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

First substantive session (13-17 December)

General exchange of views

CHECK AGAINST DELIVERY

Statement by

Mr. Amir Sagie
Cyber Affairs Coordinator
Ministry of Foreign Affairs
Israel

United Nations, New York
14 December 2021
Thank you, Mr. Chairperson.

As this is the first time Israel takes the floor we would like to start by congratulating you on your election and to express the Israeli delegation’s gratitude and appreciation for the hard work and great efforts you Chair and the Secretariat have invested in organizing and steering this process and to wish you much success in your daunting task. Israel attaches importance to the work of the OEWG and stands ready to contribute its perspective and share its knowhow and expertise. Rest assured that you will have Israel’s full support for achieving serious and productive discussions.

Israel attaches great importance to global security and stability in cyberspace, and supports the international efforts aimed to enhance global cyber resilience. Israel believes that an open, free and vibrant cyberspace is of vital importance for global prosperity in the 21st century. To protect these values of openness and innovation strong cybersecurity and extensive international cooperation are imperatives.

Israel would like to welcome and acknowledge the significant and valuable work achieved through the UN GGE processes in the past and the successful outcome of the previous OEWG. This acquis should continue and serve as the basis for any future deliberations.

With respect to the applicability of the International Law to cyberspace and the implementation of existing voluntary non-binding norms on responsible state behavior in cyberspace. We are aware that the order in
which the issues are referenced in the document does not reflect a hierarchy among them. In our view, confidence building and capacity building represent more fruitful terrain for discussion that can improve global security in a practical way.

Against this backdrop, existing international law provides the relevant legal framework, and as states increasingly share their views on how it applies to cyberspace in different fora, it will be important to adopt a careful, incremental approach. Similarly, with respect to norms, it is important to first gain a better understanding of not just what they mean, but how they have transpired in practice. This can inform discussions in the longer term as to the potential necessity of new norms.

Israel also strongly believes that in order to advance jointly the goal of stability and security the OEWG work and outcomes should continue to be consensus based.

Mr. Chair,

Israel as a small nation is proud to serve as an international high-tech hub and a leader in cybersecurity. The Israeli ecosystem attracted more than 7 billion $ in private investments in 2021, is home to more than 100 MNCs and over 400 startups conducive for its cybersecurity innovation activity, and sprung 8 new cyber unicorns in 2021 alone. Part of Israel’s success in this sphere is its advanced technological ecosystem, complemented by a robust domestic legal system based on the rule of law and human rights, and an economic environment supportive of innovation and investment.
The cyber domain poses global challenges that should be faced with global inter-state efforts. Both robust international engagement and cooperation are essential as well. Israel seeks to harness its strengths in cybersecurity to promote global cyber resilience and offer cooperation based on shared values and trust. In this context, Israel stresses the importance of core elements such as practical cooperation, confidence building and capacity building.

Nonetheless, we witness how cyber risks and threats are on the rise. as a result of the Covid-19 pandemic more interactions and operations moved online, further blurring boundaries between public and private and expanding the activity surfaces. Cyber offensive operations are becoming more sophisticated and malicious actors are becoming more brazen. Ransomware attacks turn into a global pandemic that also target essential services, including hospitals and health systems, while causing enormous economic losses. The technological landscape is becoming more interconnected and embedded in all areas of our lives while the cyber workforce is not growing as fast as the demand. All of these create an ever-growing strategic national and international challenges and threats – preparing for them and mitigating them will require will, vision, action and more cooperation crossing organizations, sectors and borders.

To conclude Mr. Chair,

Israel considers cyber security capacity building and CBM's as a key element and stands ready to support the practical and action-oriented
proposals which are aimed to increase capacity and resilience of states to advance responsible state behavior in cyberspace.

Last, but not least, as to the modalities of our work in the OEWG, Israel supports an open and inclusive dialogue which includes relevant stakeholders’ participation in the discussions. Israel is looking forward to work with all of you towards a successful, meaningful and implementable outcome.

Thank you Chair.