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

Inter-Sessional Discussions

CHECK AGAINST DELIVERY

Statement by
Mr. Amir Sagie
Cyber Affairs Coordinator, MFA, Jerusalem

United Nations, New York

5-9 December, 2022

**OEWG inter-sessional discussions Dec. 6th 2022**
**Thematic Session: CBMs – Israel's intervention**

Thank you Chair for giving us the floor.
Israel wishes again to thank you personally, the government of Singapore, the UNODA and the chair's supporting team for convening all of us here in NY and supporting these informal OEWG inter-sessional deliberations.

Israel regards the discussion on Confidence Building Measures as an essential and important part of the OEWG work. Developing effective and sustainable international cooperation requires, in Israel's view, a solid base of trust. In this context, exchanges of knowhow, best practices, cybersecurity methodologies, risk assessment models, threat analysis, trends, patterns etc. can play an important role.

Mr. Chair, in order to offer concrete suggestions that can be elaborated within the OEWG process, and a with a view to advance CBMs that can be operationalized in a voluntary, non-binding manner at the UN level, Israel, together with an open group of cross regional member states, held joint discussions aiming to present some novel and practical ideas and we wish to commend our German colleagues for initiating this process.

During recent sessions of the OEWG 2021-2025 considerable progress has been achieved on the way to operationalizing CBMs at the global level. In order to use this positive momentum for future discussions an

open, informal and cross-regional group of states was formed with the objective to advance practical and achievable CBMs within the OEWG framework (the group consisting as of today of: Australia, Brazil, Canada, Chile, Fiji, Germany, Israel, Mexico, the Netherlands, the Republic of Korea, Singapore and Uruguay). Following my intervention, you will hear some more ideas and suggestions from other group members in their national capacity. The group's work dedicated to discuss and advance ideas how we can learn from the national experiences and the multifold regional expertise how CBMs can best be used at the global level to build the needed trust, reduce the chances of misunderstanding and assist in making cyberspace more secured and stable.

We call again and invite all member state that wish to contribute to this important work of advancing practical and achievable CBMs to join our open informal group.

And on a national capacity, 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 member 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 – MSH and Cross regional fora like the GFCE, can contribute and assist states and all stake holders to better share and build the needed trust.

At the heart of Israel's international cyber strategy are its efforts to help building and advancing global cyber resilience and we are ready to work together with all partners.

Thank you chair.

**OEWG inter-sessional discussions Dec. 7th 2022**
**Thematic Session – International Law – Israel's intervention**

Thank you Chair for giving us the floor. We wish to present our national perspective on the issue of International Law.

Israel supports discussions regarding the application of international law to cyber. We feel that building a common understanding of how international law applies to the use of ICTs by states should be the first step before moving to elaborate new rules and norms. Additionally we wish to echo other speakers today and stress that Israel also does not see any need for the adoption of a legally binding instrument in this context.

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

For example, data changes and 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.

Mr. Chair,

The OEWG has played a key role in enabling states to present and publish their views on the application of international law. As the landscape continues to evolve, states will no doubt seek to continue to make their views known, relate to the international law aspects of new threats that are emerging, refine previous positions, and perhaps revise and update previous statements. In Israel's view, the OEWG can and SHOULD play a role in facilitating discussions on international law, by continuing to provide a platform for states to present and publish their views on a voluntary basis.

Thank you.

**OEWG inter-sessional discussions Dec. 8th 2022**
**Thematic Session: Capacity Building– Israel's intervention**

Thank you Chair for giving us the floor to share our national perspectives on the important topic of **capacity building**.

As many member states have alluded, Cybersecurity is an urgent issue. Currently, the growth of risk 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 in Israel's perception 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.

Israel published its international cyber cooperation strategy and continues to contribute to raise the cyber security of foreign markets by donating funds through the Inter-America Development Bank (IADB) and the World Bank, assisting countries to build their strategies and establish cyber security mechanisms.

At the government's initiative, all public Universities in Israel now have their own R&D centers for Cyber Security and offer extensive courses and training facilities, managing to more than 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. Israeli experts have worked successfully together with few countries to use this novel methodology and assist them in assessing and improving the cybersecurity maturity of some of their critical sectors. We stand ready to cooperate with interested parties and share this knowhow and experience.

