Open-ended Working Group on security of and in the use of information and communications technologies 2021–2025

First substantive session (13-17 December)

“How international law applies to the use of information and communications technologies by States”

CHECK AGAINST DELIVERY

Statement by

Ms. Keren Shahar
Senior Deputy Legal Adviser
Ministry of Foreign Affairs
Israel

United Nations, New York
15 December 2021
Thank you, Chair.

It is important for Israel and other states to continue the discussion on the application of international law to cyberspace.

Building a common understanding of how international law applies to the use of ICTs by states forms part of the broader agenda, shared by the international community, of developing a common understanding of responsible behavior of states in the cyber sphere. It complements other important efforts, chiefly among them the practical cooperation in preventing and mitigating attacks. Understanding states positions of existing international law in this context should be dealt before elaborating new rules and norms.

Israel’s position that international law is applicable to cyberspace has been consistently expressed over the years. Having said that, traditional rules of international law, which mainly evolved in a physical world, and often in domain-specific contexts, do not always lend themselves to application in the cyber domain, which has certain distinctive characteristics. Hence the need for further study.

For example, data travels globally across networks and infrastructure located in multiple jurisdictions, transcending
national borders and lacking meaningful physical manifestations. Moreover, cyber infrastructure is, to a large extent, privately-owned and decentralized, both at the domestic and international levels. The cyber domain is also highly dynamic, with technological developments and innovation advancing at a rapid pace. When considering the applicability of specific rules of international law to cyberspace, it is important to be mindful of such distinctive features, and to carry out a meticulous examination of the rules at play and the context in which these rules emerged.

Concepts, rules and principles of international law that apply in principle to ICTs, such as sovereignty, non-intervention, due diligence, state responsibility, attribution and countermeasures merit further study. Given the specialized and context-specific nature of the issues, the OEWG can take a broader role of promoting and facilitating discussions of a more general nature. In this context, we believe the most promising avenue for discussions on the application of international law within the framework of the OEWG, would be to explore how international law can enhance and streamline confidence building, capacity building and international cooperation. The OEWG can and SHOULD play a role by acting as a repository of State views on the application of existing legal rules and concepts that are pertinent to cyber activity.
To conclude, Mr. Chair, before engaging in a new path of developing norms, we believe it is more prudent to have a better understanding of state’s position regarding the application of the existing international law.

Thank you, Mr. Chair