Statement by Ambassador Fu Cong

On Cyber Security

February 2016, Geneva

Mr. President,

The rapid progress of information and communication technologies starting from the end of the last century has greatly boosted the economic and social development of all nations, enriching and improving people's lives and producing revolutionary impact on growth and prosperity throughout the world. Economic globalization and information technology are converging their forces to shape our future, turning our world into a global village, shrinking physical distances between countries and transforming the international community into one of common destiny with intertwining interests. As the ITC continues to grow horizontally and vertically, it is spearheading a steady expansion of e-commerce and heralding the arrival of the fourth industrial revolution. Looking forward, ICT is set to inject new impetus to our quest for global prosperity.

While contributing to peace and development, ICT is also throwing up a host of new problems. Cyber security is presenting new challenges to global governance and international security, as we witness the rise of cyber terrorism and cyber crimes, along with a mounting risk of an arms race and conflicts in cyber space. This, together with an unbalanced management and distribution of Internet resources, is bringing about new uncertainties which would undermine the efforts of all countries to establish a secure cyber environment.

Such risks and threats have brought into sharp focus the absence of rules governing that environment. As a matter of fact, universal, accepted norms and rules are urgently needed. In this regards, there are several factors which are playing in our favour.

First and foremost, such moves will answer the calls of the international community. In recent years, changes are taking place with profound implications on the international security, with non-traditional threats gaining new prominence. Frequent reports of cyber space incidents have heightened people's awareness of its associated security problems. Risks caused by the absence of rules in the cyber space are becoming increasingly apparent, giving rise to widespread concerns and prompting calls for formulating such rules.

Secondly, there is already a solid basis in place in this area. Starting from the end of last century, efforts began to gather pace to bring governance to the Internet, while practical cooperation in areas including clamping down on cyber crimes are also gaining strength. The UN has convened several sessions of the group of governmental experts on information security and produced some positive outcomes. International fora such as WSIS, IGF and the Wuzhen Summits and other mechanisms are flourishing. All this has promoted a greater and deeper awareness of issues on cyber security and paved the way for an emerging consensus.

Thirdly, there is converging political will from the major countries. In 2011, China and Russia jointly tabled a draft Code of Conduct on Information Security to the General Assembly. Last year, US President Obama and Secretary of State John Kerry also made several appeals for formulating norms of responsible state behaviour in cyber space, and for the first time in 17 years, the US co-sponsored the GA resolution on information security. This was followed by a recent proposal made by Mr. Jim Himes and several US congressmen for negotiating a Geneva

Convention of Cyber Space.

One can therefore conclude that for all their differences on cyber space issues, more and more countries now agree on the urgent need of adopting a code of conduct in this field. Indeed, time has come for negotiating such an instrument on the basis of broad participation and inclusive consultations of the international community on an equal footing. As we see it, in formulating norms and rules for cyber space, we need to pay special attention to the following.

Firstly, we should insist on the peaceful nature of the cyber space. Cyber space has reached all aspects of human life, making itself as indispensable as air and water. Meanwhile, peace and security in cyber space are becoming increasingly vulnerable to multiple threats, including cyber crimes and hacking. Most worryingly, some countries are working hard on building up military capabilities in cyber space, including drawing up doctrines and plans on the use of cyber weapons. We all know that cyber attacks will easily spill out of the cyber space and paralyse infrastructures in finance, transport, public health and energy supply with devastating consequences. In fact, our growing reliance on cyber space has made the price of turning it into a new battleground unbearable for all nations. What is most needed at the moment is to reaffirm the applicability of such principles as the peaceful settlement of disputes, non-use or threat of force, as well as banning attacks on infrastructures and preventing an arms race in cyber space. To clearly spell out the applicability of international law including the UN Charter to cyber space will go a long way to helping maintain peace and stability in that environment. Meanwhile, due to the unique characteristics of the cyber space, we have to be cautious about whether and how the specific rules of international law could be applied in the cyber space. Particularly, in the absence of a common understanding on the nature and characters of the cyber weapons, it is inadvisable to conclude that laws governing armed conflicts are applicable in the cyber space.

Secondly, we should uphold the principle of state sovereignty in cyber space, as reaffirmed by the UN Group of Government Experts on Information Security in its consensus report. The purpose of asserting that principle is to avoid a legal vacuum and prevent cyber space from becoming a no-man's land. To put simply, sovereignty in cyber space calls for governance over its infrastructure and contents. Suppressing hacker attacks, child pornography and cyber terrorism are all examples of exercising such sovereignty. As a matter of fact, all countries are doing that in their own ways. What people are arguing about is not the principle of sovereignty over cyber space itself but the ways of exercising it. To tackle the problem, one needs to be mindful of the following aspects. Firstly, one should have a correct understanding of a free flow of information. Re-asserting sovereignty over cyber space is to ensure its security and order rather than to impede the free flow of information. In fact, flow of information has never been an absolute right. When security and public interests come under threat, no country has hesitated from taking measures to restrict the flow of information to certain extent. Secondly, one must insist on the principle of non-interference in each others' internal affairs. To use cyber space to create social chaos or to seek regime change in other countries will only undermine regional peace and stability and will serve no one's interests. Thirdly, we need to respect each other. Countries have different circumstances and different legal, religious, ethnic and cultural taboos. All countries should respect each other and refrain from imposing on others one's own views and opinions.