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.

Cyber Security is a cutting-edge field, and the gaps in skilled cyber professionals are huge on a global scale. 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's experience has shown that Cyber can also serve as a means to improve social and economic mobility. We have therefore continued to invest in capacity building programs to reach out to citizens living in the socio-economic periphery, with inclusive training and educational

programs aimed at under-represented sectors, especially young girls and women.

Cyber does not entail only threats. It holds possibilities and opportunities. Israel continues to build its cyber ecosystem while re-enforcing its periphery, bringing together Government, Academia and the Private Sector. We are gladly sharing our experience in this field. Cyber has created novel policy and regulatory challenges due to, among other things, 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 together with broadening the participation of all stake holders. 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.

Israel wishes to thank India for its contribution we will learn this concept paper thoroughly and will be able to comment and give our opinion in a later stage.

Thank you chair.

**OEWG inter-sessional discussions Dec. 9th 2022**
**Thematic Session: Threats & Norms– Israel's intervention**

Thank you Chair for giving us the floor to present our national perspective on the existing and potential threats and on norms & principals.

In recent years, and very likely in future as well, cyber threats seem to reflect the increased sophistication of malicious actors, stronger capacities and continued malicious attempts to attack high value targets.

Recently, we have unfortunately witnessed another rise in cyber risks and threats: as the world continues to struggle with the Covid-19 pandemic consequences more interactions and operations moved online, thus blurring boundaries between public and private and expanding the threats surfaces; major geostrategic developments have increased Cyber offensive operations and they are turning more sophisticated and harmful ; Malicious actors are becoming more brazen ; Ransomware attacks turn into a real global pandemic that targets governments, and essential services including hospitals and the health systems, water infrastructures and energy supply, while instigating enormous human and economic losses; The technological landscape continues to be more interconnected and embedded in all areas of our lives while the cyber workforce isn't growing to supply the growing demand.

Israel experiences continuous malicious efforts to penetrate and damage its digital infrastructure, so far to no avail, due to the hard work,

awareness and combined efforts of the government and the private sector alike. It is the functional continuity of basic services to the public that is at stake. In fact, according to international cyber security institutes, Israel was a victim of numerous cyber activities, one of the highest rates in the world over the period of the last 2 years.

Mr. Chair,

Civil Aviation is a global sector, and we have seen a growing interest of rogue states and malicious cyber actors in this sector. The last pandemic has hurt the aviation sector, among other effects, it also deprived resources from cyber security investments. Israel has launched its national initiative to build Aviation Cyber resilience and is working on that issue with other partners. We have recently led a multinational cyber security simulation together with the UAE and other countries, to raise awareness and improve information sharing. The Maritime sector is another crucial infrastructure Israel is working hard with its partners to protect against cyber threats, building resilience and improving the cybersecurity of seaports, vessels, shipping companies and the whole supply chain connected to this strategic and essential industry. States need to break the interagency and interstate silos to protect our citizens and organizations from such attacks we need to come up with practical solutions. Israel commends and takes an active part in the US led CRI – a multinational initiative to combat ransomware.

Another phenomenon we should take into consideration is the combination between rogue states, criminal actors and terrorist organizations acting as proxies. Too often, criminals and cyber terrorists

providing hacking as a service receive a type of safe haven, which enables them to pursue their malicious activities with impunity.
Israel suggests making our Info-Sharing process faster and more efficient. Information sharing is the heart of Cyber Security and speed is of crucial importance. Israel has been operating very successfully "CYBERNET"- an Israeli propriety info-sharing system built for cyber professionals, that allows a "many to many" sharing of relevant practical information. Israel launched this initiative to allow cross-country sharing of information, which also serves as a place where various applications and investigation tools are available to explore and mitigate attacks, preventing them from propagating to the sector and market both domestically and internationally.

