Department on New Challenges and Threats

Cybercrime:
New Threat and Global Response

Chernukhin Ernest
First Secretary – MFA Russia
Expert Group on Cybercrime
Vienna, 17-21 January 2011
What are the recent developments?
(Documents)


12 United Nations Congress on Crime Prevention and Criminal Justice Resolution on Cybercrime (Brazil, 12-19 April 2010)

What are the recent developments?

(Documents)

International Narcotics Control Board (INCB) Recommendations on Internet misuse in illegal drug trafficking (Vienna, 26 November 2008)

International Telecommunication Union Agenda on Global Cybersecurity (Geneva, 16 November 2007)

Draft International Telecommunication Union Toolkit for Cybercrime legislation (Geneva, 2007)
What are the recent developments?
(Events)


12 United Nations Congress on Crime Prevention and Criminal Justice (Brazil, 12-19 April 2010)

The Council of Europe “Octopus Interface” Conference on “Cooperation against Cybercrime” (Strasbourg, 23-26 March 2010)

The OSCE expert workshop on Cybersecurity (Vienna, 17-18 March 2009)
What are the challenges of cybercrime?

- **Uncertainty of extent** (absence of reliable information about the extent of the problem and financial losses, as well as about arrests, prosecutions and convictions)

- **Transnational dimension** (difficulties for investigating)

- **Differences in national legal approaches** (preventing safe havens for criminals – a key aspect of preventing cybercrime)

- **Organized crime** (use of IT by traditional organized criminal groups and organized crime groups focusing on committing cybercrime)
What is the response to cybercrime?

- **Legislation**
  Due to limited reach of existing regional legal instruments there is necessity at the global level to harmonize legislation on cybercrime

- **Law enforcement**
  Depends on the availability of investigation tools like forensic software, management software or databases

- **Capacity-building**
  Cybercrime is an issue not only for developed countries, but also for developing countries

- **Training**
  Important to provide training to law enforcement officers, prosecutors and judges
What are the new high-tech forms of committing cybercrime?

- “Phishing”
- “Botnet attacks”
- Digital piracy
- Malicious spreading of viruses
- Attacks of criminal groups on critical information infrastructure
- Hacking
DDoS-attack scheme on Internet-server
internet
Use of computer networks by cybercriminals and cyberterrorists

Computer as a **target**

Computer as a **tool**
Why do terrorists turn to cyberattacks?

- To instill fear and shape public opinion with only small teams and minimal funds.
- To be far away, making borders and other physical barriers irrelevant.
- To cloak their true identities and locations, choosing to remain anonymous or pretending to be someone else.
- To amplify the effect of other attacks.
What Are Their Aims?

To spread havoc and cause enough harm to generate fear

To inflict death to a large scale

To cause mass destruction

To compel a government or an international organisation to do or to abstain from doing any act
CYBERTERORISM

- intentional use or threat of use of electronic information systems for the perpetration of terrorist acts inspired by certain motives (e.g., political, ideological or religious) with the aim to cause death or serious bodily injury, serious material damage, create a state of fear, compel a government or an international organization to do or to abstain from doing any act.
How Do They Achieve Their Aims?

Remotely disrupt the information technology underlying the Internet, government computer networks, critical civilian systems such as financial networks or mass media; or telephone switching equipment.

Use computer networks to take over machines that control traffic lights, power plants, or dams in order to wreak havoc.

Destroy the banks files by using anything from logic bombs to electromagnetic pulses and high-emission radio frequency guns.

Block emergency communications or cutting off electricity or water.
How Do They Achieve Their Aims?

- Remotely hijack control systems, with potentially dire consequences: breaching dams, colliding airplanes
- Hack into a hospital computer system and changing someone's medicine prescription to a lethal dosage
- Identify and recruit potential members of terrorist groups, collect and transfer funds, organize terrorist acts, as well as to incite terrorist actions, including through the use of propaganda; shutting down the power grid
What Will We Have in The Nearest Future?

Next generation of terrorists

More powerful and easy-to-use hacking tools at their disposal

Greater potential for cyberterrorism than the terrorists of today

Greater level of knowledge and skill relating to hacking
What Sectors of Critical Infrastructure Are Potentially Vulnerable to Cyberterrorist Attacks?

- Energy
- Information, communication technologies, ICT
- Water
- Food
- Health
- Financial
- Public and legal order and safety
- Civil administration
- Transport
- Space and research
- Chemical and nuclear industry
What legal basis do we have today?

Council of Europe Convention on Cybercrime
most important international legal instrument aimed at combating crime against computer security

Council of Europe Convention on Cybercrime
one of the first attempts to codify the rules for combating cybercrime, which is an especially dangerous phenomenon owing to its scale and consequences for national and international security
Is Convention enough to respond effectively to the new dynamic challenges in the computer sphere?

NO
- The notions of cybercrime and cyberterrorism have not been codified yet, and its components, in their entirety, have not been criminalized at the international level

- There is no definition of terrorist intentions, without which criminal sanctions would hardly commensurate with the terrorist threat of this criminal act

- Convention on Cybercrime does not provide any systematic response to the new trends of cybercrime

- Convention on Cybercrime does not provide any systematic response to the new challenge of cyberterrorism
- Convention on Cybercrime does not incorporate provisions excluding fully impunity of a person, who has committed an illegal act

- Responses to the threat of cyberterrorism could not be found through the combined application of the Council of Europe conventions on Cybercrime (2001) and on the Prevention of Terrorism (2005)
What Can We Suggest to Fill This Gap?

First, to encourage the international community to establish a comprehensive international legal instrument against the use of cyberspace by terrorists, including through closing everywhere the moving web-sites of international terrorist groups, criminalize cyberterrorism.

Second, to work with other countries, international groups, private sector to develop comprehensive and global plans for addressing the complex and challenging legal issues raised by unlawful conduct in the cyberspace.
What could be the possible structure of the UN Convention on cybercrime?

- Preamble
- I. General provisions
- II. Preventive measures on cybercrime
- III. Criminalization, incl. establishing of jurisdiction and prosecution
- IV. Law enforcement
- V. International cooperation
- VI. Technical assistance and information exchange
- VII. Mechanisms for implementation
What is the purpose of the UN Convention on Cybercrime?

• Promote and strengthen measures to prevent and combat cybercrime more efficiently and effectively

• Promote, facilitate and support international cooperation and technical assistance in the providing of an adequate response to all criminal challenges in the computer sphere
What could be the scope of application of the UN Convention on Cybercrime?

- This Convention shall apply, to the prevention, investigation and prosecution of:
  - criminal attempt on the computer systems and databases; and
  - using the computer systems or databases with the intent to commit criminal offence, incl. covering such offences established in accordance with the UN counter terrorism and drug Conventions, as well as UNCATOC.
Obligatory incorporated provisions

- 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
Obligatory incorporated provisions

• Apply innovative mechanisms – “24/7 Network” – to respond effectively and more flexible to the new dynamic challenges of cyberthreat
Pending issues

• Asset recovery
• Cyberterrorism
• Using the provisions of the Convention on cybercrime of COE (for example Chapters I and II)
Thank you