Statement by Mr. Seyed Mohammad Ali Robatjazi,
Director, Office for Disarmament and Non-Proliferation Affairs, Islamic Republic of Iran
On Other Disarmament Measures and International Security
First Committee of the United Nations General Assembly
New York, 30 October 2018

In the Name of God, the Most Compassionate, the Most Merciful

Mr. Chairman,

My delegation associates itself with the NAM statement delivered by Indonesia.

Along with the rapid advances in information and communication technologies (ICT) as well as the growing dependence of critical infrastructures on them, new and sophisticated cyber risks and threats continue to rise.

A number of States with subversive aims attempt to overtly or covertly use cyberspace to intervene in the political, economic and social affairs and systems of other States. Certain States have acquired cyber warfare capabilities and techniques; Malwares and cyber weapons have also been used by some States. As a result, there exists a great deal of potential for the eruption of cyber conflicts between States in the not too distant future.

To respond to these relevant concerns and challenges, some national measures are being taken. However, there is a dire need for a multilateral instrument to prevent such cyber conflict and address the security problems of cyberspace. Additionally, there is a need for an inclusive multilateral intergovernmental mechanism within the UN for sustained consideration, cooperation and coordination on cybersecurity related issues.

Accordingly, a serious substantive discussion is required to explore the ways and means of developing international norms, rules and principles for addressing cybersecurity issues. We should recall that the development of existing international law preceded the advent of cyberspace and cyber warfare. Therefore, many questions on how to apply existing international law on cyber activities must be clarified. This has to be done in an inclusive process with the participation of all States.

As a victim of cyber weapon, Iran rejects the status quo and strongly supports the establishment of international legal norms and rules concerning the prevention of the use of ICT and cyberspace for malicious purposes. Those who have an explicit policy of seeking dominance and superiority in cyberspace aspire to maintain the status quo. They reject any step forward towards developing international legal norms as it would limit their freedom in the application of their offensive cyber capabilities against other States.
The very State that, in collaboration with Israel, used Stuxnet against Iran’s critical infrastructure in 2010 has now tabled a draft resolution regarding responsible State behavior in cyberspace. This is a hypocritical move. That country wants to preserve the status quo and impede any inclusive, serious process within the UN to develop legal norms regarding the use of ICT. The sponsor of that resolution considers cyberspace as a war-fighting domain. It is also actively engaged in making cyber weapons and interfering in the political, social and economic systems of other States through cyberspace. Given such track records, why should developing countries trust its intention and the rationale behind that draft?

After several years spent examining this vital issue within the context of GGEs with limited members, it is time to conduct such discussions in an inclusive forum within the UN. This would allow all States to participate in the process of international norm-setting and rule-making, with respect to the security aspects of the use of ICT.

To that end, Iran welcomes and supports the proposal of the Russian Federation as contained in draft resolution L.27/Rev.1 on establishing an OEWG within the UN on cybersecurity and the use of ICT. Indeed, this is a step forward as OEWG is an inclusive forum open to participation of all countries. The adamant opposition to the establishment of an OEWG on cybersecurity is not comprehensible. It appears that they favor a closed and discriminatory process. Why then should developing countries be deprived from participation in the norm setting process on cybersecurity which affects their long term interests?

Mr. Chairman,

In consideration of the cybersecurity issues, the Islamic Republic of Iran underlines that the following elements, among others, should be taken into account:

- Right of all States to ICT research and development as well as to manufacturing, utilizing and transferring ICT products and services for peaceful purposes should be fully respected;

- Commitment of States, in their use of ICT, to observe the principles of the UN Charter, including respect for sovereign equality, the settlement of international disputes by peaceful means, the prohibition of the threat or use of force in any manner inconsistent with the purposes of the UN, respect for human rights and fundamental freedoms, and non-intervention and non-interference in the internal affairs of States;

- The need to remove the major impediments that developing countries face in accessing ICT and its related know-how, technologies and services;

- Establishment of specific mechanisms and measures for international cooperation and coordination.

Securing a conducive environment for the broadest possible use of ICT by all nations and preventing their use for illegal purposes is indeed an indispensable collective responsibility. Iran stands ready to contribute to the fulfilment of this noble objective.

I thank you, Mr. Chairman.