Additionally, one of the most challenging threat vectors in cyber is via the supply chain. One weak link in the chain, such as an under-protected IT vendor or compromised component, could end up becoming gateways for attackers. This is a multifaceted challenge requiring careful coordination with the private sector and the building of international trust. The world has never been so inter-connected and we are only as strong as our weakest link. Israel implements methodology, digital platform and certification scheme for supply chain security compliance officers in private corporations. A cross-border interoperability of this scheme could help build trust and greatly contribute to the cyber hygiene as an international mechanism.

ICT companies should be encouraged to embed more "Secure by design" processes in the manufacturing of their products, including "Security by default" systems, meaning that the end users will get a safer version by

default, thus reducing the attack surface. Governments should cooperate with each other to foster the development of common cybersecurity standards for different industrial sectors.

Mr. Chair,

Moving now to comment on the Norms – per the first question the chair has put forward in the guiding paper we can answer very simply and echo our colleagues from Canada and other MS that have replied – No. There is no need in our opinion to develop or elaborate new norms. Israel believes that a more cautious approach with respect to norms is warranted. As things currently stand, there lacks certainty as to the manner in which existing norms are being implemented and interpreted. The 2015 GGE norms are voluntary and nonbinding, and do not detract from or extend beyond international law. They are meant to signal expectations of the international community regarding appropriate state behavior, and from what we have seen thus far, their implementation has been uneven. Before embarking on any process of updating the existing norms or developing new norms, it would be more appropriate, in Israel's view, to focus on those norms that currently exist, assessing whether and how they are being understood and applied, ensuring that there exists a common language when referring to these norms.

Once this is done, we as a community we can begin to consider where the need is more acutely felt – whether it is an issue with a current norm, lack of clarity, or whether the original norm itself should be reconsidered. Informed by this approach, only then can we assess whether there exists a need for additional norms.

Mr. Chair,

To conclude, Israel stands ready to share its vision and expertise in building a global "Cyber dome" and cooperate with other states on the prevention and mitigation of risks and threats in the cyberspace, aiming at building stronger global resilience.

Thank you,

**OEWG inter-sessional discussions Dec. 9th 2022**
**Thematic Session: Regular Institutional Dialogue – Israel's intervention**

Thank you Chair for giving us the floor we wish to join this conversation and share our positions on the topic of Regular Institutional Dialogue including the PoA.

Israel holds the position that it is important to continue conducting an inclusive and transparent global discussion on matters pertaining to security in ICTs and their use.

The question of what should be the exact mechanism of such a regular institutional dialogue is directly related to its possible mandate, modalities and characteristics.

Israel is of the view that for the sake of inclusiveness and effectiveness of such a dialogue, the framework for such a dialogue on ICT should be of a voluntary and non-legally binding nature.

In this context, Israel also believes that as cyber security and cyber resilience are key elements of states' national security, it is essential that any future framework will be consensus-based.

Like many of our distinguished colleagues have stressed before and today any chosen institutional dialogue should avoid any duplications or fora fragmentations, as well as maximize the use of resources and maintain a practical and focused process. Like many other MS we also

can anticipate that we might encounter some difficulties equally contributing and fully engaging with parallel and multiple processes.

Israel voted in support of the creation of a Programme of Action (PoA) to advance responsible state behavior in the use of information and communications technologies in the context of international security. While having some reservations, Israel recognizes the aim of this initiative of creating an important, inclusive and permanent venue for discussing cyber security issues.

Israel still believes that there are several potential advantages to the idea of creating a PoA as the sole UN mechanism for discussing cybersecurity issues on a global level. At the same time, we still have some reservations. We have persistently made clear that it is imperative that all decisions in the new PoA be made based on the principle of consensus, applied both to the negotiation processes leading to the creation of the PoA, as well as to the decision making process within it. It should be clearly reflected in the PoA's modalities, as cybersecurity issues affect the fundamental national security interests of all States. It is our expectation that this essential and widely observed principle be maintained and safeguarded in the text and put into practice in the next phases of deliberations and the creation of any future PoA.

Secondly, going forward, it will be important in our opinion for the PoA to be objective and neutral. As past experience demonstrates, its credibility will depend in large part on ensuring that it not be politicized.

Thank you Chair.