Web site: www.coe.int/cybercrime

Strasbourg, 12 March 2008

T-CY (2008) INF 02 E

THE CYBERCRIME CONVENTION COMMITTEE (T-CY)

Information Document concerning the Opinion of the Committee of Experts on Terrorism (CODEXTER) on cyberterrorism and use of Internet for terrorist purposes

Secretariat Memorandum
prepared by
the Directorate General of Human Rights and Legal Affairs (DG-HL)

Decision adopted by the Committee of Ministers at their 1019th meeting, 27-28 February 2008

Item 10.2 Committee of Experts on Terrorism (CODEXTER)

b. Opinion of CODEXTER on cyberterrorism and use of the Internet for terrorist purposes

The Deputies

1. took note of the opinion of the Committee of Experts on Terrorism (CODEXTER) on cyberterrorism and use of the Internet for terrorist purposes, as it appears in document CM(2007)177, Appendix 2, and decided to transmit it to the European Committee on Crime Problems (CDPC) and to the Cybercrime Convention Committee (T-CY) for information.

Opinion of the Committee of Experts on Terrorism (CODEXTER)
for the attention of the Committee of Ministers
on cyberterrorism and use of Internet for terrorist purposes

On 11 July 2005, the Committee of Ministers communicated Parliamentary Assembly Recommendation 1706 (2005) – Media and terrorism, to the Committee of Experts on Terrorism (CODEXTER) for information and possible comments by 31 October 2005.

The Bureau of the CODEXTER held an extraordinary meeting on 17 and 18 October 2005 and, as per the Committee of Ministers' request, examined this recommendation, concentrating on those issues it considered as being within the scope of the terms of reference of the CODEXTER, and drafted comments.

At its 9th meeting (8-10 November 2005), the CODEXTER examined these comments in the context of its activity aimed at identifying lacunae in international law and action against terrorism and singled out cyberterrorism as a possible area for further action by the Council of Europe.

The CODEXTER agreed that the question of cyberterrorism should be integrated into the overall assessment of the implementation of the Cybercrime Convention (ETS No. 185) and requested that it be kept informed of developments in this respect.

The CODEXTER concluded that large scale attacks on computer systems appeared to be already covered by the Cybercrime Convention, without prejudice to any further proposals that might be presented on the subject. The CODEXTER further took note of proposals for practical measures aimed at countering and preventing the use of computer systems for terrorist purposes.

It was also agreed that CODEXTER would revert to this issue on the basis of proposals presented by delegations. The issue of cyberterrorism was, moreover, included in the CODEXTER's Progress report on future priority areas for the work of the Council of Europe in the fight against terrorism which it submitted to the Committee of Ministers.

On 20 January 2006, the Committee of Ministers took note of the above-mentioned Progress report, transmitted it to a number of relevant Council of Europe committees and agreed to return to the report at a later stage on the basis of additional information.

In 2006, the Council of Europe commissioned Professor Ulrich Sieber, Director at the Max Planck Institute for Foreign and International Criminal Law (Freiburg, Germany), to prepare an expert report on "the use of the Internet (also covering other analogous communication means such as third-generation mobile phones) for terrorist purposes and cyberterrorism."

At its 10th (June 2006), 11th (December 2006) and 12th (April 2007) meetings, the CODEXTER pursued its consideration of the use of the Internet for terrorist purposes and the notion of cyberterrorism on the basis of observations from delegations and two exchanges of views held with Professor Sieber (at its 11th and 12th meetings).

* * *

The Committee is currently conducting a survey of the situation in the Council of Europe's member and observer states on the basis of a questionnaire on national law and practice with regard to the misuse of cyberspace for terrorist purposes.

In the light of the work it has conducted, CODEXTER considers that the notions of cyberterrorism and use of Internet for terrorist purposes include several elements:

a. attacks via the Internet that cause damage not only to essential electronic communication systems and IT infrastructure, but also to other infrastructures, systems, and legal interests, including human life;

b. dissemination of illegal content, including threatening terrorist attacks; inciting, advertising, and glorifying terrorism; fundraising for and financing of terrorism; training for terrorism; recruiting for terrorism; as well as

c. other logistical uses of IT systems by terrorists, such as internal communication, information acquisition and target analysis.

Evaluation of the recommendations of the independent expert

The CODEXTER has discussed the following assessment and recommendations contained in the expert report, which in its view merit further consideration by competent bodies.

The existing international conventions and other instruments that promote the harmonisation of national substantive and procedural law and international co-operation are applicable to these misuses of the Internet for terrorist purposes. The basic question to be addressed is that of the existence of “terrorist-specific” gaps in “computer-specific” conventions and “computer-specific” gaps in “terrorist-specific” conventions. In this respect, the expert considered that no such gaps exist as far as the application of the conventions is concerned.

However, there may be general gaps, i.e., gaps that are not specific to the use of the Internet for terrorist purposes in “computer-specific” and “terror-specific” instruments:

a. A serious problem common to most international instruments is the insufficient number of states parties. This is especially true in the case of the Cybercrime Convention and the Convention on the Prevention of Terrorism, which are the most important international instruments for fighting cyberterrorism and other terrorist use of the Internet. Therefore, the signature, ratification and implementation of these two conventions should be supported, and any additional courses of action undertaken in this context should be carried out in such a way as to avoid hindering or distracting from this process.

b. The Cybercrime Convention could be further evaluated with regard to its ability to cover newly emerging or newly discussed technical advances, particularly in the area of forensic investigative techniques (such as online searches or the use of key logger software). In the fast-paced technical environment of cybercrime, such evaluations, which frequently lead to revisions and updates, are an absolutely normal process, especially when dealing with high risks such as those posed by terrorism.

However, an additional provision dealing with serious attacks on IT-based or IT-general infrastructures is not essential. It would suffice for countries to make sure that their domestic statutes on data and system interference provide sanctions appropriate for cases involving terrorist attacks against computer systems. Indeed, such “effective, proportionate and dissuasive sanctions” are already required by the Cybercrime Convention, and it can be left to the national legislatures to achieve this result by means of sentencing rules, aggravated offences on data interference, or infrastructure offences.

c. Reflection could be given to repressive and preventive measures that target the dissemination of illegal contents on the Internet and that are both effective and respectful of civil liberties. This could be done either with a special focus on illegal terrorist content or in a more general way that would encompass other types of illegal content as well. As far as substantive law is concerned, this could include the reflection on the responsibility of Internet providers, which could serve as the basis for international notice and takedown procedures.

CODEXTER opinion

The CODEXTER considers that the insufficient number of States Parties to the Cybercrime Convention and the Convention on the Prevention of Terrorism is a serious problem. It invites the Committee of Ministers to reiterate its stand on this problem and to encourage states to sign, ratify and implement the relevant conventions.

It further stresses that at the present stage primary focus should be on ensuring the effective implementation of the Cybercrime Convention and the Convention on the Prevention of Terrorism, as new negotiations might jeopardize their increasing impact on the international fight against cybercrime and terrorism.

The effective implementation of the Cybercrime Convention would ensure that national legislations provide appropriate sanctions for cases involving serious attacks, including terrorist ones, on IT-based or IT-general infrastructure. Likewise, the effective implementation of the Council of Europe Convention on the Prevention of Terrorism would target the dissemination of illegal terrorist content on the Internet.

The CODEXTER also proposed that further consideration could be given to the question of responsibility of Internet providers.