Statement by South Africa on regular institutional dialogue at the Open-Ended Working Group on security of and in the use of information and communications technologies, 8 March 2024, United Nations, New York

Chairperson,

Thank you for your tribute to the role of women in international relations on International Women's Day. Co-incidentally, it is Human Rights Month in South Africa, and as we say, women's rights are human rights.

This Open-Ended Working Group (OEWG) has conducted its work over the last three years against the backdrop of a difficult geopolitical climate. It was no small feat to have achieved two consensus reports in a row under your able leadership.

South Africa has been pleased that we have made steady process in adopting the global POC directory and five new CBMs to support its work. We agree with Member States that have concluded that a future permanent mechanism should be established to succeed this OEWG after its mandate expires.

In this regard, we agree with Brazil and India that your elements paper is a welcome proposal. South Africa supports paras three a to b. The future mechanism should be a single-track, State-led, permanent mechanism with flexibility to include new developments in ICT security and technologies, reporting to the First Committee of the UNGA. The future mechanism should build upon the consensus agreements on the framework of responsible State behaviour in the use of ICTs from previous OEWG and GGE reports. In the context of the interconnected nature of cyberspace, it would be vital to preserve decision making by consensus.

Chairperson,

Allow us to offer a few additional thoughts:

- We believe thematic areas of work could remain the same as in this OEWG, in a future permanent mechanism.

- The development of any future political framework should consider that developing countries are still building their ICT security structures and therefore voluntary commitments should be the basis of such a framework.

- Discussion on voluntary commitments such as norms or CBMs should be developed without prejudice to the possibility of a future legally-binding agreement if Member States see the need for such an instrument.

- Just as we have had a rich discussion on existing and potential threats to ICT security in this OEWG, we should allow the future permanent framework to allow States to develop their common understanding of the ICT threats as technologies develop.

- Capacity building should remain at the core of a any framework for regular institutional dialogue, as you have duly noted during the course of the OEWG. Cooperation on capacity-building should operate on the principle of respect for the needs and context of the recipient State/s.

- The permanent mechanism could be established as a subsidiary body of the First Committee.

- The UN Office for Disarmament Affairs could serve as the Secretariat of the permanent mechanism.

- Formal meetings could be held once or twice a year with inter-sessional meetings, as needed.

- A Global Cyber Security Cooperation Portal (GCSCP), which could include a repository of threats, could also share information relevant to the work of the permanent mechanism.

Chairperson,

Our delegation believes that we should make use of this transparent, and all-inclusive forum of the OEWG to conduct all discussions on a future regular institutional dialogue mechanism. We are not in favour of parallel, ad hoc discussions on proposals we all need to support in order for them to have any chance of effective implementation. Therefore, we look forward to hearing proposals, and views of other delegations on a framework for RID.

Thank you.