Comments submitted by Brazil to the Initial "Pre-draft" of the report of the OEWG on developments in the field of information and telecommunications in the context of international security

8 April 2020

INTRODUCTION

Paragraph 6 of the "pre-draft" contains language ("the OEWG is uniquely positioned […]") that could be interpreted as implying that the OEWG has preponderance vis-à-vis the 2019-2021 Group of Governmental Experts on cybersecurity. In Brazil's view, both processes were approved by the United Nations General Assembly (resolutions 73/27 and 73/266) and, therefore, enjoy the same degree of legitimacy.

EXISTING AND POTENTIAL THREATS

It would be advisable to add (possibly in paragraph 15 of the document) a reference to the fact that, without a culture of restraint, the tendency of militarization of cyberspace will contribute to making conflicts more likely, both in the cyber and the kinetic domains, to the detriment of peace and international security.

Also in regard to paragraph 15, the increasing development of automation and autonomy in information and communication technologies (ICTs) carries the risk that such instruments will not be subject to human control, thereby jeopardizing the effectiveness of and compliance with international humanitarian law (IHL).

Brazil attaches fundamental importance to the need for adequate protection against threats to critical infrastructure, especially electrical, water and sanitation systems (paragraph 19). Electoral processes are also vulnerable to illegitimate interference through the malicious use of ICTs, and they should also be considered an essential component of the critical infrastructure of States.

Given the inherent interconnectedness of ICTs, their malicious or offensive use entails a danger of unintended escalation and systemic effects, thereby causing damage to third parties not involved in cyber conflict or hostilities.

INTERNATIONAL LAW

Paragraph 24 of the "pre-draft" confounds areas of international law (IHL, International Human Rights Law, International Criminal Law) with its sources (custom), and by citing only one source, suggests its precedence over others, such as treaty law and general principles of law.

Additionally, regarding the following sentence (on the issue of State responsibility), the use of the term “applicable” would not be appropriate. The sentence could be replaced with the following language, adapted from the draft Articles on State Responsibility of the ILC: "It was also noted that every internationally wrongful act of a State entails the international responsibility of that State, including in their use of ICTs".

Brazil attaches great importance to the language contained in paragraph 25, which reaffirms the fundamental importance of IHL and recognizes its contribution to reducing risks and potential harm to both civilians and combatants in the context of an armed conflict, as well as underscores that IHL does not encourage militarization or legitimize conflicts in any domain, including cyber.

In view of language already agreed in the previous GGEs on cybersecurity and in order to avoid setbacks, Brazil encourages the inclusion of specific references to the principles of IHL related to cybersecurity (humanity, necessity, proportionality and distinction) in paragraph 27.

Brazil also strongly supports the elements contained in paragraph 32, especially with regard to the need for a common approach to the problem of attribution of cyber attacks, an issue that deserves further development. In the view of Brazil, this is one of the crucial (and, at the same time, one of the most contentious) points in the field of cybersecurity. The political and technical complexities associated with attribution of responsibility for the use of cyber weapons has no parallel in the regimes applicable to other categories of weapons, be they conventional or of mass destruction.

RULES, NORMS AND PRINCIPLES OF RESPONSIBLE STATE BEHAVIOR

From the point of view of Brazil, the IT infrastructures underpinning electoral processes also deserve the same protection accorded to the public core of the Internet (paragraph 38).

REGULAR INSTITUTIONAL DIALOGUE

Brazil strongly supports the continuation of the debate and institutional strengthening of the UN in the field of cybersecurity, as indicated in paragraph 61 of the "pre-draft".

As noted above in regard to paragraph 6, this section – and in particular in paragraph 62 – should steer clear of any language which implies preponderance of the OEWG vis-à-vis the GGE (such as the sentence "the OEWG format should become the standard for discussion […]").