Thirdly, all cyber crimes, including hacking for whatever purposes, must be opposed. Internet crimes are characterised as being transnational, anonymous and hard to trace. The correct course of action to deal with the issue is to strengthen cooperation. Most countries are engaged in cooperation on this, and positive headways have been made. Yet numerous issues still exist. As the Internet technology and the magnitude of the Internet economy continue to grow, Internet crimes may increase at

a pace beyond our imagination. To confront the challenge from such crimes, we must succeed in the following areas. First, the international community should forge a consensus against all forms of attacks by hackers. No difference should be made between what is for political purposes and what is for economic purposes. Secondly, in the fight against cybercrimes, dialogue must also be strengthened and international norms universally acceptable must be developed to resolve issues including disputes over jurisdiction and legal differences. Third, the international governance mechanism must be improved to strengthen cooperation in law enforcement, information sharing and tracing etc.

My next point (fourth point) is that the international cooperation in the fight against cyber terrorism must be strengthened. The current trend indicates that terrorism is spreading across the world, becoming the biggest threat to international peace and security. The Internet has become a major platform for terrorist forces to recruit, finance, obtain arms and spread information of terror. The fight against cyber terrorism shall be a priority in the struggle against terrorism. For this, several relationships should be correctly handled. One is the relationship between security and the freedom of speech, which must be handled in a balanced manner. Free speech has never been absolute, and its extent should be adjusted in a dynamic balance with security interests. In times of peace, free speech can naturally enjoy more space. Yet in the special time of war on terror, it is rational to bring the online opinions under suitable management to contain the spread of extremist information of terror. The second is the relationship between governments. Terrorism is mankind’s common enemy and the international community must stand united and desist from double standards in confronting terrorism. The United Nations must play a bigger part in the fight against cyber terrorism. The third is to rationalise the relationship between governments and businesses. Governments and businesses have their respective unshirkable obligations. Governments should develop comprehensive legislations, clearly define the duties of government and business and provide systemic support for government-business coordination and cooperation

to help businesses avoid financial overburden and legal risks. Businesses in turn must fulfil their legal obligations and social responsibilities, take actions to close all grey areas that can be exploited by terrorist forces instead of turning a blind eye to terror information by citing neutrality of technology.

Fifthly, the system for Internet governance to be established should be one which is jointly built, jointly owned and jointly managed. Cyberspace has become the homestead of the whole mankind. Internet security is a common responsibility of the international community. In an era of globalisation and democratization of international relations, the international governance of cyberspace should abide by the principles of equal participation and democratic decision-making. Our efforts for now and the coming period should be focused on the following areas. The first is to turn around the inequality in the management and distribution of the infrastructure resources of the Internet, and continue to promote the globalisation of ICANN. This is an intrinsic requirement of the international governance and conducive to the reduction of systemic vulnerability caused by over concentration. The second is to build a reasonable and effective multi-stakeholder internet governance modality. The relationship between governments, businesses and other main stakeholders should be rationalised. A balance should be struck between rights and duties to ensure that all parties are fully motivated. The third is to enhance capacity building continuously. For many developing countries, development itself means security and holds the key to all security issues. We must adopt a global vision when looking at the digital divide, and work hard to support developing countries building their capacity for cyber security, to encourage joint investment, development and ownership and to promote the interconnectivity, so that all countries can benefit from the dividends of the digital economy.

Mr President,

China has all along been a strong defender of cyber security, and has advocated and contributed to the construction of the order in cyberspace. Since 2014, China has hosted in Wuzhen two annual sessions of the World Internet Conference, and made positive contribution for forging international consensus and promoting international cooperation. On 16 December 2015, President Xi Jinping made a personal appearance at the second World Internet Conference in Wuzhen, and made a comprehensive statement on the Chinese government's position on Internet security and governance. China has also supported and participated actively over the years in the UN's Group of Government Experts on information security, and made contribution to its work. China has high expectations for the upcoming session of the GGE on information security. It is our hope that this session will focus on the development of international norms, and achieve further progress in bridging differences and expanding consensus. Following this session of the GGE, the international community should start substantive discussions or even negotiations on the development of a set of international rules for cyberspace on the basis of inclusive participation. This can proceed either within the CD, or by setting up an open-ended working group under the framework of the UN. On this, we are open-minded.

I thank you, Mr President.