Thank you Mr Chair

India takes this opportunity to thank you for your able-leadership and sincerely appreciate your initiatives to make the functioning of this working group more open, transparent and inclusive.

India would like to suggest a few edits to the section on Existing and Potential Threats.

Under Paragraph 7,

Point b(iii), “Cooperation and assistance to ensure the integrity of the supply chain...”; We would like to suggest adding “security and” before integrity.

Point (v) - that reads as “Cooperation and assistance for developing ICT security baseline studies and designing security as a critical requirement”,

We would like to suggest replacing “studies” with “standards and best practices” and “replace “designing security” with “secure by design”.

After point (vi), we suggest adding a few more sentences:

(Vi a) “Share strategies, policies and legislations/guidelines and best practices for the protection of cyberspace;

(Vi b) “Strengthen law enforcement cooperation to prevent the use of cyberspace for terrorist purposes;

On Point (ix) “Measures and initiatives to strengthen data security”,

We would suggest deleting this line as this does not pertain to this section of existing and potential threats;

Point (d), we suggest inserting ‘think tanks’ along with businesses, NGOs and academia;

Under ‘Recommended next steps” section, we suggest adding a sentence after the end of point 2 “....Experts could be invited to make presentations on these topics to facilitate further discussion”. Here we suggest adding “Exchange of information and knowledge on these topics to facilitate building a common understanding amongst Member States”

For point 3, we suggest adding ‘think tanks’ similar to suggestion for point (d).

With respect to the suggestion to include the expression ‘non-discriminatory business environment’, my delegation does not support inclusion of such expression into the annual progress report. Member States have the sovereign right to develop and implement policies that are of national importance, keeping in view the developmental goals of a Member State and such policies, as long as they are
consistent with peace and security should not be influenced with expressions that impose unnecessary obligations on the Member States.

Mr. Chair,

Under Rules, Norms and Principles of Responsible Behaviour section, we would to suggest to change the expression ‘ICT terms’ to ‘ICT terminology’ in Paragraph (a) and paragraph 2, under Recommended next steps.

Under CBMs section, 5th line of point (a), we suggest an alternative expression to ‘hotlines’. We suggest replacing with CERT-to-CERT PoCs. In the same para ending sentence that reads as “…a directory which would include experience at the regional level”, we suggest adding ‘national’ before the term ‘regional’. After edits, the sentence would read as “a directory which would include experience at the national and regional level”.

In point (b) under para 10, we suggest replacing ‘white papers’ with ‘concept papers’.

Mr. Chair,

Before suggesting edits to the capacity building section of the draft report, I would like to take this opportunity to share some thoughts on this section as it is that particular section can really help developing countries in developing their ICT capabilities to ensure security in their national ICT environment.

During the course of the last two substantive sessions and the current one, Member States are particularly interested in streamlining the capacity building area with concrete and action-oriented recommendations. We appreciate the Chair and your team for your efforts in reflecting the same spirit in the draft annual progress report. We believe that capacity building area, whatever form and character this Session agrees, would pave the way for future work that goes beyond the upcoming sessions of the OEWG. If we as Member States take a moment to see where the work we are doing would take us down next five years or ten years, we may realise that it is time to consolidate the efforts and focus on certain priorities that are of significance to everyone.

At present, we have certain measures and recommendations suggested by Member States such as ‘directory of POCs’, national survey of implementation, ‘compiling a calendar of capacity building programmes, ‘developing a list of regional and sub-regional centres of excellence’ and others.

What we are seeing is there are multiple portals or websites with different degree of capacity building. Let me please stress here that India fully appreciates each of these existing and proposed mechanisms and understands the merits each one brings to the development of ICT capabilities of Member States. At the same time, from the perspective of small and developing countries and countries that have smaller
delegations, it becomes excessively time consuming and efforts seeking to continue to keep tracking different portals or calendars of capacity building.

What we need now is ‘INTEGRATION’ of these mechanisms under the United Nations Framework. United Nations should play a lead role in capacity building and implementation of normative framework. For this reason, we need to anchor a permanent mechanism at the UN that integrates all the existing and proposed mechanism of cooperation under capacity building. Such permanent portal/mechanism goes beyond OEWG. It would be complementary to any future regular institutional dialogue including Programme of Action.

Such an integrated and comprehensive portal would bring in trust and confidence as it is anchored at the UN. The current draft report recommends the same approach under point (d) of capacity building section and reiterates it with necessity of ‘coordination’ and ‘collaboration’ with the existing initiatives. In this light, we would like to propose establishing ‘Global Cyber Security Cooperation Portal’ at the UN.

Mr. Chair,

While deliberations on the normative framework of State behaviour in cyberspace and the developments in the field of ICT in the context of international security continue in the Open Ended Working Group on security of and in the use of information and communications technologies 2021–2025 (OEWG), established pursuant to General Assembly resolution 75/240, there is an underlying need for the OEWG to focus also on concrete ideas that can help achieve the common objective of free, open, secure, stable, accessible cyberspace and its use for peaceful purposes.

During the First and Second substantive sessions of the OEWG, member states have put forward such ideas, especially in the capacity building and confidence building measures, for further consideration of the Group. The development of a “Global Cybersecurity Cooperation Portal” (GCSCP), anchored at the United Nations, as a global platform for co-operation and coordination by member states on cyber issues is one such idea.

Objectives GCSCP:

Currently, there are various bilateral, sub-regional, regional mechanisms 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 GCSCP will overcome this lacunae.

GCSCP 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.

**Management of GCSCP:**

GCSCP will be a member state driven portal with the UN Secretariat handling its overall maintenance and management. Each member state 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 organisations and other relevant stakeholders can also share information with UN Secretariat (UNODA) for uploading into the portal.

**Content of GCSCP:**

The GCSCP will provide the base platform on which various ideas to cyber security discussed under the OEWG can be implemented through a modular approach. GCSCP 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 national, regional and plurilateral cyber cooperation platforms.

**Access to GCSCP:**

- The portal can incorporate two kinds of content- public and restricted. While public content could be accessible for everyone to view, restricted content could be viewed only by member states. Member states can have the option to choose whether the information they upload or share would be public or restricted information. Information shared by UN bodies, regional organisations and other relevant stakeholders can be public, unless requested otherwise.

**How can the OEWG contribute:**

The OEWG can recommend the establishment of such a portal to the UN General Assembly. Subsequently, the Group, in its future sessions, can have focused deliberations on the content/modules of the portal for further development.

India is open to discuss this further with Member States and we invite all to study it and suggest what changes can be done to make it a better mechanism under the UN.

Under capacity building Section,
point (b), we suggest inserting ‘inter alia’ in the third line after ‘questionnaires’. We suggest similar edit to para 5, second line. “States are encouraged, on a voluntary basis, to survey their capacity needs including through inter alia the national survey of implementation and/or the cybersecurity capacity maturity model.

We would be sharing these changes with the Chair in the written format.

Finally, India would like to assure the Chair, its support and flexibility in making the session productive and outcome-oriented.

Thank you Mr. Chair.