Written Summary of South African Interventions at the informal Inter-Sessional Meeting of the Open-Ended Working Group on security of and in the use of information and communications technologies 2021-2025, December 2022

International Law

South Africa remains committed to promoting a peaceful and stable cyberspace underpinned by international law, including human rights law, and the 11 norms of responsible State behaviour.

We have stated that we believe the United Nations Charter applies to cyberspace as well.

South Africa believes that briefings from experts could assist the Working Group in its discussions on how international law may apply from a legal perspective.

We propose that we also consider a discussion on International Humanitarian Law (IHL) in the Working Group.

Confidence-building Measures

South Africa believes that the Points of Contact (PoC) directory should be established for both technical and diplomatic purposes.

South Africa supports the recommendation in the OEWG Annual Progress Report of 2022, to establish and build on the work already done at the regional level by establishing a global, inter-governmental PoC directory at the United Nations (UN).

A PoC directory should be available via a password protected webpage as a layer of security to ensure security of the information contained in the directory to avoid unauthorised access. Password protection will provide data privacy from bots and search engines. Ideally, the use of a password manager is a prerequisite for everyone accessing the directory.

We support the nomination of distinct PoCs at technical, diplomatic and policy levels. It would be useful to have the same PoCs for global and regional directories and where possible, the relevant Computer Emergency Response Team (CERT) could be the designated technical PoC.

A PoC at technical level which equates to working level and at diplomatic and policy levels which equate to senior level. Senior level PoCs should be contacted if the incident has a political element to it.

For information exchange between POCs at technical level, consideration could be given to borrowing from policies, protocols and processes adopted by the Forum of Incident Response and Security Teams (FIRST) or other regional and sub-regional bodies.

The PoCs could be institutionalised and linked to a particular post within the institution, rather than linked to a name. At any given point, the incumbent in the designated position will fulfil the role and a permanent email and contact number assigned to the position could be used. The use of all UN languages is preferred.

The POC directory should be constantly updated to ensure speedy response when assistance is required. Member States should inform the Secretariat of changes when they happen.

We also recommend regular table-top exercises, information and knowledge exchange.

We are open to further views on how a PoC directory would operate and look forward to the exchange of views.

Regular Institutional Dialogue

South Africa is pleased that we have agreed at the recent session of the First Committee to discuss a Programme of Action (PoA) in the OEWG.

We believe that discussions in the OEWG should inform the basis of a potential PoA.

A PoA should have the broadest possible support in order for it to be effective. It should address the concerns of developing countries as they build their ICT infrastructure, and the needs of States that wish to update existing ICT infrastructure.

A PoA should be added as an additional pillar of our work.

With regards to the principles of regular institutional dialogue, we should operate with inclusivity, transparency, sustainability, and in an objective-driven and results-based manner, as agreed in the final report of the first OEWG.

We should avoid duplication of existing UN mandates.

Our current mode of work facilitates inclusivity of all stakeholders in their respective roles and responsibilities. The inter-sessional meetings where Member States engage with other Stakeholders is a very efficient way of taking into consideration, views and voices of other role-players in formal sessions.

To ensure broad participation of all Member States, we must avoid parallel processes on the issue of security in the use of ICTs and keep the discussion in a single, open and inclusive track.