Statement by H.E. Mr. Masud Bin Momen, Ambassador and Permanent Representative of Bangladesh to the United Nations in the First Substantive Session of the Open-ended Working Group on developments in the field of information and telecommunications in the context of international security

CR-4, UNHQ on New York, 9 September 2019

Mr. Chairman,
I would like to join other delegations in congratulating you on your election as the chair of the Open-Ended Working Group (OEWG). Bangladesh aligns itself with the Statement delivered by Indonesia on behalf of NAM.

Excellencies,

Our Hon’ble Prime Minister Sheikh Hasina at a side-event during the high-level week of the UNGA in September 2018 said and I quote “I pledge Bangladesh’s support for promoting a culture of cyber security at the UN and beyond…. We must demonstrate our strong political resolve to create a secure, stable, peaceful, inclusive and accessible cyber space for our future generations.” The first ever digital economy report by UNCTAD which came out earlier this month echoed essentially a similar notion of a secure cyber environment for creating a “digital economy for the many, not just the few”. Indeed, cyber security is the sine qua non to preserve the inherently open and inclusive nature of the internet and digital economy for the benefit of all.

In Bangladesh, we consider ICT as a major driver of our sustainable development efforts. We envision transforming Bangladesh into a digitally advanced middle-income country by 2021 and a developed country by 2041. During the last decade, we have been able to expand benefits of e-governance and e-commerce services to our citizens in a large scale. For example, we are now offering over a hundred important public services such as birth registration, land records, passports, banking and e-Commerce to our citizens through One-stop Digital Centres in rural areas. Our export earnings from the ICT sector have significantly gone up in recent years due to some effective policy interventions and fiscal incentives. In effect, ICT has changed many old business rules by empowering people through free flow of information and easing financial transactions.

But cyber security remains a big challenge. On our part, we are working towards building a safer ICT ecosystem in the country to tackle it. Over the last few years, we put in place Bangladesh Cyber Security Strategy, National ICT Policy, Information Security Policy Guidelines and Digital Security Act. A Digital Forensic Laboratory has been set up for training purposes. Bangladesh Computer Emergency Response Team is working with other friendly countries. We held an international conference in Dhaka on cyber-security in 2017. Yet, we are aware that no single government can do it alone. Cyber space has no physical borders and it is ever expanding. In an interconnected world, a weaker link anywhere can cause disruption for others. Keeping this in mind, I would like to put forward some specific points for consideration of the group:

First, the UN must continue its norm-setting role in cyber-space in an inclusive, open and transparent manner. We welcome the opportunities for developing countries like us to voice our concerns and priorities through the works of the OEWG and play our due part towards defining future rules of the road, enhancing confidence-building and security measures in cyber-space. We also recognise the
valuable works of the previous GGEs particularly the hard-earned gains across the 2013 & 2015 GGE reports. Going forward, we expect the two parallel processes to have more informed dialogues for creating convergences and reducing duplication of efforts.

Second, international cooperation in capacity building for cyber security must be given priority. Development partners should consider specific supports to technologically less advanced countries. In Bangladesh, we fixed a target to have at least one thousand cyber security experts in the country by 2021. We need enhanced capacities in areas of defending cyber-attacks, creating awareness, and developing reliable early-warning systems through information sharing across Governments and major Tech firms.

Third, in the absence of a globally accepted norms structure, the principles of the UN Charter and relevant international laws should apply to the cyberspace. We should work together to overcome trust deficits by investing more on confidence building measures through multilateralism.

Fourth, the possibility of terrorists acquiring lethal cyber-capabilities and attacking critical infrastructures is a serious threat to international peace and security. We need constant engagements for sharing best practices to tackle terrorists’ use of cyberspace, attacks against critical infrastructures, cyber thefts, and sharing critical information, and data on cyber incidents.

Fifth, we must build public-private partnership to tackle cyber issues. In Bangladesh, we have recently signed an agreement with Microsoft's Digital Crimes Unit to build the capacity of our Cyber security experts. We see the works of the High-level Panel on Digital Cooperation convened by the UN Secretary-General involving actors from Governments, the private sector, civil society, international organizations, academia, and technical community as an important stepping stone in building multi-stakeholder partnerships & paving the way towards a global norm setting exercise.

Sixth, identifying the actual source of wrongful activity for reparations and legal measures remains a challenge. Developing countries should have access to technologies and information to detect such sources.

I thank you all.