

Statement by H.E. Mr. Masud Bin Momen, Ambassador and Permanent Representative of Bangladesh to the United Nations in the event titled “Cyber Security and Capacity Building” organized by Singapore in collaboration with UNODA on 25 April 2019 at 1:15 PM

Excellencies

Ladies and Gentlemen,

I thank the Permanent Representative of Singapore for inviting me to this event and for making me part of the launching of the UNODA-Singapore flagship online training course on international cybersecurity. I appreciate the focus of this event on cyber capacity building of actors and users beyond high-tech experts and professionals. Last year, we partnered with Singapore and UNODA for organizing a high-level side event on Cyber Security and International Cooperation on the margins of the high-level week where our Prime Minister Sheikh Hasina participated. We are also happy to be part of the groups of Friends on Cyber security and E-governance co-chaired by Estonia and Singapore.

Ladies and Gentlemen,

In today’s world I can hardly imagine a more important but less understood issue than cyber-security. Over the last few decades, cyber threats have evolved as one of the most serious economic and national security challenges. Moreover, the strategic rivalries in the cyber domain are on the rise. The future looks even more dangerous with threats emanating from possible weaponization of robots, AIs etc. Despite all these real and enormous threats we are still struggling with globally agreed definitions about the meaning of offense, defense, deterrence, escalation, and norms & regulations in cyber space.

Dear friends,

In Bangladesh, we consider ICT as a key driver of our sustainable development efforts led by Hon’ble Prime Minister Sheikh Hasina. We envision transforming Bangladesh into a digitally advanced middle-income country by 2021 and a developed country by 2041. During the last decade, our investments in the ICT sector have paid us rich dividends. We have been able to expand access to ICTs for our people in an unimaginable pace. Taking advantage of e-governance and e-commerce, we could bring services and commodities to the doorsteps of our people. The Government has become more efficient, transparent and accountable in delivering services.

Along our journey, our financial sector endured a big setback in 2016, when more than 80 million USD of Bangladesh Central Bank was siphoned by hackers. Eventually, a large portion of the money landed in another country and through its banking channel reportedly reached the country’s casino system. Ever since the money remains traceless. The fact that the hackers had been able to breach the supposedly secure global money transfer system is, no doubt, an alarming development. Also, more revealing had been the weaknesses of global financial system in terms of detecting imminent threats, preventing damage, identifying and attributing cyber offenders, gathering evidential proofs, lack of legal remedies and the question of application of international law in cases of such transboundary crimes.

We reckon that our hard-earned gains in the ICT sector need to be made secure. On our part, we are working towards building a safer ICT ecosystem in the country. We felt the need for strengthening not only the cyber resilience of our financial sectors, but also promoting a cyber-security culture across various administrative, legal and business continuums. Over the last few years, we put in place Bangladesh Cyber Security Strategy, National ICT Policy, Information Security Policy Guidelines and Digital Security Act. We are also working towards formulating Digital Security Agency Rules and National Digital Commerce Rules. In terms of capacity building, we have a target to have at least one thousand cyber security experts in the country by 2021. 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.

But this is not enough. We all know that the cyber space has no physical borders, no single government can manage its security on its own. Our only hope for a free, secure, stable, accessible and peaceful ICT environment is through cooperation & partnership. I put forward a few points for your consideration:

First, the UN must continue its norm-setting role in cyber-space. In doing so, it is critical to build on the previous works of the GGE. Alongside, it is crucial to bridge gaps with parallel processes across OEWG for defining future rules of the road, enhancing confidence and building security measures. The future processes also need to create more opportunities for developing countries to voice their concerns. Rightfully, in Secretary general's Agenda for Disarmament there is adequate focus on this issue.

Second, we must demonstrate strong political commitments to ensure a secure cyber space for our future generations. Prime Minister Sheikh Hasina pledged Bangladesh's support for promoting a culture of cyber security and called for a UN High-level Conference on Cyber-security in September 2018. We look forward to working with our partners towards achieving that goal.

Third, in absence of a globally accepted norms structure, the principles of the UN Charter and relevant international law should apply to the cyber space. We should work together to overcome trust deficits and address the question of appropriate balance between civil rights and responsibilities in cyber space.

Fourth, we need meaningful global cooperation for defending cyber-attacks, creating awareness, developing reliable early-warning systems, creating capacity to coordinate across sectors including Governments and major Tech firms. Development partners should consider specific supports to technologically less advanced countries.

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 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.

I thank you all.