On the matter of promoting common understandings on existing and potential threats in the sphere of information security, my delegation would like to make the following points:

Cyber security threats are one of the fastest emerging and rapidly evolving challenges to States’ security. The complexity of the cyber-security challenges is compounded by the fact that these threats could emanate from domestic or international sources, or from state or non-state actors. The risks may take the form of attacks on critical national infrastructure, criminal activity, “hactivist” protest action or bulk identify theft. In particular, ransomware attacks taking advantage of weak cybersecurity measures and practices as well as limited incident detection and response capabilities are a cause for concern.

States, especially developing countries, are all at varying positions of risk given the varying capacities of States to respond to the threats posed by malicious acts in cyberspace. The challenge for governments in responding to these threats is that cyber-security activities need to be pursued across the whole of government, including sub-national levels such as provincial or local government, independent agencies, state owned enterprises and contractors, and in coordination with the private sector actors.

South Africa remains concerned by the growing threat of cyber-attacks on critical infrastructure and critical information infrastructure. While we believe we should confront these threats through greater cooperation and the development of best practice
mechanisms, such efforts should be context-appropriate, support national priorities and
efforts to identify, designate and safeguard such infrastructure.

The challenges emanating from the inter-connectedness of cyberspace are not only
relevant to interactions between States, but also extends to the public and private
domains within States. The developmental perspective to close the digital divide does not
only support socio-economic objectives, but also supports the peace and security
objectives. Specifically, raising the general level of the ICT capacities in States will also
buttress the overall resilience to cyber threats of States.

In addressing these challenges, the first OEWG report already provides important
practical markers which the current OEWG may wish to take forward: national
implementation of the existing norms, developing and sharing of experience and good
practice.

In this regard, capacity building and assistance in support of national priorities remain
critical in bringing States on par for the betterment of the security of global cyberspace,
as this is truly a global challenge that requires global solutions.

To govern the use of cyberspace and especially the threats posed to international peace
and security, South Africa supports the applicability of international law and specifically
the United Nations Charter in its entirety. South Africa believes a discussion on how to
practically operationalise applicability of international law will enrich national and
international efforts to prevent and counter threats in area of information security.
Achieving common understandings on how international law applies and implementing
these will build essential trust amongst States.

Finally, we believe that the engagement of all relevant actors, including civil society and
the private sector, is important to both understand the nature of these threats and to
cooperate and adequately address, across all of society, the threats posed by both State
and non-State actors.

Thank you,
On rules, norms and principles of responsible states behaviour and their implementation:

South Africa believes that voluntary norms add an additional layer of understanding to the applicability of international law in cyberspace and is, therefore, an important aspect of our work and outcomes. South Africa looks forward to the exchange of views on where Member States may see the need for the further development of rules, norms and principles for responsible State behaviour.

Chairperson,

It may help our work to approach this discussion from the assumption that efforts towards implementing the current norms and their further development are not mutually exclusive. Having said that, we are also cognisant of the potential strain or difficulty of handling both the implementation of current and development of future norms in parallel could have on our limited resources.

Another point of departure that may assist our work is to agree that the further development of norms, rules and principles should be understood as a process of evaluating, updating where necessary, and refining rather than seeking to develop a completely new set of norms. The latest First Committee and GA adopted resolution on Developments in the field of information and telecommunications in the context of international security supports this understanding. It is our understanding that if the focus was to be solely on the development of new norms, the impact of the international community’s efforts in addressing the fast-emerging threats will be minimal.

At a practical level, my delegation believes that it is important for Member States to document their implementation in a standardized template so that gaps may be identified and addressed. For this reason, South Africa supports the use of the model of the National Survey of Implementation of United Nations General Assembly Resolution 70/237.

Chairperson

As for national efforts, South Africa’s Cybersecurity Policy Framework is aimed at creating a secure cyberspace environment and reinforcing the regulatory framework,
project information infrastructure in cyberspace, reduce vulnerabilities, build capabilities to prevent and respond to attacks or threats, and reduce damage from cyber incidents. We aim to achieve this through structured and regular inter-departmental and inter-agency coordination and implementation according to the respective mandates. Coordination with the private sector forms an essential part of the work.

Finally, Chairperson, my delegation appreciates some of the practical proposals that have been made in terms of the implementation of rules, norms and principles, and we believe that the proposed Programme of Action on implementing the UN framework in this regard, is one aspect of implementation that we can consider as an action orientated approach, which should go hand in hand with capacity building and strengthening our global response to cybersecurity challenges.

I thank you.

On how international law applies to the use of information and communications technologies by States we would like to make the following brief remarks:

South Africa supports a rules-based international system. To govern the use of cyberspace and especially the threats posed to international peace and security, South Africa supports the applicability of international law and specifically the United Nations Charter in its entirety.

Chairperson

We live in an increasingly interconnected world, and thus jurisdiction and territory have become complicated. The responsibility of States to reject the use of their territories for launching attacks is more important now than ever. South Africa looks forward to fruitful discussions on international law which, although sufficient may not be adequately responsive to the emerging challenges of cyber security.

South Africa welcomes the conclusion of the first OEWG that international law applies to the cyberspace and the recognition that more work is needed to reach common understandings on how international law applies. We therefore could support an approach
of referring the question to the International Court of Justice and the international law commission to establish their views on the matter.

I thank you.

On **Capacity Building**, Chairperson,

It would be fair to say that cyber risks disproportionately affects States lacking cyber capacity, and in this regard it is our understand that our global response is only as strong as its weakest link. It is in this context that we consider capacity building as the most important issue for developing countries, and vital in our multilateral response to the challenge of cybersecurity.

States generally, but especially developing countries, are all at varying positions of risk given their varying capacities to respond to the threats posed by malicious acts in cyberspace. Capacity building is critical in bringing States on par for the betterment of the security of global cyberspace, as this is truly a global challenge that requires pervasive solutions.

While, South Africa supports the approach to capacity building as set out in the report of the first OEWG, we would, however, have preferred to see emphasis on a context specific or context appropriate approaches being added to considerations of capacity-building, and that activities in this regard should be evidence-based, politically neutral, transparent, accountable, and without conditions.

As in other areas, capacity building efforts are dependent on sustainable financing, and facilities or mechanisms in support of national cybersecurity efforts. Linked to this, the OEWG may wish to consider some form of appropriate institutional arrangement to take this matter forward. Options which the OEWG may explore include the development of a general norm, mechanism or system dedicated to capacity building, or special programs tailored to specific needs or priorities. We, therefore, look forward to specific engagement in developing a way forward in this regard.

I thank you.