



Position of Russian Federation for the purpose of the conference held by Forum for 21st Century on 29 November 2011 reflected in the second draft of the negotiation paper, regarding the global security issues.

Russian Federation welcomes the progress in acknowledging the global threats present in cyberspace, the essential need of international cooperation in preventing and fighting cybercrime as well as lack of legal framework in this field. At the same time Russian Federation honestly believes that further negotiations and good will of participating states in understanding political, historical and cultural specificities will lead to commonly acceptable results which will be later implemented in national law systems to promote international security and stability and will not act contrarily. Therefore a sovereign-based international cyber agreement respecting fundamental human rights, fundamental principles and norms of international law, promoting and not threatening economical, social and national development and security must be proposed to be acceptable in all means. Russian Federation is ready to actively participate in final version of such an agreement and thus presents its position to second draft notes and proposals and encloses its own proposals to establish just and safe global cyberspace.

🛡️ Global cybersecurity is an integral part of global security and international cooperation is a key element to secure it. The main threats to international peace and security are the use of informational and communicational systems and technologies to engage in hostile activities threatening political, economic and social system of other government, illegal acquiring and use of information causing economic loss, jeopardizing safety and welfare of nation, governmental or non-governmental organizations or individuals, spread of information for terrorist, extremist and other criminal purposes and difficulty to identify sources of these actions that should be internationally define as illegal. Informational and communicational systems and technologies seen as the total amount of methods, production processes, and programming and technical elements, integrated with the goal of forming, converting, transferring, using, and storing information. At the same time agreeing with the definition of Cyberspace proposed by the Forum for 21st century.

🛡️ To be able to effectively fight abovementioned activities legislative or other steps are necessary to be taken to empower the law enforcement authorities of the participating states to criminalize, prevent, avert, investigate and persecute hostile activities. Each state has the right to make sovereign norms and govern its cyberspace according to its national laws without any foreign interference in its sovereignty. Simultaneously each state has the responsibility for its own cyberspace and must ensure that no hostile activities will be conducted against other states, its people, organizations or institutions. All states are obliged to take action in the case of



cyberattack from its cyberspace aiming other country, its people, organizations or institutions and liquidate consequences of crime.

- ❖ In compatibility with the right of each individual to seek, receive, and distribute information and ideas but to protect the national and social security of each state, as well as to prevent the wrongful use of informational and communicational systems, limits in anonymity of internet users should be set. This limits embodied in making anonymous domain registration illegal and further legislative or other steps are necessary to be taken to empower the law enforcement authorities of the participating states to legitimize and persecute internet and intranet users involved in sharing internationally illegal content. Russian Federation sees illegal content as follows: all information inciting terroristic, xenophobic and extremist activities and endangering sovereignty of states. Unless violating these principles there is need for other limitations in exercising human rights and freedom.
- ❖ Russian Federation agrees on creation of Basic Cyberspace Principles document as far as it does not violate its sovereignty in execution of all powers within its territory without any foreign interference.
- ❖ All the activities within the information infrastructure of one state, citizen, or corporation under the jurisdiction of that state when the effects of those actions are only felt by citizens and corporations under the jurisdiction of that state and no other state shall not be subject of international discussion or any other international activity.
- ❖ To create safe global cyberspace Russian Federation propose creation of international body with representation of all countries interested in maintaining security and prosperity. The body shall work as information center, collecting relevant information, sharing best practices and technologies in fight with cybercrime and cyberterrorism, developing new technologies in cooperation with private sector, exchanging information on possible attacks, helping to detect and localize hostile activities, identify terrorist organizations, monitoring the content of websites and sharing information about ongoing investigations. A database of terroristic and extremist groups that present a threat for national and social security shall be elaborated and kept up to date to be able to avert such activities within the frame of proposed body.
- ❖ Russian Federation stresses the necessity to increase the awareness of cybersecurity and cyberterrorism in developing countries and provide assistance in developing their cyberdefense in order to make global cybersecurity global. Accordingly proposed international body shall serve also for professional trainings for experts from developing countries.
- ❖ Russian Federation considers establishment of CYBERPOL unnecessary as reported criminal activities will be immediately, after report from victim of a cyberattack and location of the source with help from proposed international body, investigated and sovereign state will be obliged to take all necessary measures.




The Model Conference Global Security Issues

Faculty of International Relations, University of Economics in Bratislava



Modelová konferencia Bezpečnostná sekcia

Fakulta medzinárodných vzťahov, Ekonomická univerzita v Bratislave

-  Each state has an inalienable right to self-defense against cyberattack and right to use appropriate retaliatory measures if the source of the cyberattack can be reliably located. In no means is military attack an appropriate retaliatory measure to cyberattack. All states have to work together to develop technologies and exchange valuable information to prevent cyberattacks and cyberterrorism in peaceful way and in accordance with international law. Respecting fundamental principles and norms of international law and keeping in mind global peace all states must abstain from use of force or of threat of use of force. Intervention in sovereignty is unacceptable. If the cyberattack is to be defined as an act of aggression in the means of international law, Russian Federation will no longer participate in negotiations.