Work to Build a Peaceful, Secure and Equitable Information and Cyber Space

-- Speech by H.E. Ambassador Wang Qun at the First Committee of the 66th Session of the GA on Information and Cyberspace Security

New York, 19 October 2011

Mr. Chairman,

The 21st century is the century of information. Information and cyber technology represents advanced productivity, and its rapid development and wide application have given a strong impetus to economic and social development and the progress of human civilization. They are also transforming people’s lives and the mode of operation of human society in a profound way. Information and cyber network system has become a critical infrastructure for countries of the world.

Mr. Chairman,

While countries enjoy the great convenience offered by information and cyber networks, they also find themselves more vulnerable in terms of security because of the inter-connected nature of information and cyber networks and multiple sources of potential risks and threats existing in information and cyber space.

In recent years, in addition to the vulnerability of its own information and cyber networks per se, China has been subjected to increasing cyber attacks from abroad, which caused enormous losses to us. China has become one of the major victims of cyber attacks. This has made us realize that the inter-connectivity of information and cyber networks has contributed to making countries of the world “a community of common destiny” in which our security is inseparably linked together. Therefore, maintaining information and cyberspace security is maintaining the security of the whole international community, not that of just one country.

At present, the information and cyberspace security represents a major non-traditional security challenge confronting the international community. Effective response to this challenge has become an important element of international security and a major topic for multilateral diplomacy for arms control.
Mr. Chairman,

China believes that the international community should view this issue from the new perspective of “a community of common destiny” and work together towards a peaceful, secure and equitable information and cyber space. To this end, the following five principles should be followed:

Firstly, the principle of peace. In recent history, humanity experienced two world wars and at times came to the brink of nuclear war. In the information age, we must not go through the old sequence of “suffering the pains of wars first and learning to cherish peace afterwards”.

The international community should engage in active preventive diplomacy and promote the use of information and cyber technology in advancing economic and social development and people’s welfare and in maintaining international peace, stability and security.

Countries should commit themselves to non-use of information and cyber technology to engage in hostile activities to the detriment of international peace and security, and to non-proliferation of information and cyber weapons and related technologies. In the meantime, countries have the right and responsibility to protect, in accordance with their respective national laws and regulations, their information and cyber space and critical information infrastructure from threats, disturbance, attack and sabotage.

Countries should work to keep information and cyber space from becoming a new battlefield, prevent an arms race in information and cyber space, and settle disputes on this front peacefully through dialogue.

Secondly, the principle of sovereignty. Sovereign states are the main actor in effective international governance of information and cyber space. In this area, respect for sovereignty and territorial integrity enshrined in the UN Charter and other universal basic norms of international relations should also be respected.

Countries should act responsibly and constructively in information and cyber space, take a multi-pronged approach in strengthening effective management in an effort to build a comprehensive and integrated national management system that comprises, inter alia, sound legal norms, self-discipline by the industries, security safeguard and social education.

While ensuring the healthy development and effective utilization of information and cyber space, it is also necessary to keep information and cyber technology from being turned into another tool to interfere in internal affairs of other countries.

Thirdly, the principle of balance between freedom and security in information flow. While fully respecting the rights and freedom of all stakeholders in information and cyber space, countries should uphold rule of law so as to effectively keep order in information and cyber space. Rule of law should be the guiding beckon to activities in information and cyber space, too. Moreover, practicing power politics in cyberspace in the name of cyber freedom is untenable.
Fourthly, the principle of cooperation. Since information and cyber networks both interlink with each other and belong to different sovereign jurisdictions, no country is able to manage only its own information and cyberspace business, still less to ensure its information and cyber security by itself. Such a task requires all countries to work together and further strengthen international exchanges and cooperation.

Fifthly, the principle of equitable development. The developed countries should help the developing countries enhance capacity in information and cyber technology and narrow the digital divide to enable the latter to share the dividend brought by the development of information and cyber technology in this globalized world and this information age so as to realize genuinely equitable and universal development.

Mr. Chairman,

In this information age, information “highway” has reached almost all corners of our planet. It is worrisome, however, that in this virtual space where traffic is very heavy, there is, hitherto, no comprehensive “traffic rules”. As a result, “traffic accidents” in information and cyber space constantly occur with ever increasing damage and impact. Therefore, the development of international norms and rules guiding the activities in information and cyberspace has become an urgent task in maintaining information and cyberspace security of various countries.

As the most universal and authoritative international organization, the United Nation is the most appropriate forum for the formulation of such norms and rules. In September, China, together with Russia, Tajikistan and Uzbekistan, submitted to the current session of the GA “International Code of Conduct for Information Security” (A/66/359) with a view to launching an open and transparent process for developing, within the framework of the UN, international norms and rules for information and cyberspace security, which, we hope, will prompt countries to act responsibly and constructively in information and cyber space and address concerns of all parties in a balanced way. We wholeheartedly welcome comments and proposals from member states so as to make the Code better and further reflect concerns of all parties.

Mr. Chairman,

Information and cyber network has linked all of us closely together, making distance among countries a matter of microseconds in many cases. Let us work together to intensify our exchanges and cooperation in the field of information cyberspace security and reach an early consensus on the Code with the objective of building a peaceful, secure and equitable information and cyber space. Let us also work together to make information and cyber technology produce more development dividends and better serve world peace and well-being of mankind.

Thank you, Mr. Chairman.