

STATEMENT BY AMBASSADOR ANUPAM RAY AT CD PLENARY ON AUG 11, 2022 ON 'THE CENTRALITY OF INTERNATIONAL COOPERATION AND CAPACITY BUILDING IN BUILDING SAFE AND SECURE CYBERSPACE'

Statement

Mr. President

Thank you for convening today's Plenary with focus on international cooperation and capacity building for a safe and secure cyberspace. As a developing country that recognizes the immense benefits that ICT can offer to our people, India supports a open, stable, accessible, secure and peaceful cyberspace.

2. Cyberspace has become an indispensable domain for governments, the public and industry to carry out their day-to-day activities. A vast number of socio-economic and Government to Citizen services are being increasingly delivered using tools and technologies in cyberspace. This is transformational for small and developing countries as it facilitates affordable and effective access to public services

3. At the same time, cyberspace is facing a number of challenges and threats and is being misused by criminals and terrorists. The serious ICT threats identified in various UN reports highlight the challenges to States in ensuring cybersecurity. Incidents involving the malicious use of ICTs by States and non-State actors have increased in scope, scale, severity and sophistication. While ICT threats manifest differently across regions, their effects can be global. India is fully aware of the catastrophic consequences of malicious ICT activity by State and non-State actors that threaten international peace and security, as well as well-being and safety of individuals.

Mr. President

4. New and emerging developments in cyber space also expand the attack surface, creating new vectors and vulnerabilities that can be exploited for malicious ICT activity. This constitutes a serious challenge to ensuring security in ICT infrastructure, especially Critical Infrastructure (CI) and Critical Information Infrastructure (CII)

5. The use of ICTs for terrorist purposes, beyond recruitment, financing, training and incitement, including for terrorist attacks against ICTs or ICT-dependent infrastructure threatens international peace and security.

Mr. President

6. The COVID-19 pandemic underscored the importance of protecting health care and medical infrastructure and facilities, including through the implementation of the norms addressing Critical Infrastructure. There are increasing attempts to disrupt essential services to the public. Resilient communication systems need to be established urgently at the international level for increased and timely exchange of information and cooperation between Member States. Ensuring confidence and trust in cyber technologies that protect an individual's privacy and data is a goal that both Member States and industry are striving for.

Mr. President

7. It is encouraging that there is continuation of the inclusive and transparent negotiation process on ICTs in the context of international security under the auspices of the UN OEWG on ICT 2021–2025, established pursuant to UNGA resolution 75/240. It is a positive sign that the OEWG adopted its First Annual Progress Report during the 3rd Substantive Session last month.

8. Capacities to secure information systems continue to differ worldwide, as do the capacities to develop resilience, protect critical information infrastructure and identify threats and respond to them in a timely manner. These differences in capacities and resources, as well as disparities in national law, regulation and practices related to the use of ICTs, and unequal awareness of and access to existing regional and global cooperative measures available to mitigate, investigate or recover from such incidents, increase vulnerabilities and risk for all States.

9. The variability between Member States, in terms of cyber preparedness to tackle various cyber threats and respond accordingly, has been duly recognized by multiple GGEs. They have highlighted the need for concrete and action-oriented approach towards international cooperation under the UN framework.

10. To guide small and developing countries in enhancing their cyber capabilities, we need to anchor a permanent mechanism at the UN that integrates all the existing and proposed mechanisms of international cooperation under capacity building. In the recent 3rd substantive session of the OEWG in July, India proposed the development of a “Global Cybersecurity Cooperation Portal” (GCSCP), anchored at the United Nations, as a global platform for international cooperation and coordination amongst Member States on security of cyber infrastructure and improving cyber capabilities.

Mr. President

11. Currently, there are various mechanisms at different levels for exchange of information and coordination among cyber agencies of member States. However, there is no global platform, which enables such an exchange. Establishment of this Cooperation portal will overcome this gap. This is envisaged as a one-stop platform for enabling global cooperation and coordination between Member States on matters related to cyber security. The portal can incorporate various components, some of which are currently being discussed by the OEWG.

12. India envisions the GCSCP to be a member State driven portal with the UN Secretariat handling its overall maintenance and management. Member States will be provided dedicated access credentials by the UN Secretariat. Member States can upload information under the various sections of the portal on a voluntary basis. UN bodies, regional organizations and other relevant stakeholders can also share information with the UN Secretariat for inclusion in the portal.

13. The portal will provide the base platform on which various ideas to cyber security discussed under the OEWG can be implemented through a modular approach. It will have different modules on areas like capacity building, policy frameworks, cyber threats etc, which can be developed independent of each other. It can also integrate best practices under existing cyber cooperation platforms.

14. Such permanent portal/mechanism would go beyond the ongoing OEWG on ICTs 2021-2025. It would be complementary to any future regular institutional dialogue. Such an integrated and comprehensive portal would bring in trust and confidence as it is anchored at the UN.

15. India hopes that such a proposal would help achieve our common objective of ensuring a secure cyber space and achieve international peace and security.

Thank you, Mr. President
