Fourth Substantive Session of the UN Open-Ended Working Group (OEWG) on Security of and in the Use of Information and Communication Technologies (ICTs) in the Context of International Security

(6 – 10 March 2023)

Statements Delivered by: Mr. Shahrukh Khan, Deputy Director (Arms Control & Disarmament), Ministry of Foreign Affairs, Pakistan

Agenda Item 1: Existing and Potential Threats in the Sphere of International Information Security

Chair,

Thank you for giving me the floor and the opportunity to present Pakistan's views on the most important topic i.e. the existing and potential threats facing in the sphere of international information security.

I would like to express my appreciation for the untiring efforts of the Chair to steer the work of OEWG in a steady and balanced manner especially the adoption of the Annual Progress Report during the last session.

Pakistan also commends your work for holding substantive discussions on the establishment of the PoC Directory during the informal session held in December.

Chair,

The growing trend of malicious cyber activity, as highlighted in the Annual Progress Report, has given rise to significant concerns about the protection of critical infrastructure, supply chain security, and data security. The attacks on vital systems such as energy, health, water, and transportation pose a severe threat to international security.

Furthermore, the militarization of cyberspace, the development of offensive cyber capabilities by nations, the malicious use of ICTs by non-state actors like terrorists and criminal groups, and the unchecked military applications of new and emerging technologies, are all contributing to a dangerous erosion of global peace and security. The possession of capabilities by Non-State Actors to disrupt, deny, degrade, and destroy critical infrastructure is making the cyber threat landscape more precarious.

Chair,

Pakistan acknowledges the significant benefits of new and emerging technologies, but we also recognize the potential risks associated with them. New and emerging technologies provide malicious actors with new vectors and vulnerabilities that can be exploited to launch cyber-attacks. These attacks can result in the theft of sensitive information, disruption of essential services, and even the compromise of critical infrastructure. The exploitation of these technologies for malicious ICT activity is a growing concern that requires urgent attention from the international community and calls for the formulation of a framework to ensure their responsible use.

Chair,

Pakistan is facing serious threats from an increasingly ungoverned cyberspace. These threats include cyber-attacks on critical infrastructure, DDoS attacks, data theft, and targeted disinformation campaigns. To tackle these challenges and secure its digital assets and information systems, Pakistan has put in place its first National Cybersecurity Policy in 2021. This policy aims to secure the entire cyberspace of Pakistan and to establish a stable cybersecurity ecosystem.

The policy sets national security standards and processes for the design, development, and operation of information systems to protect critical infrastructure. Additionally, the policy aims to raise awareness about cybersecurity through mass communication and education programs, as well as to build capacity and skills among cybersecurity professionals.

Overall, Pakistan's National Cybersecurity Policy is a comprehensive approach to ensuring the security of the country's digital assets. The country is also advocating for a legally-binding international instrument to promote responsible behavior in cyberspace. With these efforts, Pakistan is working towards a safer and more secure cyberspace for all its citizens.

Chair,

On the militarization of cyberspace, Pakistan’s position is consistent. The rapid employment of offensive cyber capabilities, in conjunction with modern warfighting technologies, may result in rapid escalation, especially in the early stages of conflict. Because the internet is like a “common heritage of mankind”, Pakistan calls for an outright ban on the development of offensive cyber weapons.

I would like to conclude by affirming that Pakistan stands ready for enhancing inter-State cooperation to effectively counter the threats posed by ungoverned global cyberspace.

I thank you, Chair.

<u>Agenda Item 2: On the Development of rules, norms, and principles of responsible behavior of States</u>

Chair,

Pakistan attaches great importance to the further development of rules, norms, and principles of responsible behavior of States and considers this as one of the priority mandates of the OEWG.

Pakistan welcomed the GGE report of 2015 when Member States expressed their agreement on 11 norms of responsible State behavior. Pakistan believes that there is a need of equipping the Member States with the required skills and technologies and clearly define the modalities for the implementation of the agreed norms.

However, on the further development of rules, norms, and principles of responsible behavior, Pakistan's position is quite clear. Though we do consider the formulation of non-binding voluntary norms important for secure and stable cyberspace, however, non-binding norms can't be an alternative to a legally binding instrument. The main difference between non-binding norms and a legally-binding instruments is that the latter imposes certain obligations and their violation triggers the law of State responsibility. Moreover, norms are effective during peacetimes only and will lose efficacy in an event of war.

