PIR CENTER
The Russian Center for Policy Studies

PLOUGHSHARES FUND

Meeting of the SuPR (Sustainable Partnership with Russia) Group

December 6-7, 2011

Washington DC

International Information Security and Global Internet Governance in US-Russian Relations: Expert's View

A Policy Memo

Michael YAKUSHEV

Observer

Introduction

Internet became one of the major factors not only in socio-economic development of selected countries, but also in international relations, as well as in bi-lateral and multi-lateral cooperation. Recent (2011) initiatives of Obama's administration (*International Strategy for Cyberspace*) and joint proposals of Russia and China (*Concept of the Code of Conduct of the States in Cyberspace*) demonstrate growing interest to the cyberspace security issues. Meanwhile there is also a common understanding that any initiatives in cyberspace regulation cannot be efficient without 'multi-stakeholders' approach (with equal opportunities for participation of states, business companies and civil society).

Both American and Russian law-enforcement agencies are active in the attempts to prevent cybercrimes by co-ordinated bi-lateral efforts. It can be a good contribution to the improvement of our cooperation on the government level, as well to make such cooperation more efficient and trustworthy.

However, there is a number of open issues to be defined, fixed and converted from threats and uncertainties to opportunities and success.

Possible topics for discussions

Main topics for US-Russian bilateral discussions on International Information Security and Global Internet Governance (relevant for sustainable development and strengthening international peace):

(A) Multilateral and bilateral framework for International Information Security, based on international legal instruments;

(B) Prevention of cyber-crimes, cyber-terrorism, cyber-wars: common understanding, uniform terminology, acceptable solutions;

(C) “Multi-stakeholders” principle in the Global Internet Governance: practical implementation;

(D) Issues of common interest (in Internet technologies) to improve mutual trust and bi-lateral cooperation.

Institutional framework for cooperation

Framework for International Information Security should be based on a solid fundament of multi-lateral and bi-lateral agreements and conventions. The U.S.A. and Russia demonstrate an example of efficient bi-lateral cooperation between their law-enforcement institutions, what can be finalized in a binding bi-lateral agreement on cyberspace security.

Open issues:

(a) Is the current stage of the bi-lateral relationship (cooperation) really efficient and trustworthy?

(b) Why Russia disagrees with the Budapest Convention on Cybercrime? Is the issue with its Art.32B the only “show-stopper”?

(c) Why the U.S.A. are not interested in discussing Russian (+ Chinese) proposals in the UN on prevention of cybercrime?

(d) The role of international institutions (United Nations, Council of Europe, …) in strengthening sustainable development and international peace in cyberspace.

First steps: subjects of the common interests and pressure from the common threats

Prevention of cybercrime, countering terrorism in cyberspace, non-proliferation of and control on emerging “cyber-warfare” requires certain joint actions by the most advanced technological powers like United States and Russia.

Open issues:

(a) How the cooperation against cybercrime can be efficient without multilateral institutional framework (i.e. Russian Federation outside Budapest Convention)?

(b) Is there is a common understanding what “cybercrimes” are? In what legislative acts (and/or international agreements) such understanding can be considered as a ground for harmonization of the “cybercrime” laws? What are the positive cases, success stories etc.?

(c) What common principles of countering terrorism in cyberspace can be applied in practice? Does the threat of cyber-terrorism have equal meaning

for both counterparts? To what extent the measures against cyber-terrorism can undermine the widely-accepted standards of human rights and freedoms?

(d) Can the "cyber-wars" be a realistic potential development of the international relations? If yes – what can be done jointly to prevent it? If not – why it is so frequently mentioned? How the U.S.A. and Russia can work together on this issue?

(e) A practical proposal – what can be done to develop the uniform terminology for international information security (English/Russian/Chinese/etc. equivalents)?

Multi-stakeholders approach to the Global Internet Governance

"Multi-stakeholders" principle became an imperative in the Global Internet Governance (such governance requires joint efforts of the three stakeholders – governments, business companies, and civil society, in their respective roles).

Open issues:

(a) What roles should the governments of the U.S.A. and the Russian Federation implement on the global level to guarantee the development of the Internet and the universal access to the relevant technologies?

(b) What priorities can be defined for the next stages of the global dialogue on internet governance?

(c) Is the U.S.Government ready for the next steps of the internationalization of the Internet Governance? What can be the main trends for such internationalization?

Internet technologies for mutual trust and efficient cooperation

Internet technologies can become a useful tool for the improvement of mutual trust and the diversification of the bi-lateral cooperation between our two countries. We can already find a number of areas, where the interaction between our government agencies and private companies can have immediate positive practical consequences.

Possible areas of discussion:

(a) 'Digital Diplomacy',

(b) Global Identity Initiative,

(c) Global Infrastructure of On-Line Payments,

(d) Intellectual Property on the Internet,

(e) Protection of Critical Infrastructure,

(f) Anything else?

Policy Recommendations

***For the U.S. Government*:** Analyze Russian proposals on cyberspace regulation trying to define issues of common interest, rather than pointing out differences, motivated by internal political reasons; start a bi-lateral discussions with the Russian counter-parts on the internationalization of the global Internet governance.

***For the Russian Government*:** Drop the demand for replacing Budapest Convention with a kind of 'Universal Document' without clear explanation why it cannot be acceptable and whether Article 32B is the only reason for that. The idea to insist on 'alternative' conventions raises only unnecessary confrontation.

***For both Governments*:** Examine the possibility and forms of inclusion of the national businesses and NGO's in discussions on international cyberspace security and Internet Governance, to make bi-lateral dialogue more efficient and comprehensive; start analyzing cross-border (trans-national) issues of the development of the Internet, including protection of critical infrastructure