

An International Code of Conduct for Information Security

**-- China's perspective on building a peaceful, secure,
open and cooperative cyberspace**

(10 February 2014, Geneva)

Dear Colleagues,

First, I would like to thank UNIDIR for organizing this event. I am very glad to participate and sit on this panel to talk about the code of conduct for information security, as proposed by China, Kazakhstan, Kyrgyzstan, Russia, Tajikistan and Uzbekistan in recent years. I hope that through my presentation today, you will have a better understanding of the code of conduct we have proposed and China's perspective on possible ways to enhance the security of cyberspace.

I. Why we need a code of conduct?

Information or cyber security has become an important issue on the international agenda and in international relations in recent years. It involves security and development interests of all countries. The rapid development of information and communication technologies (ICTs) brings enormous benefits to people all over the world. At the same time, the specific features of this virtual, transnational and sometimes anonymous cyberspace also bring about severe challenges to international security as well as economic and social development.

Nowadays, the information "highway" has reached almost every corner in the world. It is of great concern, however, that in this virtual space where traffic is very heavy, there is still 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 a set of universal and effective international norms and rules guiding the activities in information and cyber space has become an urgent task in maintaining information and cyberspace security.

To this end, China, Russia, Tajikistan and Uzbekistan jointly elaborated in the form of a potential General Assembly resolution on an international code of conduct for information security and called for international deliberations within the UN framework on such an international code, with the aim of achieving the earliest possible consensus on international norms and rules guiding the behavior of States in the information space. This document (A/66/359), in the form of a letter from the Permanent Representatives of China, Russia, Tajikistan and Uzbekistan to the UN addressed to the Secretary-General was circulated in the 66th Session of the General Assembly in 2011. We welcome the co-sponsoring of this document by Kazakhstan and Kyrgyzstan last year.

II. What is the Code of Conduct?

Highlights of the draft code of conduct

The draft code of conduct includes three parts: Preamble, Purpose and Scope, and Code of Conduct itself

- The Preamble part recognizes the need to prevent the potential use of information and communication technologies for purposes that are inconsistent with the objectives of maintaining international stability and security, as well as the need for enhanced coordination and cooperation among States. It also stresses the need for enhanced efforts to close the digital divide by facilitating the transfer of information technology and capacity-building to developing countries.
- The second part makes it clear that the purpose of the code is to identify the rights and responsibilities of States in information space, promote their constructive and responsible behaviours and enhance their cooperation in addressing the common threats and challenges, so as to ensure that information and communications technologies are to be solely used to benefit social and economic development, with the objective of maintaining international stability and security.
- The third part provides a list of possible pledges States will undertake on voluntary basis as code of conduct. It can roughly be divided into four categories:

Category I: Peace. States pledge not to use information and communications technologies to carry out hostile activities or acts of aggression, pose threats to international peace and security. To settle any dispute resulting from application of the code through peaceful means and to refrain from the threat or use of force.

Category II: Security. To ensure the supply chain of information and communications technology products and services, in order to prevent other States from using their resources, critical infrastructures, core technologies and other advantages to undermine the right of other countries.

Category III: Openness. To comply with the Charter of the UN and universally recognized norms governing international relations, that enshrine, inter alia, respect for the sovereignty, territorial integrity and political independence of all states, respect for human rights and fundamental freedoms and respect for the diversity of history, culture and social systems of all countries. To promote the establishment of a multilateral, transparent and democratic international Internet management system to ensure an equitable distribution of resources, facilitate access for all.

Category IV: Cooperation. To assist developing countries in their efforts to enhance capacity-building on information security and to close the digital divide. To bolster bilateral, regional and international cooperation in the field of information security and enhance coordination among relevant international organizations.

III. Next steps forward

Firstly, we put forward this draft code of conduct as a basis to facilitate relevant international discussions. In preparing this draft, China and other cosponsors tried their best to reflect international consensus in a comprehensive and balanced manner. We would prefer to regard this as an open and sustained process of building international consensus. The draft code of conduct is not the end product, but only the beginning of the process. We welcome further comments and proposals to improve the draft code of conduct and to promote international deliberations in this regard.

Secondly, we should make full use of the UN GGE on information security as an important platform to deepen mutual understanding and explore the international norms and rules. China welcomes the consensus report submitted by the GGE last year, which contains specific

recommendations developed by the group to address existing and potential threats from States or non-State actors through the use of ICTs. China supports UN to establish the GGE again this year to continue to study existing and potential threats in the sphere of information security and possible cooperative measures to address them. We hope that the new GGE will achieve new consensus and make new achievements built upon the outcomes of previous sessions of the GGE.

Thirdly, we should give full play to the leading role of the governments. As the main body to participate in the national administration and international cooperation, governments should play a major role in the area of information and cyber security. At the national level, governments should lead all stakeholders, including private sectors, in addressing the security challenges and strengthening the legislation and institutional capacity building. At the international level, States should carry out effective cooperation in preventing and combating cyber crimes and cyber terrorism, protection of critical information infrastructure, as well as the maintenance of stable and secure functioning of information and communication systems.

IV. Relation between the code of conduct and the CBM

As pointed out by the report of GGE, voluntary confidence-building measures can promote trust and assurance among States and help reduce the risk of conflict by increasing predictability and reducing misperception. States should consider the development of practical confidence-building measures to help increase transparency, predictability and cooperation.

However, we are of the view that the CBMs along will not be able to fully safeguard security of cyberspace. What is more important is the formulation of code of conduct to guide responsible behaviours of countries. This will not only increase mutual trust and predictability, but will also constitute solid foundation to set rules and regulations in the cyberspace for the benefit of mankind. We believe that this is the fundamental way to build trust and cooperation among States and enhance security of cyberspace.

Dear colleagues,

China attaches great importance to the issue of cyber security. Maintaining information and cyber security is an important part of China's national strategy and is high on the government agenda. Like many other countries, China faces serious security threats in information and cyber space. We are ready to join hands with the international community to build a peaceful, secure, open and cooperative cyberspace.

Thank you for your attention.