Chair,

Pakistan recommends that the States must be encouraged to take the following measures while conducting further discussions on cyber-norms building:

a. Initiate discussions on the adoption of a legally binding instrument to regulate the behavior of States in cyberspace.

b. Ensuring prohibition of ICT activity that knowingly or unintentionally damages critical infrastructure.

c. Enhancing cooperation to reach an agreement on prohibiting the creation of harmful hidden functions or accumulation of vulnerabilities in ICT products, as well as to commit to responsible and timely reporting of ICT vulnerabilities.

d. Facilitating cooperation in the context of supply-chain security of ICT products.

e. Ensuring safe cross-border data exchange and taking measures against data theft.

f. Refrain from allowing the ICT infrastructure to be used for malicious activities that threaten international peace and security, and avoid interfering in the internal affairs of other States through means such as fake news and disinformation.

g. Formulation of an agreed mechanism, under the auspices of the UN, to resolve the conundrum of attribution.

I thank you, Chair.

Agenda Item 3: Application of International Law in Cyberspace

Chair,

The application of international law in cyberspace is one of the most important mandate areas of the OEWG. Pakistan believes that the stability of cyberspace, in reality, rests on the formulation of a legally-binding mechanism to ensure the responsible use of the global internet, a mechanism, which promotes responsible State behavior by holding actors responsible for their acts and forbids the use of cyberspace for destructive purposes.

Taking this opportunity I would like to inform you that Pakistan has submitted its position paper which, in detail, articulates our position regarding the application of international law in cyberspace.

Chair,

Pakistan's position on the application of international law in cyberspace has remained consistent. Pakistan believes that the principles of non-use of force, sovereign equality of all nations, non-interventionism, and peaceful settlement of disputes, as enshrined in the UN Charter, apply to cyberspace. We are supportive of "rules-based" cyberspace, open for all for reaping maximum economic benefits.

Pakistan believes that, compared to the physical world, Cyberspace is unique because of its transnational nature, anonymity, and its use by State and non-State actors. Thus the existing framework of international law and IHL has certain gaps. Therefore, Pakistan welcomes the initiation of focused discussions among Member States on the application of international law in cyberspace.

We believe that such debates shall help in identifying the areas of convergence among the Member States.

In addition to this, Pakistan also proposes the formulation of a common lexicon to get definitional clarities on the different cybersecurity-related terminologies.

Pakistan also stresses the need to fulfill the capacity-building needs of Member States in the area of cyber policymaking and regulatory mechanisms to develop expertise in the subject area. In this regard, we welcome the initiatives taken by the EU and the Republic of Singapore.

Last but not least, the OEWG must discuss and find ways to solve the challenge of cyber attribution, which we believe is difficult, but not insurmountable.

I thank you, Chair.

Agenda Item 4: Confidence Building Measures (CBMs) / PoC Directory

Chair,

Let me take this opportunity to commend the work done by you and your team in the area of Confidence Building Measures. I would also like to acknowledge the positive role played by all Member States in their support of the establishment of the Points of Contact (PoCs) Directory.

Pakistan endorses your revised non-paper on the key elements of the PoC Directory and appreciates the efforts put in by you in drafting it. We firmly believe that the non-paper is in line with the views we have already submitted on the PoC Directory. We agree with the purposes and principles of the Directory which will be used for information sharing, trust building, crisis handling, and facilitating communication among States in an event of ICT related incident. However, we believe that the PoC Directory, shall in no way, be used to determine the technical and political attribution of cyber incidents.

Under the modalities section, we agree that the participation and sharing of information in the Directory should be voluntary and confidential and the adoption of an incremental approach. However, we believe that there is a need to outline the key responsibilities of Diplomatic and Technical PoCs. The duties of the Diplomatic PoC may include representing the country during bilateral and multilateral negotiations relating to cyber incidents and facilitating cyber dialogue among the States, while the Technical PoC may be tasked with technical evaluation of the information exchanged through the Directory and sharing and receiving of data relating to cyber threats.

In the Modalities section, part (c) concerning "*Information Access*", we request further clarification on the type of information that will be accessible on the public page. We would like to emphasize that, as previously stated in our views submitted on the PoC Directory, there needs to be a mechanism for private entities and tech companies which are engaged in cyber threat hunting and identifying hardware/software vulnerabilities to promptly notify PoCs about cyber threats. This would significantly enhance the effectiveness of the PoC Directory in preventing cyber incidents.

