



Statement by H.E. Mr. Ronaldo Costa Filho
Permanent Representative of Brazil to the United Nations

During the Security Council Arria-Formula Meeting
“Cyber Stability, Conflict Prevention and Capacity Building”

22 May 2020

Mr. Chairman, I thank Estonia, Belgium, the Dominican Republic, Indonesia and Kenya for convening this Arria-Formula meeting of the Security Council, which provides an opportunity for us to discuss the prevention and response to threats to international peace and security emanating from the cyberspace, and the role of the Security Council in this regard.

Cybersecurity is an issue to which Brazil attaches the utmost importance. The Brazilian government adopted, in 2018, of a specific law on data protection and privacy, complementing a 2014 law on internet governance. This year, the Brazilian Government adopted a new National Strategy on Cybersecurity, which aims at increasing Brazil's resilience to cyber threats and at contributing to the country's prosperity and reliability in the digital environment.

As any other human domain, cyberspace ought to be subject to law. The UN General Assembly has unanimously endorsed three consensus reports adopted by the Groups of Governmental Experts (GGE) it established since 2004. These reports clearly stated that international law, and the UN Charter in particular, applies to cyberspace, and put forward a set of norms, rules and principles for responsible State behavior in cyberspace. The GGE reports also advanced a set of principles on confidence-building and capacity-building. Taken together, these three mutually-reinforcing elements form a “triad” that is the basis of the ongoing efforts to build a comprehensive and effective international cybersecurity regime.

These norms, rules and principles and the challenges associated with their implementation are being further examined and developed in the context of two fora established by the UN General Assembly in 2018, namely the Open-Ended Working Group (OEWG), chaired by Switzerland, and a new iteration of the Group of Governmental Experts (GGE), which is chaired by the Brazilian expert, Ambassador Guilherme Patriota.

The differences between the GGE and the OEWG in terms of format, mandate and membership represent both challenges and opportunities. Their respective strengths and comparative advantages must be utilized fully, so their results complement and reinforce each other.

Turning now to the issue of the role of the Security Council, Brazil believes that it would be inappropriate for the Council to seek to create new norms in the cyber-security realm, especially because this theme is the object of two dedicated fora established by the General Assembly. In our view, and in order to avoid duplication of efforts, the Council should also abstain from organizing cyber capacity-building either, owing to limitations from its mandate, composition and institutional framework.

However, it must be recalled that, as a consequence of the mandate given to it by the UN Charter, the Council has a responsibility to address and respond to specific threats to international peace and security that may arise from the cyber domain. So far, however, the Council has only touched upon the issue of cybersecurity in the very limited context of counter-terrorism and of country-specific sanctions.

The relentless growth in the number of malicious cyber operations is a worrisome hallmark of our age. Even though most such operations do not fall under the recognizable category of acts of war or even of use of force, they are of an unequivocally unpeaceful nature. This entails a recognition of a unique, hybrid state of "unpeace" in cyberspace. Suffice it to say that the harmful consequences of those sub-threshold cyber operations have been greater than in any previous period of the post-cold war. In fact, the damage to national and economic security from malicious cyberattacks and cyberespionage is conceivably greater than even some acts of war or use of force could achieve.

How should the Security Council react to such situations, in particular those that are caused by actions of States?

In Brazil's view, the Council should be guided first and foremost by the objective of promoting adherence to the past and future recommendations adopted by the UN General Assembly on the issue of cybersecurity.

Regarding possible cases of internationally wrongful acts in cyberspace affecting peace and security, the work of the Council will be impaired by the absence of credible and consensual criteria for attribution of responsibility for such acts. Brazil believes, therefore, that there is a pressing need for in-depth and inclusive discussion on this matter.

Once again, I thank the organizers of this Arria-formula meeting, and I reiterate Brazil's firm and constructive engagement regarding the issue of cybersecurity.

Thank you Mr. Chairman.