China's Submissions to the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security

Global governance in cyberspace is a significant task for the international community. The Open-ended Working Group (OEWG) is the first UN process open to all member states to discuss the formulation of international norms and rules in cyberspace, which is of great significance. We should pursue shared prosperity and shared responsibility, take a balanced approach to both development and security issues, work towards mutual benefits and win-win cooperation, and contribute to building a community with a shared future in cyberspace. We should build upon the work of previous UN Groups of Governmental Experts, and meanwhile, respond to the emerging cybersecurity challenges in the digital age and strive for new progress in promoting global governance in cyberspace.

I. Existing and Potential Threats

ICTs are evolving at a fast speed. Cyberspace and physical space are deeply interconnected, and states are more dependent on ICTs than ever before. The following challenges and threats deserve our attention:

-- Surging cyber attacks and cyber crimes, as well as cyber terrorism as a global menace, pose grave threats to security and stability of states.

-- Some states take cyberspace as a new battlefield, where they pursue a strategy of deterrence by forging military alliance and introducing rules of engagement, thus increasing the risk of conflicts in cyberspace and undermining international peace and security.

-- Cyber attacks on national critical ICT infrastructures threaten economic development, national security and people's livelihood.

-- Fake news and the leak and abuse of personal data aggravate trust

deficit.

-- Certain state politicizes technology and cybersecurity issues and willfully suppresses other states' ICT enterprises, jeopardizing global development and cooperation.

-- Internet of Things (IOT), artificial intelligence (AI), big data, cloud computing, blockchain, among other emerging ICTs bring about new development opportunities as well as security risks.

-- The current imbalanced distribution and unjust management system of critical Internet resources pose grave security threats to the smooth functioning of critical infrastructure.

-- The widening digital divide among countries and regions.

II. Norms, Rules and Principles for the Responsible Behavior of States

China supports and has been constructively participating in the efforts of developing universally accepted norms, rules and principles of responsible behavior of States within the framework of UN. With a view to making contribution to the UN discussion, the Shanghai Cooperation Organization Member States submitted to the General Assembly in 2011 "International Code of Conduct for Information Security" and a revised version in 2015. Taking into account the latest developments in ICT environment, the Group should work on the following issues:

i) States should pledge not to use ICTs and ICT networks to carry out activities which run counter to the task of maintaining international peace and security.

ii) State sovereignty in cyberspace

It is widely endorsed by the international community that the principle of sovereignty applies in cyberspace. The Group should enrich and elaborate

on the specification of the principle, thus laying solid foundation for the order in cyberspace.

-- States should exercise jurisdiction over the ICT infrastructure, resources as well as ICT-related activities within their territories.

-- States have the right to make ICT-related public policies consistent with national circumstances to manage their own ICT affairs and protect their citizens' legitimate interests in cyberspace.

-- States should refrain from using ICTs to interfere in internal affairs of other states and undermine their political, economic and social stability.

-- States should participate in the management and distribution of international Internet resources on equal footings.

iii) Critical infrastructure protection

Security of critical infrastructures bears on the economic development, social stability, public interests and national security of all states, which is the common concern of all parties. China proposes the following norms of states' behavior in this regard:

-- States have the rights and responsibilities regarding legal protection of their critical ICT infrastructures against damage resulting from threats, interference, attack and sabotage.

-- States should be committed to refraining from launching cyber attacks on the critical infrastructures of other states.

-- States should not exploit policy and technical advantages to undermine the security and integrity of critical infrastructures of other states.

-- States should increase exchanges on standards and best practices with regard to critical infrastructure protection and encourage enterprises to embark on such exchanges.

iv) Data security

With the development of digital globalization, states have an increasing demand for the collection, analysis, application and cross-border flow of data, adding more weight to the importance of security. China proposes norms as follows:

-- States should take a balanced approach with regard to technical advancement, business development and safeguarding national security and public interests.

-- States have the rights and responsibilities to ensure the security of personal information and important data relevant to their national security, public security, economic security and social stability.

-- States shall not conduct or support ICT-enabled espionage against other states, including mass surveillance and theft of important data and personal information.

-- States should pay equal attention to both development and security, and push for the lawful, orderly and free flow of data. States should facilitate exchanges of best practices and cooperation in this regard.

v) Supply chain security

Supply chain security is crucial for enhancing users' confidence and promoting digital economy. China proposes as follows:

-- States should not exploit their dominant position in ICTs, including dominance in resources, critical ICT infrastructures and core technologies, ICT goods and services to undermine other states' right to independent control of ICT goods and services as well as their security.

