Web site: www.coe.int/economiccrime

Strasbourg, 21 March 2006

T-CY (2006) 12
English only

THE CYBERCRIME CONVENTION COMMITTEE (T-CY)

CYBERTERRORISM

Information submitted by the Delegation of the Russian Federation

Cyberterrorism

- The Russian Federation highly estimated the Council of Europe Convention on Cybercrime of 2001. We associate ourselves with those who think that the Convention is not a dead letter, it's a living mechanism.
- We witness that the Convention represents 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 as well as its dynamics.
- However we think that the Convention could hardly respond effectively and adequately to the extremely dangerous challenges of the cyberterrorism.
- For the time being the international law, in particular Convention on Cybercrime does not provide any systematic response to the new challenge of cyberterrorism.
- The notion of cyberterrorism has not been codified yet, and its components, in their entirety, have not been criminalized at the international level. It blocks the elaboration of a coordinated international approach to countering cyberterrorism.
- There is no definition of terrorist intentions, without which criminal sanctions would hardly commensurate with the terrorist threat of this criminal act. Article 2 of the Convention (p. 8) "Illegal access" contains the only definition of "dishonest intent", but it's not enough.
- The systemic antiterrorist approach provides qualitatively new forms of cooperation, including for the prosecution of cyberterrorists. Convention on

Cybercrime does not incorporate, for instance, provisions excluding fully impunity of a person, who has committed an illegal act. However, this is against the basic principle of the fundamental antiterrorist conventions, including those adopted within the Council of Europe, which envisage the rule of *"aut dedere aut judicare"* with a view to bring an alleged offender to justice. This mechanism prescribed in para 6, Art. 24 (p. 18) of the Convention on Cybercrime in fact has a limited scope.

- It concerns as well cases of denial to extradite with a reference to a political character of this type of terrorist offences. It is worth reminding that for the purposes of criminal prosecution, antiterrorist treaties, including those of the Council of Europe, traditionally do not regard terrorist offences as ones of a political character. Unfortunately, the Council of Europe Convention on Cybercrime does not include this provision. Moreover, the Convention does not include political exception clause in Article 29 "Expedited preservation of stored computer data" and Article 30 "Expedited disclosure of preserved traffic data". In our opinion it could be detrimental to effective fight against terrorist manifestations in cyberspace.

- Arguments such as those that responses to the threat of cyberterrorism could be found through the combined application of the Council of Europe conventions on Cybercrime (2001) and on the Prevention of Terrorism (2005) can hardly be justified. Those treaties advocate not only different legal approaches (including criminal prosecution); they, rather, may also differ as to the range of their Parties.

- We are in favor of establishing a common international legal "denominator" against the use of cyberspace by terrorists, including through closing everywhere the moving web-sites of international terrorist groups. It would be advisable to develop a single document to avoid duplication as well as the risk

of gaps and inconsistencies connected with the regulation of certain aspects of this issue in various international instruments.

- We do not in any way prejudge the issue of the development of a new international legal instrument in this area. It is for the States to give a final answer to this question.
- We fully share the approach prescribed in the reply of the Committee of Ministers to this Recommendation 1706 (2005) taken by the PACE (CM/AS (2006) Rec1706 final 20 January 2006): "…the notion of cyberterrorism as such merits further consideration. In any event, procedural means for criminal prosecution of such crimes should be in line with the international antiterrorist regime set up, inter alia, by the Council of Europe. The Bureau of the CDPC and CODEXTER have agreed to explore this issue further".
- We support the idea of working out an additional protocol to the Convention on Cybercrime or any other international instrument. There are already movements towards this objective in other regions, for instance, in ASEAN region. The participants of the 2nd ASEAN Regional Forum on Cyberterrorism held in Cebu City, Philippines last October reached an agreement to work towards establishment of a regional legal framework pertaining to cyberterrorism.
- We are convinced that creation of a necessary set of international instruments would provide an important step towards implementation of the UN Security Council antiterrorist resolutions, including 1373 (2001), 1566 (2004), and 1624 (2005), aimed at depriving terrorists of material and ideological support, as well as effectively suppressing incitement to terrorism, and its apologie in general.