# China's Positions on International Rules-making in Cyberspace

The phenomenal development of information technology revolution and digital economy is exerting far-reaching influence over social and economic development of States and human civilization. All parties should uphold multilateralism, ensure fairness and justice, put equal emphasis on security and development, step up dialogue and cooperation, promote global governance and international rules-making, and build a community of shared future in cyberspace.

I. Cyberspace and physical space are deeply interconnected, which brings us immense development opportunities as well as risks and challenges.

Some States take cyberspace as a new battlefield for military advantages, 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. Critical ICT infrastructure faces considerable vulnerability and potential risk. Cyber attacks and crimes surge, and cyber terrorism becomes a global menace. Fake news floods with massive leak and abuse of personal data. The current distribution and management system of critical Internet resources is imbalanced and unjust. The unbalanced development and widening digital divide among countries and regions are prominent. Certain States politicize technology and cybersecurity issues, willfully suppress other States' ICT enterprises and impose unfair and unjust barriers on global ICT supply chain and trade, jeopardizing global development and cooperation.

II. The international community should develop universally accepted norms, rules and principles within the framework of the UN, to jointly address the risks and challenges, and uphold peace, security and prosperity in cyberspace.

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. With a view to furthering international efforts, China submitted to the General Assembly in 2020 the "Global Initiative on Data Security". China believes

that the following norms, rules and principles should be observed:

i. States should foster a cyberspace featuring peace, security, openness, cooperation and order, and should not use ICTs to carry out activities inconsistent with the objectives of maintaining international peace and security.

ii. The principle of sovereignty applies in cyberspace. States should exercise jurisdiction over the ICT infrastructure, resources, data as well as ICT-related activities within their territories, and have the rights to protect their information systems and important data against damage resulting from threats, interference, attack and sabotage. States have the right to make ICT-related public policies, laws and regulations to protect legitimate interests of their citizens, enterprises and social organizations. States should refrain from using ICTs to interfere in intermal affairs of other States and undermine their political, economic and social stability, or to conduct activities that undermine other States' national security and public interests. States should participate in the management and distribution of international Internet resources on equal footings, and build a global Internet governance system of multilateralism, democracy and transparency.

iii. States should enhance critical ICT infrastructure protection. States should stand against ICT activities that impair other States' critical infrastructure, impair or steal important data of other States' critical infrastructure. States should increase exchanges on legislation, best practices and technologies with regard to critical ICT infrastructure protection, and promote international cooperation on personnel training, technological innovation, early warning and prevention, emergency response, standards and regulations, and information sharing.

iv. States should handle data security in a comprehensive, objective and evidence-based manner. States should foster an open, fair and non-discriminatory business environment, and maintain an open, secure and stable supply chain of global ICT products and services. States should take actions to prevent and put an end to activities that jeopardize personal information through the use of ICTs, and oppose mass surveillance against other States and unauthorized collection of personal information of other States with ICTs as a tool. States should encourage companies to abide by laws and regulations of the State where they operate, should not request domestic companies to store data generated and obtained overseas in their own territory, or obtain data located in other States through companies or individuals without other States' permission.

ICT products and services providers should abide by laws and regulations of the State where they operate, not install backdoors in their products and services to illegally obtain

users' data, control or manipulate users' systems and devices. ICT companies should not seek illegitimate interests by taking advantage of users' dependence on their products, nor force users to upgrade their systems and devices. Products providers should make a commitment to notifying their cooperation partners and users of serious vulnerabilities in their products in a timely fashion and offering remedies.

v. States should step up cooperation against cyber terrorism. 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, and develop cooperative partnership with international organizations, enterprises and citizens in countering 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.

III. The international community, with a view to maintaining international peace and security, should undertake discussions within the framework of the UN on how international law applies to the use of ICTs by States, taking into account the unique attributes of ICTs, and further develop common understandings on this issue.

The UN Charter and the principles enshrined in it, including sovereign equality, refraining from the use or threat of force, settlement of international 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 the peace, security and stability in cyberspace.

States should handle the applicability of the law of armed conflicts and jus ad bellum with prudence, and prevent escalation of conflicts or turning cyberspace into a new battlefield.

To maintain long-lasting peace and stability in cyberspace, new international legal instruments tailored to the attributes of ICTs and evolving realities should be developed based on broad participation of all States. Cyber terrorism imposes significant threat on national security and social stability of States, which could be considered as an important direction for new legal instruments.

IV. States can conduct policy and technical exchanges, law-enforcement cooperation and

information sharing on a voluntary basis to enhance mutual trust and reduce misperception and miscalculation.

For realizing fair, reasonable and universal access to the Internet, popularization of ICTs, equal sharing of digital dividends and global common and sustainable development, international cooperation and assistance on ICT security should be promoted. States should step up cooperation on emergency response capabilities. States should not conduct malicious cyber activities against the State which is seeking the assistance or a third State under the pretext of providing assistance.

V. China supports the establishment of an inclusive and sustainable process with broad participation of all States within the framework of the UN to deal with the issue of cybersecurity, and welcomes the 2021 report of the Open-ended Working Group on Developments in the Field of Information and Telecommunications. States should observe and implement previous international consensus, including norms, rules and principles for responsible State behavior, and formulate new international norms and rules on issues such as data security in compliance with the evolving situation and technological development. China is ready to work together with all parties to promote positive progress of the Open-Ended Working Group 2021-2025, and to build a community of shared future in cyberspace.