-- States should prohibit ICT goods and services providers from illegal obtainment of users' data, control and manipulation of users' devices and systems by installing backdoors in goods. States should also prohibit ICT goods and services providers from seeking illegitimate interests by taking advantage of users' dependence to their products, or forcing users to upgrade their systems or devices. States should request ICT goods and services providers to make a commitment that their cooperation partners

and users would be noticed in a timely manner if serious vulnerabilities are detected in their products.

-- States should be committed to upholding a fair, just and non-discriminatory business environment. States should not use national security as a pretext for restricting development and cooperation of ICTs and limiting the market access for ICT products and the export of high-tech products.

vi) Counter-terrorism

Terrorist groups' use of the Internet for promotion and incitement, recruitment, and plan and coordination of attacks is the major source of the current terrorist activities, and jeopardizes the security and stability of all states. The international community has a high degree of consensus on this. The Group should probe into discussions in following norms:

-- States should prohibit terrorist organizations from using the Internet to set up websites, online forums and blogs to conduct terrorist activities, including manufacturing, publication, storage, and broadcasting of terrorist audio and video documents, disseminating violent terrorist rhetoric and ideology, fund-raising, recruiting, inciting terrorist activities etc.

-- States should conduct intelligence exchanges and law-enforcement cooperation on countering terrorism. For instance, one state should store and collect relevant online data and evidence in a timely manner upon request from other states for cyber-related terrorism cases, provide assistance in investigation and deliver prompt response.

-- States should develop cooperative partnership with international organizations, enterprises and citizens in fighting cyber terrorism.

-- States should request Internet service providers to cut off the online dissemination channel of terrorist content by closing propaganda websites and accounts and deleting terrorist and violent extremist content.

vii) Norms, rules and principles regarding emerging technologies

To minimize security risks brought by emerging digital technologies such as IOT, AI, big data, cloud computing and blockchain, at the same time guaranteeing their contribution to economic development, further study is needed on the norms, rules and principles in these realms.

III. Application of International Law

The issue of which international laws are applicable to cyberspace and how they can apply deserves further study on a factual basis, especially in the following aspects:

-- The principles enshrined in the UN Charter, including sovereign equality, refraining from the use of force, settlement of disputes by peaceful means and non-intervention in the internal affairs of other states, apply in cyberspace. The application of these principles is the cornerstone of a just and equitable international order in cyberspace.

-- From the perspective of maintaining peace and preventing conflict, states should focus on the implementation of such principles as settlement of disputes by peaceful means and refraining from the use or threat of use of force. Willful use of force, punitive and confrontative countermeasures should be prevented.

-- The applicability of the law of armed conflicts and *jus ad bellum* needs to be handled with prudence. The lawfulness of cyber war should not be recognized under any circumstance. States should not turn cyberspace into a new battlefield.

-- New international legal instruments tailored to the attributes of ICTs and evolving realities should be developed. Priority can be given to developing an international convention on countering terrorism in cyberspace, and establishing an international legal instrument on combating cyber crimes within the framework of the UN.

IV.Confidence Building Measures

Purpose of introducing confidence building measures is to increase mutual trust, predictability and reduce misperception for the interest of ensuring cybersecurity.

States can conduct policy and technical exchanges, law-enforcement cooperation and information sharing on a voluntary basis. Confidence building measures should be taken progressively so as to enhance mutual trust and reduce misperception.

V.Capacity Building Measures

For bridging the digital gap and realizing global common and sustainable development, international cooperation and assistance on ICT security should be promoted through the following measures :

-- The developed countries are encouraged to enhance their technological and financial assistance to developing countries to improve their emergency response capabilities.

-- States and ICT enterprises with the capability to detect vulnerabilities or threats should publish those vulnerabilities or threats without delay.

-- States should work together to create a multilateral, democratic and transparent global Internet governance system. The organization charged with management of critical resources such as Root Servers should be truly independent from any state’s control to ensure the broad participation and joint decision-making of all states.

VII. Regular Institutional Dialogue

China welcomes the idea of establishing a permanent and sustainable international process within the framework of the UN to deal with the issue of cybersecurity, which is conducive to the long-lasting peace and stability in cyberspace.