On Directory maintenance, we agree on conducting ping tests, however, for the sake of clarity, a brief technical description of “ping tests” may be added in the footnotes. Moreover, in future meetings, there is a need to discuss the means and methods to ensure the protection of information that will be contained in the Directory.

We highly appreciate the detailed road map presented in the non-paper under the capacity-building section, especially the proposals like the development of e-learning modules and tabletop exercises. However, it is necessary to put into action these proposals as soon as possible.

Chair,

Pakistan is open to constructively taking part in discussions on finalizing the different technical aspects of the Directory such as the communications protocols and the measures for the proper handling and labeling of the information that will be exchanged through the platform and stands ready to contribute towards its successful implementation.

Pakistan has always maintained that cyber CBMs, like the PoCs Directory, are extremely important for fostering trust, cooperation, transparency, and predictability among the Member States.

However, we believe that the Directory is one of the CBMs, not the CBM. Therefore, Pakistan proposes discussions on the adoption of the CBMs in the areas such as capacity building, research and investment in cybersecurity-related projects, exchange of best practices, countering fake news and disinformation

I thank you, Chair.

<u>Agenda Item 5: Capacity-Building</u>

Chair,

Pakistan believes that capacity building has a crucial role to play in effectively responding to current and potential cyber threats. Moreover, the need for capacity building becomes more important because of the large gap in terms of capacities and skills between States to deal with the threats emanating from cyberspace. In this regard, we greatly appreciate the cyber fellowships offered by the Republic of Singapore and the EU's Institute for Security Studies. These initiatives provide a good template for future cyber capacity-building programmes. However, a focused approach to the legal capacity building including developing expertise in the areas of cyber governance and cyber policy making is required.

We also welcome the proposal for the development of an action plan to support interested States in building their requisite institutional strength to effectively participate in the POC directory and to deal with cyber threats.

Pakistan is of the view that the capacity building of all States on equal footing is a key measure for secure and stable cyberspace, especially when the cyber threats are increasing globally and developing countries lack the necessary expertise to better guard their cyberspace.

Pakistan believes that the principles of future capacity-building programmes should include the following:

1. Capacity building should be **demand-driven**, made upon request by the recipient State, taking into account the specific needs and contexts of Member States, and have sustainable impacts. In this regard, the OEWG Secretariat may perform a match-making role to fulfill the capacity-building needs of States.

2. By ensuring **fair, unconditional, and equitable access** to cybersecurity-related technologies, products, and services with an aim to bridge the digital divide.

3. Capacity-building efforts should be designed with a long-term vision that ensures **sustainability** beyond the initial funding period.

4. Capacity building should be **holistic** and include training and certifications, technology transfer, policy development, and awareness-raising.

5. Establishing a **dedicated funding mechanism** to support capacity-building projects in developing countries.

I thank you, Chair.

Agenda Item 6: Regular Institutional Dialogue

Chair,

Pakistan maintains a consistent and clear position on the topic of regular institutional dialogue. We propose that the key principles that should be considered in the formulation of future platforms for discussions on ICTs must include inclusivity, consensus-driven decision-making, multi-stakeholder participation, global collaboration, and sustainability. Pakistan believes that the future institutional dialogue must also include in its mandate the topics of capacity building, norms building, and discussions on the application of international law in cyberspace. Furthermore, we hold the view that this dialogue should take place under the auspices of the UN.

It is essential to emphasize here that at this stage there is no need to create any parallel structure to the existing OEWG. We firmly believe that the existing OEWG is the most appropriate forum for all discussions related to the ToRs and mandate areas of any future platform, including the PoA.

Pakistan's decision to abstain from the resolution on PoA is driven by our belief that any mechanism or structure created after the existing OEWG in 2025 must be built on a sustainable foundation and developed through a consensual process. Therefore, the existing OEWG provides an ideal platform for such discussion. Therefore, we advocate for a collaborative and all-inclusive approach for the PoA, which would ensure its effectiveness and long-term sustainability.

Taking this opportunity I would like to renew Pakistan's support for this intergovernmental process for safe, secure, and stable cyberspace for all. We believe that the success of the OEWG process depends upon equal and all-inclusive participation of all Member States.

I thank you, Chair.

****