South African Statement on Agenda Item 5 “Existing and potential threats in the sphere of information security, inter alia, data security, and possible cooperative measures to prevent and counter such threats,” at the 4th Substantive Session of the Open-Ended Working Group on security of and in the use of information and communications technologies 2021-2025

6 March 2023

Thank you, Chairperson.

First, we would like to express appreciation to you and your team’s consistent, and action orientated effort throughout this working group process. As always, you can count on our support and active engagement.

We also look forward to fulfilling the aims of the first annual progress report and its recommended next steps, as a roadmap for continuing our work building towards the adoption our next substantive annual progress report.

Chairperson,

At this point, allow me to make a few points related to existing and potential threats in the sphere of ICT security, inter alia, data security, and possible cooperative measures to prevent and counter such threats:

States have agreed via the adoption of the 11 Rules, Norms and Principles of Responsible State Behaviour in Cyberspace that we should cooperate in developing and applying measures to increase stability and security in the use of ICTs and to prevent ICT practices that are acknowledged to be harmful or that may pose threats to international peace and security. In this vein, South Africa believes that States can only operate as well as our current understanding allows us, therefore we agree that the discussions in the Open-Ended Working Group (OEWG) should facilitate sharing of knowledge, information and experiences on existing and potential threats.

South Africa believes that new and emerging technologies have opened a new front for malicious ICT activity using the Internet of things (IoT), Artificial Intelligence (AI), Machine Learning (ML), cloud computing, quantum computing and 5G. We have seen the number of unsecured IoT devices increase, allowing attackers to easily access confidential and sensitive data. The modality of working from home has created an opportunity for cybercriminals to infiltrate computer systems. The development of AI phishing attacks has made it difficult to distinguish between a phishing email and an authentic email.

It is our understanding that the evolving nature of cyber threats requires a long-term, cooperative approach between States. We believe that to counter existing and potential threats States could improve the level of communication between them. It would be ideal if we were able ~~to~~ to adopt protocols on how information relating to existing and potential threats could be shared.

We note that some progress in the OEWG has been made in this regard. The establishment of a global Points of Contact (PoC) directory is a commendable initiative that would facilitate discussions between States, in particular, through the sharing of contact details for technical experts. This in turn will facilitate timeous sharing of threats related information and proactive ways to address them. Other methods of cooperation to mitigate extreme threats could include developing and sharing the tools to protect the security of ICT networks and applications.

Chairperson,

South Africa hopes that through this Open-ended Working Group States could agree on the importance of addressing rapidly-evolving threats to their ICT infrastructure in line with Norm 1 of the Rules, Norms and Principles of Responsible State Behaviour in Cyberspace.

Thank you.