Web site: www.coe.int/cybercrime

Strasbourg, 11 March 2008

T-CY (2008) 01
English only

THE CYBERCRIME CONVENTION COMMITTEE (T-CY)

COMPILATION OF RESPONSES TO QUESTIONNAIRE FOR THE PARTIES CONCERNING THE PRACTICAL IMPLEMENTATION OF THE CONVENTION ON CYBERCRIME

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

Replies to each question are presented by States Parties

Questions concerning general information

1. a. Before becoming a Party to the Convention on cybercrime what steps were taken by your State to carry out a general assessment of its cybercrime legislation and procedures (e.g. by setting up a Special Commission, technical co-operation with the Council of Europe or with others)?

Bulgaria

Bulgaria signed the CoE Convention on Cyber crime on 23 November 2001 in Budapest when it was opened for accession. Since November 2001 measures were taken in two main directions with regard to the facilitation of the future ratification: preparing and adopting relevant amendments to the Penal Code in order to introduce the substantive provisions of the Convention and amending the Penal Procedure Code in order to comply with the procedural standards of the Convention.

A Working group for drafting a Law amending the Penal Code was established to the Ministry of Justice with the participation of the representatives of the responsible institutions, IT and legal experts. In the process of drawing up the draft amendment texts, the proposals made by MPS, the Ministry of Interior and the working group to the MoJ were discussed upon its publication on the web page of the Ministry of Justice. The results from this public discussion have been taken into account in the drafting process.

In addition to the abovementioned at a Seminar on Cyber crime organised by the National Institute of Criminology of Romania in cooperation with the Council of Europe that took place in Bucharest on 25 – 26 March 2004, the CoE experts provided valuable contribution with concrete proposals for amendments of the National legislation (both substantive and procedural provisions) with regard to the acceleration of the ratification process.

Germany

Preliminary remark, not related to question above: although Germany is not a party of the Convention [ETS No 185] and its additional Protocol [ETS No. 189] yet, there is the strong intention to ratify both as soon as all necessary legal acts have been implemented into national law. This intention was already stressed by the early signing of the Convention in November 23, 2001. All relevant legal acts by which the Convention and the Protocol will be implemented into German law are either already enacted or they are currently in the legislative procedure to be implemented until the end of this year.

Hungary

Though the ratification of the Convention by Hungary only took place on 4 December 2003, parallel with the preparation of the Convention, the development of the modifications necessary in the area of material and procedural rules of criminal law started in the Ministry of Justice. In December 2001, within one month after the signing in November 2001, the Hungarian Parliament passed those laws

(Act CXXI of 2001, Act I of 2002) that established the harmony between the directions of the Convention and the regulation of Hungarian criminal law.

Romania

It was established a Working Group of representatives from the competent Romanian authorities (Ministry of Justice, Ministry of Communications and Information Technology, Ministry of Interior and Administrative Reform and Prosecutor Office of the High Court of Cassation and Justice) having the task to draft the law on cybercrime in order to comply with the provisions of the Convention.

Subsequently, the Council of Europe in collaboration with National Institute of Criminology organized in Bucharest (25-26 March 2004) a technical workshop with the purpose of assessing the Romanian and Bulgarian legislation on cybercrime (at that time the Romanian draft of law was still under debates in the Parliament).

Russian Federation

As early as in 1997 a new chapter was included into the Criminal Code of the Russian Federation (Chapter 28, articles 272 – 274 of the CC of RF) stipulating criminal liability for such crimes in the sphere of computer information as:
- article 272 – illegal access to information in computers, their systems and networks;
- article 273 – creation, distribution and use of computer malware. It envisages liability for creating computer programs or making changes to existing programs, which knowingly lead to unsanctioned destruction, blocking, modification or copying of the information, disruption of the work of a computer, a system or a network of computers, as well as use or distribution of such programs or machine-readable media with such software;
- article 274 – violation of rules of operation of computers, their systems and networks.

