United Nations A/75/245

General Assembly

Distr.: General
21 September 2020

Original: English

General Assembly
Seventy-fifth session
Agenda items 15, 18, 98, 112 and 137

Culture of peace

Follow-up to and implementation of the outcomes of the International Conferences on Financing for Development

Developments in the field of information and telecommunications in the context of international security

Countering the use of information and communications technologies for criminal purposes

Seventy-fifth anniversary of the end of the Second World War

Letter dated 18 September 2020 from the Permanent Representative of China to the United Nations addressed to the Secretary-General

Upon instructions from my Government, I have the honour to transmit to you herewith the attached "Global Initiative on Data Security" proposed by China, which calls upon all States to put equal emphasis on development and security, and take a balanced approach to technological progress, economic development and protection of national security and public interests, to forge a community with a shared future in cyberspace featuring peace, security, openness, cooperation and order (see annex).

I should be grateful if you could have the present letter and its annex circulated as a document of the General Assembly, under agenda items 15, 18, 98, 112 and 137.

(*Signed*) **Zhang** Jun
Ambassador Extraordinary and Plenipotentiary
Permanent Representative of the People's Republic of China
to the United Nations

20-12340 (E) 290920

Annex to the letter dated 18 September 2020 from the Permanent Representative of China to the United Nations addressed to the Secretary-General

[Original: Chinese]

Global Initiative on Data Security

The phenomenal development of the information technology revolution and the digital economy is transforming the way of production and life, exerting far-reaching influence over the social and economic development of States, the global governance system and human civilization.

The explosive growth and aggregation of data, as a key element of digital technology, has played a crucial role in facilitating innovative development and reshaping people's lives, which has a bearing on security and the economic and social development of States.

In the context of closer global cooperation and new developments in the international division of labour, maintaining the supply chain security of ICT products and services has never become more important for boosting users' confidence, ensuring data security and promoting a digital economy.

We call upon all States to put equal emphasis on development and security, and take a balanced approach to technological progress, economic development and the protection of national security and public interests.

We reaffirm that States should foster an open, fair and non-discriminatory business environment for mutual benefit, win-win outcomes and common development. At the same time, States have the responsibility and right to ensure the security of important data and personal information, which has a bearing on their national security, public security, economic security and social stability.

We welcome Governments, international organizations, ICT companies, technology communities, civil organizations, individuals and all other actors to make concerted efforts to promote data security under the principle of extensive consultation, joint contribution and shared benefits.

We underscore that all parties should step up dialogue and cooperation on the basis of mutual respect and join hands to forge a community with a shared future in cyberspace featuring peace, security, openness, cooperation and order. To make this happen, we would like to suggest the following:

- States should handle data security in a comprehensive, objective and evidence-based manner, and maintain an open, secure and stable supply chain of global ICT products and services.
- States should stand against ICT activities that impair or steal important data of other States' critical infrastructure, or use the data to conduct activities that undermine other States' national security and public interests.
- 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 the 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. States should not request domestic companies to store data generated and obtained overseas in their own territory.

- States should respect the sovereignty, jurisdiction and governance of data of other States, and shall not obtain data located in other States through companies or individuals without other States' permission.
- Should States need to obtain overseas data out of law enforcement requirement such as combating crimes, they should do it through judicial assistance or other relevant multilateral and bilateral agreements. Any bilateral data access agreement between two States should not infringe upon the judicial sovereignty and data security of a third State.
- ICT product and service providers should not install back doors in their products and services to illegally obtain users' data or 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. Product 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.

We call upon all States to support this initiative and confirm the aforementioned commitments through bilateral, regional and international agreements. We also welcome global ICT companies to support this initiative.