Statement delivered by

MR. ARIEL R. PENARANDA
Minister
Mission of the Republic of the Philippines to the United Nations

Cluster 5 of the First Committee
(Thematic Debate on Other Disarmament Measures and International Security)
25 October 2018
United Nations General Assembly, New York

Mr. Chair,

The Philippines associates itself with the statements of ASEAN and the NAM.

The importance for the Philippines of information security is reflected not only in our National CyberSecurity Plan, but also in our National Security Strategy. The programs under our national plan aim to ensure the protection of critical infrastructure, the government itself, businesses and supply chains, as well as individuals. Our national strategy, on the other hand, lays down the government’s strategic actions on cybersecurity, which include our Cyber Security Plan 2022. We also have in place the requisite laws to address issues on information security.

International cooperation on cybercrime, including cooperative efforts to develop effective national legislation, is a major focus for national efforts. Such cooperation is crucial given cybercrime’s transnational nature and the close relationship between crime and national security in cyberspace. Thus, the international community has seen the development of a number of multilateral instruments. However, they are sometimes cooperative and sometimes competing.

While the Philippines sees the importance of efforts to collectively address disruptive global cyber threats, we also recognize the challenges in addressing divergent interests and forging a common approach.

The Philippines proposes that we pursue the following elements:

1. Continue international and regional dialogue with the aim of reducing and anticipating the risks and protecting critical infrastructures.
2. Implement existing norms such as those arising from the previous UN GGEs, and nurture synergies in the work of the newly established OEWG and GGE.

3. Aim, where possible, for the standardization and universalization of legislations by sharing and comparing good practices on a global scale.

4. Facilitate the engagement of leaders from industry, academia, and civil society with governments to prevent cyber conflict, restrict offensive cyber operations by nonstate actors, and mitigate the daily threats to the global economy. We need an approach that is inclusive, comprehensive, and responsive.

5. Enable an easier cyber incident attribution. This will ensure that states are held responsible for what happens in their cyber realm, but at the same time ensuring observance of international law principles such as noninterference in the internal affairs of states.

6. Facilitate the provision of assistance to states that lack the capacity to thwart cyber threats.

Mr. Chair,

In order for us to move forward, my delegation believes that we must give acute focus on building trust and confidence to facilitate our work.

Thank you, Mr. Chair.