It should be stressed that the fact that Russia has not joined the Convention does not prevent her from assuming an active position, rendering comprehensive assistance and support to all interested countries. Russia has been firmly integrated into the international law enforcement system of fight against cybercrimes for a long time.

Slovakia

The Criminal Code of the Slovak Republic and Code of Criminal Procedure of the Slovak Republic were amended as well as the Act on e-communications. For the time being the Slovak Republic is preparing the ratification of the Convention (probably during the 28 Conference of Ministers of Justice in Lanzarote.

United States of America

The United States has had for many years domestic legislation applicable to numerous aspects of cybercrime. These laws, both substantive offenses and procedural mechanisms for the investigation of cybercrime, have been amended from time to time to strengthen prohibitions and to facilitate investigations, consistent with U.S. constitutional protections. Prior to ratification, an assessment was conducted on U.S. legislation and a report was prepared for the United States Senate, which is the legislative body that must advise and consent to the ratification of all treaties. This report noted that current U.S. law was consonant with all provisions of the Convention on Cybercrime, taking into account reservations and declarations permitted under the Convention.

1. b. Were any gaps found in the legislation or procedures requiring further action in order to enable your State to become a Party to the Convention (e.g. did the provisions of the Convention lead to the amendment of the existing law or was new legislation necessary to cover certain issues such as misuse of devices: Article 6; child pornography: Article 9; interception of content data: Article 21)?

Bulgaria

Before Bulgaria becoming a State Party to the Convention, there was a possibility under the Bulgarian Penal Code to investigate and prosecute child pornography, crimes against intellectual property rights, serious frauds and crimes against human rights of racist and xenophobic nature, committed by using Internet.

In addition, in 2002 the National Assembly adopted the amendments to the Penal Code in order to synchronise the legal framework with the standards of the Convention.
New texts were included for introduction of the definitions. They represent an adapted version of the definitions of the Convention.

A new Chapter on Computer crimes was also introduced in the Penal Code (Chapter 9a). It contains provisions concerning offences against the security and integrity, the confidentiality and the proper functioning of computer systems and computer data.

In order to improve the legal ground for combating the cyber crimes and to overcome some weaknesses of the criminal law the Bulgarian Parliament adopted new amendments to the Penal Code in May 2007. Some new definitions facilitating the practical application were introduced – e.g. computer programme, computer virus, computer network and pornographic materials. In addition the notions of computer system and computer data were defined more precisely.

The necessity of reinforcement the criminal liability with purpose to strengthen the child protection safeguards constituted the ground for amending the text criminalizing the child pornography offences. Art. 159, para 4 provides for aggravated corpus delicti for the whole list of offences under Art. 9 of the Convention in cases where for the purposes of creation of the work, was used a person under 18 years or person with such an appearance, including when the distribution of the pornographic materials has been carried out trough Internet. It should be noted that the new paragraph 2 provides for explicit criminalization of the distribution of pornographic materials trough Internet and it is punishable with longer term of imprisonment.

Some of the provisions of Chapter 9a were also amended in order to make some of them more accurate or to broaden the scope of the criminal protection. Such example is the case of Art. 319 d. It provides for punishing the inputting of computer viruses in a computer or in an information network. Now the criminal liability is extended also to the cases of introducing another computer programmes that are designed to hinder the functioning of a computer system or computer network (for ex. Trojan horses, warms etc.)

With regard of the procedural provisions of the Convention in May 2003 the Parliament adopted the relevant amendments that were reflected later in the new Penal Procedure Code, in force from April 2005.
These changes mainly refer to the obligation of voluntary delivery of evidence and to the procedures of search and seizure of computer information data, such as traffic data, subscriber data or content data. It is regulated the legal procedure of preparing and applying all the records on paper or other type of carrier of computer information; thus they will be considered as valid material evidence. It is ordered as well that all offices, legal persons, public officials and citizens, are

required to keep the computer records in their possession, the carriers of such data and data about the subscriber, which might be of significance to the trial, upon request by the court or by the bodies of pre-trial proceedings. These requirements refer also to the providers of information services who are obliged to ensure the keeping of data about the traffic, having the goal to trace the path of the transmitted information in connection to the case, which passes through the computer information system.

