



General Assembly

Distr.: General
7 January 2021

Original: English

Seventy-fifth session

Agenda items 98 and 112

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

Letter dated 22 December 2020 from the Permanent Representative of Uzbekistan to the United Nations addressed to the Secretary-General

I have the honour to convey a joint statement by the Heads of State of the Commonwealth of Independent States on cooperation in the field of ensuring international information security (see annex).

I would appreciate it if you could circulate the present letter and its annex as a document of the General Assembly under agenda items 98 and 112.

(Signed) Bakhtiyor **Ibragimov**
Permanent Representative



Annex to the letter dated 22 December 2020 from the Permanent Representative of Uzbekistan to the United Nations addressed to the Secretary-General

[Original: Russian]

Joint statement by the Heads of State of the States members of the Commonwealth of Independent States on cooperation in the field of ensuring international information security

The Heads of State of the States members of the Commonwealth of Independent States note the considerable progress made in the development of information and communications technologies and their significant impact on the daily lives of people around the world.

The Heads of State recognize that information and communications technologies have created significant potential to advance human capabilities and the full enjoyment of human rights and freedoms. They provide new tools for the effective functioning of society and the State, and contribute to the development of economies around the world.

At the same time, they are concerned that the use of modern information and communications technologies for destructive, politico-military and other purposes that threaten international peace, security and stability poses a direct threat to the State, its citizens and society as a whole.

In order to safeguard national and international interests, they advocate increasing the level of inter-State cooperation aimed at preventing and peacefully resolving conflicts that may arise from the misuse and destructive use of information and communications technologies.

They call upon the global community to take all necessary measures to prevent the use of information and communications technologies for interference in the internal affairs of sovereign States and for terrorist and other criminal purposes. They also emphasize the importance of strengthening the fight against disinformation and fake news through national legislation, as reflected, inter alia, in paragraph 29 of the United Nations General Assembly resolution entitled “Comprehensive and coordinated response to the coronavirus disease (COVID-19) pandemic”. In that regard, they advocate the further development of comprehensive cooperation and the prevention of conflicts in the information sphere.

They call on the global community to refrain from the militarization and misuse of information and communications technologies, and from the creation of new technologies specifically designed to damage the information resources, infrastructure and critical facilities of States.

They express concern at the increasing threats and challenges to the information security of States members of the Commonwealth of Independent States in the context of global crisis situations. A clear example of this has been the increase in deliberate and malicious attempts to hack global and national information infrastructure during the COVID-19 pandemic. In this connection, they advocate strengthening the exchange, at both the regional and international levels, of positive experiences and practices in countering threats to international information security.

Given the transboundary nature of information and communications technologies, they are convinced that measures taken at the national level to ensure international information security should be complemented by consolidated action at the bilateral,

regional and global levels. At the same time, they confirm their intention to cooperate in this area at all specialized international forums.

They stress the particular importance of activities carried out within the United Nations to elaborate rules, norms and principles for the responsible behaviour of States in cyberspace.

Reaffirming the importance of successful outcomes to the work of specialized forums on international information security, they welcome and note the timely launch under the aegis of the United Nations of the first negotiation mechanism on this topic – an open-ended working group in which all States can participate. They are convinced of the need to ensure the successive and continuous nature of negotiations on international information security at various forums under the auspices of the United Nations.

They emphasize the focus on practical cooperation in combating the misuse of information and communications technologies and, in this context, reaffirm the need for a comprehensive international convention on countering the use of information and communications technologies for criminal purposes under the aegis of the United Nations. In that regard, they welcome and support the decision of the United Nations General Assembly to establish an ad hoc open-ended intergovernmental expert committee to elaborate such an instrument.

They recognize the importance of fostering cooperation among the States members of the Commonwealth regarding the use and management of national segments of the Internet, including to ensure the equal rights of States to access the global network and participate in its management, and note the need to enhance the role of the International Telecommunication Union in this context.

They reaffirm the desire of States to continue to work together within the Commonwealth of Independent States to ensure information security on the basis of the previously adopted instruments to which they are parties, including for the protection of information resources and critical facilities from unauthorized use and external interference.
