CONSIDERATIONS ON THE INITIAL PRE-DRAFT OF THE OPEN -ENDED WORKING GROUP (OEWG) ON DEVELOPMENTS IN THE FIELD OF INFORMATION AND TELECOMMUNICATIONS IN THE CONTEXT OF INTERNATIONAL SECURITY

We would like to thank H.E Ambassador Jurg Lauber, Chair of the United Nations Open-Ended Working Group (OEWG) on the Developments in the Field of Information and Telecommunications in the Context of International Security, FOR THIS INITIAL Pre-Draft.

We welcome the Chair's attempt to produce a balanced report and the Pre-draft's recognition that the benefits of digital technologies are not evenly distributed and that the narrowing digital divides remains an urgent priority for the international community. We underline that Zimbabwe together with other developed countries face this predicament. It is our shared concern that development of offensive ICT capabilities, militarisation of the cyberspace, cyber- attacks, cyber-crimes as well as cyber terrorism are now a global menace and significantly pose grave threats to the security and stability of nations.

We seek to strengthen the following as areas of agreement in the text, as well as additional input on the norms and recommendation sections of the report.

1.Existing and potential threats

We note that the Pre-draft appears to emphasize on State, proxies and criminal behaviour in the cyberspace. We reiterate concern over the prevalent misuse of media platforms, including social media networks, for hostile propaganda, interference in the internal affairs of other States, dissemination of discriminatory and distorted information of events such as election results, and campaigns that defame and incite hatred among citizens. Cybersecurity should indeed, follow a multistakeholder approach, however, private sector, non- governmental organisations and social media platforms should be also regulated and made accountable for their behavior in the ICT environment.

We support proposals from some States (China, Cuba and Russia) that any rules, norms and principles aimed at ensuring responsible behaviour of States in the cyberspace environment should therefore not undermine sovereign rights of respective States. States have the right to make ICT-related public policies consistent with national circumstances to manage their own ICT affairs and protect their citizens' legitimate interests in the cyberspace. States have the rights and responsibilities to

ensure the security of personal information and important data relevant to their national security, public security, economic security and social stability.

2.Capacity Building

We welcome the realisation that Capacity Building helps to develop the skills, define the policies and build the institutions that increase the resilience and security of States so they can fully enjoy the benefits of digital technologies. The suggestion that developed countries should be encouraged to enhance their technological and financial assistance to developing countries to enhance their emergency response capabilities and commitments to the 2030 Sustainable Development Agenda is encouraging. However, the Pre-draft should expand on challenges and restrictive measures that were identified that hinder or reduce the effectiveness of capacity-building. Unjustified sanctions and embargoes in any form are a threat to this initiative. These unilateral measures prevent universal access to the benefits of ICTs.

The provision of assistance and cooperation should be demand-driven and made upon request by the recipient State, taking into account its specific needs and peculiarities.

All efforts should be exerted to fully protect the confidentiality of information related to the recipient State's policies and measures to protect its national infrastructures and the confidentiality of its ICT emergency response plans in order to avoid any possibility of jeopardizing such information or undermining the effectiveness of these measures and plans.

Global governance in cyberspace is a significant task for the international community. States should work together to create a multilateral, democratic and transparent global Internet governance system. Service providers charged with management of IT critical resources should be independent from any State's control to ensure the broad participation and joint decision-making of all States.

3.International Law

The text presented in the pre-draft states that *"existing international law, complemented by the voluntary, non-binding norms that reflect consensus among States, is currently sufficient for addressing State use of ICTs"*. It is our view that there was no outright consensus on this topic. On the contrary, the existing international law is insufficient and should be adjusted in a way to become applicable to the ICT environment. The legal gaps should be filled by new international legal rules and norms. New international legal instruments tailored to the attributes of ICTs and evolving realities should be developed to hold wrongdoers accountable within the

framework of the UN to cover security issues that have been overlooked. The principles enshrined in the UN Charter, including sovereign equality, refraining from the use of force, settlement of disputes by peaceful means and non-intervention in the internal affairs of other states, apply in cyberspace.

From the perspective of maintaining peace and preventing conflict, states should focus on the implementation of such principles as settlement of disputes by peaceful means and refraining from the use or threat of use of force. Willful use of force, punitive and confrontative countermeasures under the guise of article 51 of the Charter, which legitimizes the right to self-defense, cannot be automatically applied in the event of a cybersecurity incident nor be used to justify a conventional attack in response. The recognition of the applicability of the "right to self-defense" under Article 51 as well as the applicability of international humanitarian law would turn the cyberspace into a conflict zone.

4.Confidence Building Measures

The Purpose of introducing Confidence Building Measures is to increase mutual trust, predictability and reduce misperception for the interest of ensuring cybersecurity. States can conduct policy and technical exchanges, law-enforcement cooperation and information sharing on a voluntary basis. Confidence building measures should be taken progressively so as to enhance mutual trust and reduce misperception.

5.Supply Chain Security

Supply chain security is crucial for enhancing users' confidence and promoting digital economy. It appears the pre-draft is silent on this important topic and should have included proposals from other states (China) that States should not exploit their dominant position in ICTs, including dominance in resources, critical ICT infrastructures and core technologies, ICT goods and services to undermine other states' right to independent control of ICT goods and services as well as their security.

6.Regular Institutional Dialogue

Zimbabwe supports efforts to develop universally accepted norms, rules and principles of responsible behavior of States within the framework of United Nations, and recommends the renewal of the mandate of the OEWG with the same aims and

objectives it was founded at the 75th session of the UNGA to enhance its continuity. The recommendations in the Pre-draft report to resume the works of the OEWG at the 76th session of the United Nations General Assembly is retrogressive.

Further, the recommendation that the 76th Session of the General Assembly of the United Nations also consider requesting the Secretary-General to establish a new group of governmental experts is misplaced. This recommendation should instead only arise within framework of the GGE.