Pursuant to the provision of Art. 35 of the Convention and in compliance with the powers legally entitled to the Ministry's of Interior services a 24/7 Contact Point was established. It is empowered with all relevant competences in conformity with the provisions of the Convention. The 24/7 Contact Point is located in the Sector "Cyber crimes" to General Directorate for Combating the Organized Crime" which has nationwide responsibility for all IT or computer crime related investigations.

Germany

Preparing Germany for ratification several actions have already taken place. Changes are mainly amendments to existing laws which require legislative decisions.

Chapter 2, Section 1, Title 1 of the Convention (offences against the confidentiality, integrity and availability and title 2 (computer-related offences) have been already implemented into German law.

The following criminal offences are primarily relevant in terms of an attack on or misuse of computer systems which have been slightly amended to be in full accordance with the Convention and the protocol:

Section 202a of the German Criminal Code (Strafgesetzbuch – StGB) (data espionage), section 303a StGB (alteration of data), section 303b StGB (computer sabotage).

Additional provisions were created to reach full accordance with the Convention:

- A separate criminal offence of data interception in a new criminal provision, section 202 b StGB;
- An amendment to section 303b StGB which extends its paragraph 1 to all data processing that is of substantial significance to another" and includes as criminal conduct the entry and communication of data;
- Extending criminal liability for preparatory activities to additional cybercrime offences by establishing a new criminal offence in section 202c StGB, which criminalises the preparation of a criminal offence pursuant to section 202a or 202b StGB.

Provisions concerning Article 9 (offences related to child pornography) going to be adopted in accordance with the requirements of the Convention by the adoption of existing criminal law. This law is currently dealt with in the German legislature (Bundestagsdrucksache 16/3439).

Furthermore, provisions concerning procedural law (chapter 1, Section 2) fulfill already the reqirements of the Convention. Necessary changes e.g. concerning Article 21 (interception of content data) will be implemented by a new law amending the Code of Criminal Procedure (Strafprozessordnung – StPO), which is dealt with in the German legislature (Entwurf eines Gesetzes zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG - Bundestagsdrucksache 16/5846).

Hungary

Act CXXI of 2001 enacted the text of the criminal facts of the case of the criminal conduct for breaching computer system and computer data, as well as the criminal facts of the case of the compromising or defrauding the integrity of the computer protection system or device; furthermore, it supplemented the acts of the crimes with illegal pornographic material with the obtainment, possession, distributing of pornographic images or making them available.

In connection with the directions of the Conventions related to criminal procedural law, it was necessary to modify Act XIX of 1998, on criminal proceedings. By virtue of this, as of 1 January 2003, a new coercive measure, the order to reserve computer data, was introduced into the act.

On 1 January 2004, Act C of 2003 on electronic communications came into force. Through this it became possible to transfer traffic and billing data by the electronic communication services to authorized national security bodies, investigating authorities and the competent court of justice for the protection of national security, national defense or public safety and for the prosecution of criminal acts and any unauthorized use of the electronic communications system.

Romania

The analyze of the existing legislation with the purpose to assess its compatibility with the provisions of the Convention concluded that in Romania, like other countries, traditional criminal law focused on tangible objects and does not cover specific computer-based attacks.

Some provisions on the matter at that time were included in the following laws:

- Criminal Code;

- Law (No. 21/1999) on prevention and sanctioning money laundering, which introduced as a premiere in Romanian legislation the concept of “offences committed through computers”(abrogated by Law no.656/2002 on prevention and sanctioning money laundering);

- Law on preventing and combating pornography – no.196/2003;

- Law on electronic signature – no. 455/2001;

- Law on electronic commerce – no. 45/2001;

- Ordinance no.130/2000 - Legal regime of distance contracts;

- Law on copyright no.8/1996.

In order to harmonize the Romanian legislation with the provisions of the Convention on cybercrime it was adopted Law 161/2003 , which regulates the combating and prevention of cybercrime by implementing specific measures to prevent, discover, and punish the offences committed through computer systems.

