

COMMITTEE OF EXPERTS ON TERRORISM (CODEXTER)
CYBERTERRORISM – THE USE OF THE INTERNET FOR
TERRORIST PURPOSES

ARMENIA

October 2007



COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

www.coe.int/gmt

A. National policy

1. Is there a national policy regarding the analysis, detection, prosecution and prevention of cybercrime in general and the misuse of cyberspace for terrorist purposes in particular? If yes, please briefly describe it.

A national policy regarding the analysis, detection, prosecution and prevention of cybercrime and the misuse of cyberspace for terrorist purposes has not yet been worked out in the Republic of Armenia. There are several reasons for that: computer network technologies are not widely used in Armenia yet and so far no case of the misuse of cyberspace for terrorist purposes has been registered in Armenia.

The maintenance of the security of computer network technology, including the misuse of cyberspace for criminal purposes, is among the items included in the National Security Strategy of the Republic of Armenia (adopted in February 2007). One of the main directives of the Strategy is to participate in global security efforts, particularly in relation to the fight against terrorism.

B. Legal framework

2. Does your national legislation criminalise the misuse of cyberspace for terrorist purposes, and

- are these offences specifically defined with regard to the terrorist nature or technical means of committing the crime, or
- is the misuse covered by other, non-specific criminal offences?

How are these offences defined and which sanctions (criminal, administrative, civil) are attached?

The misuse of cyberspace for terrorist purposes is not defined in the Criminal Code of the Republic of Armenia as a separate *corpus delicti*, but in case of such offences the misuse of cyberspace is defined with regard to the technical means used to commit the crime.

Chapter 24 of the Criminal Code of the Republic of Armenia, entitled Crimes against computer information security, criminalises actions such as accessing (penetrating) computer information systems without permission, changing computer information, computer sabotage, illegal appropriation of computer data, manufacture or sale of special devices for illegal penetration into computer systems or networks, manufacture, use and dissemination of hazardous software, breach of rules for operation of a computer system or network.

Article 217 of the Criminal Code of the Republic of Armenia defines the *corpus delicti* of "Terrorism"; Article 217.1 refers to the Financing of terrorism and Article 389 refers to International terrorism.



For further information please see the Country profiles on counter-terrorism capacity at www.coe.int/gmt.

Pour plus de renseignements, veuillez consulter les Profils nationaux sur la capacité de lutte contre le terrorisme: www.coe.int/gmt.



Sanctions for the misuse of cyberspace for terrorist purposes are applied with the aggregation of crimes, which incorporate articles on terrorist offences (Chapter 23 of the Criminal Code) and offences in the field of computer information security (Chapter 24 of the Criminal Code).

3. Do you plan to introduce new legislation to counter terrorist misuse of cyberspace? What are the basic concepts on these legislative initiatives?

The competent authorities of the Republic of Armenia are working now on a draft Law on Information Technologies and Information Security which contains provisions on the misuse of cyberspace for terrorist purposes.

4. What are the existing national practices in the field of detecting, monitoring and closing down websites used for terrorist purposes?

No cases of the detecting, monitoring and closing down of websites used for terrorist purposes have been registered in the Republic of Armenia.

5. Does your national legislation provide criteria for establishing jurisdiction over such offences? What are those criteria?

Since the national legislation of the Republic of Armenia does not define misuse of cyberspace for terrorist purposes as a separate *corpus delicti* there are no criteria for establishing jurisdiction over such offences.

6. Does your national legal system establish ancillary offences related to the misuse of cyberspace?

There are no ancillary offences related to the misuse of cyberspace in the national legal system of the Republic of Armenia.

7. What kind of national procedures do you have for submitting an application on the activities of Internet-providers and/or hosting companies, to deprive a user from a domain name or to cancel his/her/its registration license?

According to the national legislation of the Republic of Armenia, the illegal activities of Internet providers and/or hosting companies are cancelled by the Court on the basis of the grounded decision of an investigator who initiates an application to the Court.

8. What non-legislative measures do you have in your country to prevent and counter terrorist misuse of cyberspace, including self-regulatory measures?

No non-legislative measures to prevent and counter terrorist misuse of cyberspace are applied in Armenia.

C. International co-operation

9. Please describe the general framework for international co-operation regarding the misuse of cyberspace for terrorist purposes.

Taking into consideration that no cases have been registered in the field of detecting, monitoring and closing down websites (see question 4) the competent authorities of Armenia do not have any experience in the framework of international co-operation.

10. What are the existing practices and experiences with regard to international co-operation, in particular in relation to the procedures described in question 4?

-

D. Institutional framework**11. Please list the institutions that are competent for countering terrorist misuse of cyberspace.**

According to the Law on Combating Terrorism, the National Security Service, the Police and the Ministry of Defence are directly involved in the fight against terrorism. Within their competencies, the other bodies of Executive Power are also involved in the activities related to the fight against terrorism.

12. Are there any partnerships between the public and private sectors (Internet-service providers, hosting companies, etc.) to counter terrorist misuse of cyberspace?

The private (Internet service providers, hosting companies, etc.) and public sectors of Armenia cooperate with each other to counter terrorist misuse of cyberspace.

E. Statistical information**13. Please provide relevant statistics on offences relating to the misuse of cyberspace for terrorist purposes (including possibly: cases recorded, investigated, brought to court, convictions, victims etc).**

There are no statistics on offences relating to the misuse of cyberspace for terrorist purposes.

14. Where possible, please describe briefly the profile of offenders typically involved in the misuse of cyberspace for terrorist purposes (professional background, gender, age nationality), and possible typical organisational characteristics, including trans-national links and links to other forms of organised crime.

The competent authorities of Armenia do not have any statistical information about offenders typically involved in the misuse of cyberspace for terrorist purposes.