South African Statement Agenda Item 5 on the "applicability of international law to the use of information and communications technologies by States," 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

7 March 2023

Chairperson,

We welcome the opportunity to elaborate our views on how international law applies to the use of information and communications technologies by States.

South Africa has consistently expressed its commitment to promoting a peaceful and stable cyberspace underpinned by international law, including human rights law, and consistent with the 11 norms of responsible State behavior.

We maintain our belief that the United Nations Charter applies in its entirety to cyberspace and that the principles of the UN Charter apply to cyberspace such as sovereign equality; the settlement of international disputes by peaceful means; respect for human rights and fundamental freedoms; and non-intervention in the internal affairs of other States.

Chairperson,

When discussing this matter, we should consider that a cyber operation may, depending on its scale and effects, violate the prohibition on the threat or use of force in Article 2(4) of the UN Charter.

When a cyber operation constitutes an armed attack under Article 51 of the UN Charter, States may exercise their inherent right of individual or collective self-defence, recognised in the Charter, while customary international law principles of necessity and proportionality remain applicable.

It is South Africa's view that a cyber operation could be deemed an internationally wrongful act when it is attributable to a State under international law and involves a breach of an international obligation of the State.

Therefore, States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs. If a State is notified of harmful activity emanating from its territory it must take reasonable steps to address such activity.

If a situation amounts to an armed conflict and cyber operations are carried out during that conflict, International Humanitarian Law (IHL) applies to these cyber operations as it does to all operations with a nexus to an armed conflict in general. It is our understanding that IHL prohibits the use of cyberspace to attack civilian infrastructure for example. During war and peacetime, States are required to take all feasible precautions to protect civilians and civilian objects.

Chairperson,

With this understanding in mind, we should encourage States to forge closer cooperation in developing and applying measures to increase security in the use of ICTs and to avoid ICT practices that could endanger the maintenance of international peace and security.

South Africa believes that we should develop a common understanding of the applicability of international law, including international humanitarian law, in cyberspace based on existing legal frameworks. In this regard, the Working Group would also benefit from briefings from international legal experts, and we have proposed garnering the views of bodies such as the international law commission to this end.

Chairperson,

We are closely following the discussion on this matter and we would propose having more time to discuss it, perhaps during the intersessional period.

I thank you.