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

First substantive session (13-17 December)

Confidence Building Measures and Capacity Building

CHECK AGAINST DELIVERY

Statement by

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

United Nations, New York
16 December 2021
Thank you, Mr. Chair.

Israel regards the discussion on Confidence Building Measures and capacity building as an essential and extremely important part of the OEWG work.

Developing effective and sustainable international understanding requires, in Israel’s view, a solid base of trust. In this context, exchanges of knowhow, cybersecurity methodologies, risk assessment models, threats, trends, patterns etc. can play an important role.

In addition to extensive bilateral information sharing, Israel supports CBM efforts on a regional and cross-regional levels. Israel supports the important work that has been carried out by the OSCE and as a Mediterranean Partner Israel also contributes its vast experience in this field. Furthermore, Israel is one of the founding members of the Global Forum on Cyber Expertise (GFCE) and is an active partner in developing various CBM’s and Capacity building initiatives in the GFCE framework.

At the heart of Israel’s international cyber strategy are its efforts to build global cyber resilience. Israel has recently published its international cyber cooperation strategy and continues to
contribute to raise the cyber hygiene of foreign markets by donating funds through the IADB and the World Bank, assisting countries to build their strategies and establish cyber security mechanisms.

Mr. Chair,

As many member states have alluded, Cybersecurity is an urgent issue. Currently, the growth of risks far outpaces defensive capacity building. The global community needs to do more and to do it faster. Developing countries struggling to bridge the ‘digital divide’ seek to leapfrog their digital economies, and do so securely. Capacity Building in this context refers to the family of efforts conducted to empower partner countries so they can achieve this objective. Specifically, capacity building can also serve as an important measure in building trust, as well as promoting a stable and resilient global cyberspace and facilitating continued human prosperity and progress in the information age. Israel’s capacity building efforts are aimed at improving global resilience on a politically neutral basis, thus adopting a constructive and cooperative approach, while encouraging innovation.
At the government’s initiative, now all public universities in Israel have their own research centers for Cyber Security, managing to more that quintuple our amount of cyber related research. Leading Israeli researchers in the academia have developed a sectorial survey, called PROGRESS, which allows sector regulators and decision makers to get a holistic view over their sector's cyber posture.

Israel is actively sharing best practices with many countries and organizations who wish to build their own national cyber security capacities, and Israel is ready to collaborate with other states and organizations on this important matter.

Mr. Chair,

Cyber Security is a cutting-edge field, and the gaps in skilled cyber professionals on a global scale is huge. The need to have skilled hands-on and updated training is crucial in order to establish and sustain an effective cyber defending force. Israel is a hub for online hands-on updated simulation scenarios that may serve many other nations to build their national cyber capacities.
Israel proved that Cyber could also serve as a social and economic mobility means. Israel has been investing in capacity building programs in its periphery, and is aiming training programs at special populations to make the pie bigger, encouraging girls and women, as well as other groups in the population, to pursue cyber education.

Cyber does not entail only threats. It holds possibilities and opportunities. Israel continues to build its cyber ecosystem while re-enforcing our periphery, bringing together Government, Academia and the Private Sector. We are gladly sharing our experience in this field.

To conclude Mr. Chair,

Cyber has created novel policy and regulatory challenges due to, among others, the involvement of the private sector, so it merits a broad discussion that requires thinking out of the box, breaking existing silos and strengthening multinational cooperation. Though we tend to speak about technology, it is really people-driven, and it should be treated as such, starting from education at young age, and working rapidly to minimize existing gaps.

Thank you Chair.