Russian Federation

By cybercrimes the Ministry of the Interior of the Russian Federation understands a broad spectrum of unlawful actions, such as:

- computer-related crimes,
- telecommunication crimes,
- unlawful circulation of intellectual property objects,
- unlawful circulation of radio-electronic and special technical devices,

- illegal business in the information technologies' sphere,
- distribution of child pornography in the Internet.

Article 242.1 of the CC of RF envisages liability for production, storage and movement across the state border of the Russian Federation with the purpose of distribution, public demonstration or advertisement or distribution, public demonstration or advertisement of materials or objects with pornographic images of minors.

Slovakia

Implementation of the Cybercrime Convection into the legal order of the Slovak Republic was prepared within the adoption of re-codificated versions of Criminal Code (Act No. 300/2005 Coll.) and Code of Criminal Procedure (Act No. 301/2005Coll.) with entry into force on 1 January 2006. Related provisions of the Criminal Code, falling within the scope of the Cybercrime Convection. have been amended. Also Act No. 610/2003 Coll. on e-communications has been amended.

United States of America

No gaps were found in either U.S. substantive offences or procedural authorities that required further action before the United States could become a Party. Specifically, the U.S. had pre-existing legislation that met the requirements of Article 6, Article 9, and Article 21.

2. a. Please provide a short assessment of the effectiveness of your cybercrime legislation, procedures and mutual assistance (e.g. provisions and procedures working well, problems encountered including electronic evidence, gaps identified)?

Bulgaria

It is reached high degree of compliance of the Bulgarian legislation with the provisions of the Convention that assures ground for efficient enforcement of the procedures in practice.

There are also some weaknesses that appeared in the course of its practical implementation. The crimes under Chapter 9a "Computer crimes" in the Special part of Bulgarian Penal Code are not serious crimes according to the requirements of Art. 93 p. 7 PC which reads that "serious crime" is any crime for which the law provides punishment by deprivation of liberty for more than five years, life imprisonment or life imprisonment without substitution". The highest punishment for an offence criminalized in Chapter 9a PC is imprisonment from 1 to 3 years. As a consequence, in the course of the investigation of these crimes special intelligence devices can not be used as provided in Art.172 para 2 of the Penal Procedure Code, e.g. requiring the information service providers to assist the court and the bodies of the pre-trial procedures in gathering and recording computer data through the application of special technical means according to Art. 172 para 3 of PPC. The lack of these possibilities could compromise the detection and investigation of serious crimes, that can be committed in conjunction with or after committing cyber crimes under Chapter 9a PC /for example money laundering or serious frauds/.

Bulgaria encounters also some problems with the proper implementation of the Art.6 para 1 of the Convention. In terms of its practical application it is very difficult to give a proof to the criminal intent described in Art. 6. The usual case is that every device that is kept legally could be used for committing one of the offences mentioned in Art. 6 and in practice the provision of para 2 is applied in general until a crime has been committed by such devices. But such behaviour results in triggering the criminal liability of the offender on the basis of the respective provisions. Furthermore,

the approach applied in the national criminal system should be also mentioned. The criminalisation in the Bulgarian criminal law is based primarily on objective criteria and the criminal intent is main feature of the mental element of the offence.

Hungary

In harmony with the Convention, the Department Against High Technology Crime of the National Investigative Office, the independent unit against computer crime, was established on 15 February 2007. Prior to this, the Hungarian police did not have an organisational unit meeting the requirements of the Convention; in connection with computer crime, police departments and county police departments acted on the basis of general competence. It is to be noted that the Department Against High Technology Crime does not have exclusive competence: it acts in complicated cases with international relevance, requiring special knowledge.

Romania

The Romanian legislation on cybercrime consists mainly of Title III of the Law No.161/2003 on cybercrime, the provisions of the Criminal Procedure Code, Criminal Code and the above-mentioned laws, which meets the requirements of the Convention and proved to be effective.

