Sri Lanka Remarks
by Satya Rodrigo, Deputy Permanent Representative
First Session of the Open-ended Working Group on developments in the field of information and telecommunications in the context of international security
New York, 10th September 2019

Merci Monsieur le President,
Excellencies,
Distinguished Delegates,
Colleagues,
Ladies and Gentlemen,

May I take this opportunity to congratulate Ambassador Lauber on his election as Chair of the Open-ended Working Group on developments in the use of information and telecommunications in the context of international security. My delegation assures you of our full support and cooperation in your stewardship of this very important process.

Many date the World Wide Web to 1989. But I am not sure if many are aware of the first use of IoT 7 years before, in 1982, when a group of computer scientists in Carnegie Mellon University, tired of running back and forth to a coke machine-added some sensors and connected it to their local network, so they could log in and check how many Coke Bottles were left and how cold they were, without leaving their rooms. Today, we are connected to the web, in multiple ways. It is estimated that 50 Billion devices will be connected by 2020.

Across the globe, digital technologies have evolved into an impowering economic tool that has helped improve the quality of life of people and it has transformed the way that businesses, governments and people connect, engage and access information and services. Societies are now dependent on digital technologies and these are now considered a fundamental social infrastructure prerequisite for development. Many small businesses are using the internet, social media tools and devices to sell their goods and find a market. In more developed countries, many connect their smart phones to every aspect of their live.

With all this promise and potential, there is also peril. From the abuse and misuse of social media, hacks, bots, our data and information is vulnerable. Cybercrimes account for trillions of dollars of losses, with some figures for 2019 indicating around $ 2 Trillion Dollars. An IoT device can be hacked in the first 5 minutes it is connected to the internet.

In this backdrop, we welcome the convening of this Open-ended Working Group (OEWG), as an inclusive process where all Member States can work collectively to take forward our discussions and share experiences and best practices, to reach common understandings on the use of Information and Communication Technologies (ICT) and work on developing rules, norms and principles of responsible behavior of States as we seek to ensure an open, secure and safe ICT environment for our socio-economic development in the global landscape.

We are fortunate that there has been much work done by the Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security (GGE). Our collective work can be facilitated by the complementarity between the OEWG and the GGE. The GGE has produced substantive reports in their work with assessments and recommendations that provide a strong foundation for this Group to build on.

While these processes are member state driven, if we are to be truly effective in our work, there is a vital need to also engage other stakeholders such as the private sector, academia, think-tanks, the ICT industry and civil society.

This is particularly important to ensure that our discussion and work is current. Developments in the ICT world, often fast outpace our government documents and studies. Resources of ICT companies alone, exceed the GDP of most countries.

Greater collaboration between both States and other stakeholders in the private sphere, would also help bridge the digital gap, between many states that do not have the expertise or resources to have robust solutions for digital security. This cross dialogue is also very essential if we are to take serious steps to develop common understanding on issues related to security and use of ICTs, and on the

larger objective to have a common basis for Norms, Rules and Principles for State behavior in cyberspace and that of International Law. In this regard, the principles identified by the GGE report in 2015 on the application of international law to State use of ICTs are useful.

Sri Lanka, like most countries is aware that the economic prosperity and social wellbeing of the country is increasingly dependent on an open, secure and safe cyber network that links up with the outside world. The Government has been looking at these related issues of ICT very seriously and in November of last year, the Government launched the "National Information and Cybersecurity Strategy" to be implemented over a five year period from 2019 to 2023.

In addition the Government in the process of enacting a "Cyber Security Act" to protect cyberspace and essential services from cyber attacks, that will also provide for the establishment of a high level "Cyber Security Agency". A variety of different stakeholders in government, including the industry and private sector have been consulted in the preparation of the Act and the Final Draft is now open for public comments before it is finalized.

If I may close with another example from Sri Lanka, from one of our long term resident Science Fiction writers- Arthur C. Clarke. In the 4th and final book of his Space Odyssey series- "3001: The Final Odyssey" about the adventures of Frank Poole, the astronaut killed by the HAL 9000 computer. In the book, "3001" the future of mankind is saved by the infection of the monolith with a computer virus; but in turn is infected with a computer worm and to safeguard the future, is locked up in a deep vault below the surface of the moon.

While this is a more drastic measure, we would like to highlight the imperative need to work together creatively and with flexibility to find common ground and collaborate together as we forge ahead in the work before us.

Please be assured that we stand ready to help you Mr Chairman in your work ahead.

Thank you.