Department on New Challenges and Threats

Cooperation against Cybercrime

Chernukhin Ernest
First Secretary – MFA Russia
Octopus Conference
Strasbourg, France, 6-8 June 2012

New general trends in the cybercrime market in 2011

- Targeted attacks on the financial sector
- Increase in online banking fraud incidents
- Surge in the number and complexity of DDoS attacks

What are the new high-tech forms of committing cybercrime?

- **"Phishing"**
- **"Pharming"**
- **"Carding"**
- **"Botnet attacks"**
- **Digital piracy**
- **Malicious spreading of viruses**
- **Attacks of criminal groups on critical information infrastructure**
- **Hacking**
- **and many others**

Main indicators of the cybercrime market in 2011

- Strong growth this past year, reflected in the number of crimes and the volume of profits earned by the hackers
- Professionalization of cybercrime, expansion of provided services, and interest from traditional organized crime groups, leading to an increase in damages from hacker activities
- No clearly defined global geographical centers with a high concentration of cybercriminals, they can carry out their attacks from anywhere in the world

Pending issues

- Fix the fundamental principle of the protection of the state sovereignty (for example based on the article 4, pp. 1 and 2 of the UNCAC)
- confirm the principle “aut dedere aut judicare” with a view to bring an alleged offender to justice
- confirm the rule “excluding fully impunity of a person, who has committed an illegal act”
- Stress the importance of state-business partnership by elaborating the codes of conduct for private sector

Pending issues

- Transboder access
- National Jurisdiction

Pending issues

- Apply innovative mechanisms – "24/7 Network" – to respond effectively and more flexible to the new dynamic challenges of cyberthreat
- Asset recovery
- Cyberterrorism

What does the International Information Security (IIS) mean?

IIS based on the nature of the inseparable «triad» of threats:

- ❑ Politico-military
- ❑ Terrorist
- ❑ Criminal

Russian strategy to fight Cybercrime

- Based on the comprehensive and balanced approach
- Necessity to codify global cyberspace
- Start working out the universal glossary or terminology on the IIS issues for further elaboration of the UN regulatory documents in this area and generally recognized international norms and criteria for fighting cyberthreats

Russian Initiatives

- CIS Agreement on cooperation to combat information computer crimes was signed in 2001 (July, Minsk)
- In 2009 for the first time in international practice it was signed an Agreement among the Governments of the SCO Member States on Cooperation in the Field of Ensuring International Informational Security
- In 2010 the Russian Federation and Brazil signed a bilateral agreement on cooperation in the field of international security for information and communication

Russian Initiatives

- Initiated in 2010 within the framework of the UN Commission on Crime Prevention and Criminal Justice Resolution 19/3 «Strengthening public-private partnerships to counter crime in all its forms and manifestations»
- Prepared the draft "Rules of conduct" in the sphere of international security disseminated as an official document of the 66-th session of the UN General Assembly
- Offered the concept of Convention on ensuring international security submitted at the 2nd International Meeting of High-Ranking Officials Responsible for Security Matters in Yekaterinburg (2011)

Russian Initiatives

- Strongly supports and shares the idea (reflected in the Declaration of the 12-th UN Congress of CPCJ) of drafting the universal Convention on cooperation in combating information/cyber crime under the aegis of the UN

Solution?

To elaborate a universal Convention on cooperation in combating information crime under the aegis of the UN

Thank you