Proposal for threats chapter for OEWG annual report 2022 from Australia, Botswana, Chile, Costa Rica, Denmark, Indonesia, Malaysia, the Netherlands, and the United Kingdom

We propose the following language to expand upon paragraph 7a of the Chair's draft Rev 1:

7. States ~~made concrete, action-oriented proposals to address~~ exchanged views on existing and potential threats, ~~The following is a non-exhaustive list of proposals with varying levels of support from~~ , and possible cooperative measures to prevent and counter such threats[1]. States ~~that may be further elaborated upon and supplemented at forthcoming OEWG sessions: recalling~~ recalled the threats identified in the 2021 OEWG report, reiterating increasing concern that threats in the use of ICTs continue to intensify and evolve, and underscoring the implications of the malicious use of ICTs for the maintenance of international peace and security[2].

States recalled the risk that any use of ICTs by States in a manner inconsistent with their obligations under the framework, which includes voluntary norms, international law, and CBMs, undermines international peace and security, trust and stability between States[3]. States also recalled that a number of States are developing ICT capabilities for military purposes and that the use of ICTs in future conflicts between States is becoming more likely[4]. These statements have been realised.

In particular, States noted factors that could play an escalatory role in and around armed conflict. These include malicious activity that results in cascading critical infrastructure effects in other States, and the role of non-state actors. Furthermore, the Group notes a worrying increase in States' malicious use of ICT-enabled covert information campaigns to influence the processes, systems and overall stability of another State[5]. Noting the potentially devastating security, economic, social and humanitarian consequences of malicious activity against critical infrastructure[6], States acknowledged that malicious ICT activity in conflict situations may also disrupt humanitarian operations.

New and emerging technologies expand the attack surface creating new vectors and vulnerabilities that can be exploited for malicious ICT activity[7].

States also highlighted the increasing implications for international peace and security where the effect of malicious use of ICTs by non-state actors, including terrorists and criminal groups, rises to the level of a national emergency, particularly when CI and CII are targeted, including the threat posed by ransomware. States recalled that threats may be experienced differently by States according to their levels of digitisation, capacity, ICT security and resilience, infrastructure and development.[8]

In light of the increasingly concerning digital threat landscape, and recognizing that no State is sheltered from these threats, States underscored the urgency of implementing and further developing cooperative measures to address such threats[9] under the respective elements of the framework. States emphasized the importance of a global, interoperable, open internet[10].States proposed that the OEWG, as a UN inter-governmental body, could be ~~a platform~~ an open, inclusive and democratic multilateral process to foster global, ~~inter-regional~~ cooperative approaches ~~on security in the use of ICTs~~ and measures in this regard[11].

[1] Chinese proposal adapting Chair's draft Rev 1

[2] Chairs draft Rev 1

[3] Para 17 of 2021 OEWG report

[4] Para 16 of 2021 OEWG report

[5] Para 9 of 2021 GGE report

[6] Para 18 of 2021 OEWG report

[7] Para 11 of 2021 GGE report

[8] Para 21 of 2021 OEWG report

[9] Para 22 of 2021 OEWG report

[10] Reflects Chinese proposal

[11] Chinese proposal adapting Chair's draft Rev 1