Permanent Mission of the Republic of Kenya
To the United Nations, New York

FIFTH SUBSTANTIVE SESSION OF THE OPEN-ENDED WORKING GROUP (OEWG) ON SECURITY OF , AND IN THE USE OF INFORMATION AND COMMUNICATIONS TECHOLOGIES (ICT) 2021-2025

24TH JULY-29TH JULY 2023 - 10-1pm - **CR 2**

REMARKS BY AMB. MICHAEL KIBOINO - DEPUTY PERMANENT-REPRESENTATIVE

Session 1:

Existing and Potential Threats in The Sphere of Information Security, inter alia, Data Security, and Possible Cooperative Measures to Prevent and Counter Such Threats

Mr. Chair, (*Amb. Burhan Gafoor*)

Deputy to the USG and High Representative of for Disarmament Affairs Mr. Adedeji Ebo

Excellencies and Colleagues,

1. Kenya commends you Chair, and your team for your continued efforts in providing us with an action-oriented programme of work , as we put our efforts together to engage with the second Annual Progress Report for a consensual outcome for this session.

2. You can count on Kenya's support. It is our position that the revised draft of the second APR reflects the actual discussions tabled and therefore a good starting point for discussion and negotiations. We commend your efforts long before the beginning of this session to consult and try and find a middle ground on the issues.

3. Chair, "On Existing and Potential Threats" , the concerns reflected in paragraph 10; and the subsequent sections, 10 bis, 10 ter, and 10 quater are reflective of the broad implications that existing threats continue to pose to our ICT ecosystems, including Critical Infrastructure (CI) and Critical Information Infrastructure (CII) . Not to mention the urgency to address them.

4. **Colleagues**, the nature of emerging technologies, including their ubiquity, programmability, and data-driven nature, has also opened a door for misuse by cyber threat actors.

5. The increasing malicious use of ICTs by terrorist and criminal groups continues to hamper developing nations' efforts in delivery of essential services to its citizens and subsequently stalling efforts to bridge the digital gap.

6. It is our hope that highlighting this issue in para 10 will lead to enhanced global collaborative efforts in combating violent extremism and terrorist activities in the ICT ecosystem.

7. In relation to AI and quantum computing, **Mr. Chair**, and specifically AI and its use in deepfake, we support the language of para 14 including the emphasis that despite the neutrality of the technology, it has the potential of being used for high-stake national mis- information, dis-information and mal-information with capabilities of destabilizing a states' peace and national, regional and international security given the increasing exploitation of threat vectors related to information systems.

8. One of the challenges Kenya has experienced is with mal-information or deepfakes where mimicking of high-level

representatives contributes to fanning hostilities and divisions. Consideration of possible interventions and mitigation measures must remain a priority.

9. Malicious cyber threat actors exploit these technologies using malware, ransomware, Distributed Denial of Service (DDoS), and crypto jacking attacks, which compromise container-based cloud systems, restrict access to services, expose restricted data, and enhance backdoor attacks.

10. **Mr. Chair**, in relation to para 15, we appreciate the inclusion and urge the retention of this para as an implementation , and capacity building measure. Its reflection here is a non-politicized urge for the international community to enhance its cooperation in addressing existing and potential threats to information and data security, while leveraging accessibility to the threat landscape for all.

11. To deepen our understanding of potential risks, the international community should consider establishing a UN-run repository of common threats that members can regularly update in the face of new and emerging threats.

12. The language of para 15 as it stands allows for a voluntary, practical, and neutral platform that Kenya believes will be critical once operationalized. Based on discussions in the Fourth

Substantive Session, my delegation has since circulated a revised draft working paper that further emphasizes the non-attribution and non-duplicatory nature of this proposal for your further consideration.

13. My delegation looks forward to your views including an engagement on the modalities of the platform within the OEWG.

14. **Chair**, we all agree that technology transcends international borders , and such an effort is in the spirit of the mandate and building blocks of the OEWG. We therefore wish to request that the para remains as is , and we retain the words stricken out, that is " and facilitate a discussion on cooperative measures to address them."

15. Additionally, para 15 lends credence to paragraph 18, as such a repository would be an ideal source of information and addressing the lack of awareness of existing and potential threat including the lack of adequate capacities to detect, defend against or respond to malicious ICT activities.

16. Paragraph 16 Chair articulates the need for a gender perspective in addressing ICT threats including specific risks faced by vulnerable groups. Kenya supports this para considering the important role of ICTs and the role they play in socio-economic development that encompasses even the most vulnerable members of our society, the underserved, marginalized and People With Disabilities (PWD).

17. As a country, we have embarked on an ambitious project which has borne fruit, in the inclusive digitization of 5068 Citizen services. This is against the reality of how irresponsible acts from both state and non-state actors can have significant impact to the delivery of citizenry services and even a potential threat to its stability.

18. On recommendations and next steps, Kenya supports the recommendation as outlined in Paragraph 19 , and 21 as spelled out in the APR but with a more approach that includes Quantum computing, artificial intelligence and "ALL other emerging technologies. "

19. We also however wish to request that the language in paragraph 20 remains as was initially worded or the reasons we have outlined.

20. On our part , we have sought initiatives to mitigate against new and emerging ICT threats by enhancing broad multi-stakeholder conversations, and forge partnerships with technology providers to have security by design that factors in geo-cultures whose preservation is important in maintain regional security.

21. In its quest to secure its digital space, Kenya has among others established the National Kenya Computer Incident Response Team (National KE-CIRT/CC); implemented the National Public Key Infrastructure (NPKI); and recently inaugurated the National Computer and Cybercrimes Co-ordination Committee (NC4) comprising relevant ministries, and agencies with a fully-fletched secretariat.

22. Colleagues, more must be done to assist States in their efforts to deal with the challenges associated with the increased levels of digitization, use of cryptocurrencies, and miniaturization of devices that have led to increased anonymity in internet and network accessibility especially with unregulated technologies.

23. **I therefore conclude** by reiterating our call for practical support for efforts to establish programs and mobilize resources to unlock greater access for developing countries, to ensure that no State is left behind.

I thank you.