

**Contribution of the Russian Federation
to the report of the UN Office for Disarmament Affairs
on national ICT security capacity-building programs and initiatives**

We are convinced that the UN should play a coordinating role in the global efforts in the field of capacity-building. The activities of the Open-ended Working Group in the field of strengthening ICT capacities of States should be as pragmatic and result-oriented as possible. Joint efforts will enable increased protection of the most vulnerable States – and thereby strengthen security in the global information space in general. The Group's activities should result in specific recommendations and proposals for assistance programs.

Russia pays special attention to the issue of capacity-building. This relates, first and foremost, to personnel training in the field of information security. Russian universities provide educational programs in the following areas of specialization: information and computer security, methods of detecting and countering network computer attacks in open information systems, methods and techniques of protecting information from unauthorized access, collection of open source data, countering crimes in the field of computer information, techniques for investigating ICT crimes and international cooperation in this field, computer forensics, countering telephone fraud, countering the use of ICTs and international postal services in drug trafficking and for theft of funds, identification and investigation of illegal transactions with digital assets, including cryptocurrencies and their use for financing terrorism. We accept applications from interested foreign countries.

As part of the implementation of bilateral agreements and cooperation programs signed with the competent authorities of foreign states, expert training programs, round tables, working meetings with foreign partners are held in order to exchange best practices on ensuring information security and countering ICT crime and information on relevant national legislation.

Russian competent agencies conduct scientific and practical seminars and conferences on the entire range of threats in information sphere. In 2023, a series of educational events on the prevention, disclosure and investigation of crimes with the

use of ICTs were held with CIS partners. We hold annual seminars held on terminology in the field of security of and in the use of ICTs, as well as on countering the use of ICTs for criminal purposes within the ASEAN Regional Forum. We have also organized online workshops on sustainable and secure development of the Internet and on digital forensics, as well as a training course on investigating crimes in the field of embezzlement of funds using ICTs at the Conference on Interaction and Confidence-Building Measures in Asia. Similar events are envisaged for partners from Asia, Africa, Latin America and the Middle East.

Russia annually hosts the International Forum “Partnership of state authorities, civil society and the business community in ensuring international information security”, as well as the International Conference on Information Security “KubanCSC” – discussion platforms on international information security with the participation of states and non-state actors. These events encompass seminars for exchange of best practices in such areas as international cooperation in the field of information security, the applicability of international law to the use of ICTs, digital forensics, as well as measures to counter the use of ICTs for criminal purposes and public-private partnership in the field of information security.

We see merit in engaging other interested parties, in particular, businesses, academia and non-governmental organizations, in capacity-building efforts. It is clear that assistance from non-state actors should be carried out on a strictly non-discriminatory and impartial basis. Capacity-building should not be used to lobby the interests of individual companies / groups of companies, as well as to “enslave” less developed countries.