According to the Romanian law there are three categories of criminal offences:

1. Offences against the confidentiality and integrity of computer data and systems:

1.1 illegal access to a computer system;

1.2 illegal interception of a transmission of computer data;

1.3 data interference;

1.4 system interference;

1.5 misuse of computer devices or programs.

2. Computer-related offences

2.1 computer-related forgery;

2.2. computer-related fraud.

3. Child pornography through computer systems

4. Law no 8/1996 on copyright and related rights criminalizes the infringements of copyright and related rights.

The procedural provisions of the Romanian legislation provide for interception of content data, preservation of stored computer data and preservation of traffic data, search of a computer system etc.

The framework for international cooperation on cybecrime is provided by the Law No.161/2003, which implemented the provisions of the Convention, corroborated with the Law No.302/2004 on international judicial co-operation in criminal matters, which regulates cooperation procedures including on extradition and surrender based on European Arrest Warrant.

The specialised Service on cybercrime within the Directorate for Investigating Organized Crime and Terrorism Offences is the permanent contact point 24/7, both to the assistance network set up by the Parties to the Convention, and to the G8 Network High-Tech Crime Subgroup.

Some difficulties in dealing with cybercrime arise from the extraneous element which is present in 80% of the cases.

It has to be distinguished between:

- offences committed in Romania but the results of which occur abroad;

- offences committed both in Romania and abroad committed by Romanian nationals but also foreign nationals;

- offences committed entirely outside Romania but the proceeds of the offence are collected in Romania.

These led to a delay in assessing the evidence, incorporate them in the indictments or administrate them before courts.

Other difficulties in determine the occurrence of a cyber crime:

- the failure by banking units or other institutions using public or private networks to report them selves or to communicate with their clients to report any kind of attacks on the systems that they manage;

- incidents are solved by the specialists from inside who try to identify the source or the perpetrator and they don't alert the competent authorities and don't preserve the electronic evidence.

It would be useful to get some information from software companies or companies that provide security and audit for networks in order to assess the type of acts and the size of the phenomenon.

Russian Federation

Legislators of the Russian Federation have included new crimes in the Criminal Code – computer ones. That has enabled law enforcement bodies to fight against the new threats on a new legal basis in combination with fight against traditional crimes on a traditional basis. For example, "fraud" as a type of crime exists in criminal codes of many countries, but its essence does not change, only means and tools do. The Russian legislation on fight against IT-related crimes is more flexible and convenient, its efficiency has been proved by practical experience, it covers the entire spectrum of provisions set forth in the Convention, and in some areas it has even more universal and prospective regulations.

When we receive a request substantiated by arguments from a law enforcement body of any other state, we can not only execute that request in a narrow framework, but also carry out a number of additional measures. As a rule, the obtained information can shed light on other criminal situations, which allows for not only exchange of information, but also preparation of favorable conditions for criminals' exposure and prosecution. As it has been mentioned, the Russian legislation, in general, contains legal norms that are necessary for that.

It should be noted that in the sphere of approximation of approaches on countering modern IT-related threats the issue of development of transparent and operational interaction of law enforcement bodies of different countries is still topical. It is extremely important to increase the volumes and the pace of information exchange on activities of transnational criminal groups in the Internet, on organizations and persons using information technologies with terrorist purposes, on new methods and means to commit crimes.

Slovakia

Unfortunately the Slovak Republic (in opposite with other countries) has no sufficient experiences in that respect. The provisions on the mutual assistance are provided in Part V of the Code of Criminal Procedure named as “legal relations with other countries” Those provisions are applied for all cases of mutual assistance in general unless an international treaty provides otherwise. In respect of the implementation of the Cybercrime Convections no amendments of those provisions was necessary.

