on this important topic.

I thank you.