United States of America

The U.S. experience has been that current legislation on cybercrime, procedures, and mutual assistance is effective. However, U.S. authorities are continually seeking to improve current processes, to strengthen laws where there have been specific challenges in prosecutions and, generally, to increase efficiency in responding to assistance requests. Thus the U.S. statutes that relate to cybercrime are frequently amended. In addition, the United States regularly provides training and other assistance to foreign partners on both Convention provisions for mutual assistance and U.S. procedures for responding to requests for assistance. Generally, the MLAT process remains the primary vehicle for requests for assistance to and from the United States. However, with respect to electronic evidence, U.S. authorities continue to emphasize the importance of the 24-7 contact network for quick requests for the preservation of relevant electronic evidence. In many cases, the U.S. has received delayed MLAT requests for electronic evidence where an earlier, informal request for assistance would have permitted authorities to promptly preserve the requested electronic evidence.

2. b. If your State is a Party to the Additional Protocol please provide an assessment of your legislation, procedures and mutual assistance.

Bulgaria

Bulgaria is not a State Party to the Additional Protocol.

Hungary

Hungary is not a Party to the Additional Protocol.

Romania

Romania signed the Protocol but hasn’t ratified it yet.
Analysing the compatibility of the Protocol with the provisions contained in the national legislation lead to the conclusion that the existing provisions are insufficient to ensure effective implementation of the Protocol.
The main law on the matter is the Emergency Ordinance Government no. 31/2002 (EOG no. 31/2002) on prohibition of organisations and symbols of fascist, racist or xenophobic nature and prohibition of promoting the cult of persons who are guilty of crimes against peace and humankind (subsequently amended and supplemented) and also some of the provisions from the Criminal Code.

The procedures and mutual assistance provisions are already implemented by the Law on cybercrime.

Russian Federation

Slovakia

Slovak republic is not a Party to the Additional Protocol.

United States of America

The United States is not a Party to the Additional Protocol.

2. c. If there are problems which further steps could be taken by your State or other States to remedy these difficulties?

Bulgaria

The increase of the sanctions for the specific computer crimes under Chapter 9a and for other non-specific computer crimes should be considered in order to provide ground for making use of the possibilities under Art.172, PPC. It is also of significance for giving larger effect to the general prevention principle.

Hungary

In connection with the Convention, most commonly problems emerge in connection with the servicing of contents. In the interest of the remedying of problems emerging in practise, international legal assistance is applied, in harmony with Act XXXVIII of 1996 on international criminal legal assistance.

Romania

EOG no. 31/2002 regulates some traditional ways of committing acts of racism and xenophobia and it does not cover the scope of the Protocol regarding the commission of some offences through computer systems, which involve essential differences as regards commission and the investigation procedure.

Some of the issues that have to be considered:

- to establish as an offence the racist and xenophobic motivated threatening/insulting, through a computer system, of a group. According to the specialised literature in the event that a threat/insult is directed at a group of persons, there will be as many victims and offences as there are persons in the group . Moreover, there is no offence of threat/insult where the author is addressing to an indeterminate community or unidentified persons .
- whether the insult should longer be criminalized in the Criminal Code or not is a controversial issue in Romania. Therefore a reservation might be considered.

As a general conclusion some amendments of the existing legislation are necessary in order to implement the Protocol.

Russian Federation

The main problems that need to be solved both in Russia and in other countries are collection of evidence and disclosure of transnational IT-related crimes not covered by the provisions of the Convention on Cybercrime.
As a rule, the majority of crimes is of economic nature and aims at gaining illegal financial profit or unlawful acquisition of other material values.
Therefore, actions by physical and legal persons in the cyberspace relating to illegal business, as well as deceits and abuse of trust are still not regulated by the Convention on Cybercrime, which, in turn, in case of a transnational nature of such crimes requires balanced approach in application of civil, administrative and criminal legislation of the states involved in the investigations.

Slovakia

Since the Slovak Republic is on the way to ratify the Convention it is premature to comment on this issue. However, it should be noted that following the TC-Y meeting the internal consultation started concerning the domestic structures. The experience will be gained also from U.S experts during the participation of the Slovak expert in the international Visitors Program, which includes the cyber crimes issues. Following the visit the consultation will continue and if appropriate, proposals will be made to the responsible ministers (one of the ideas is to establish a working party composed of different experts, where the cases will be discussed and the experience would be extended to the authorities concerned). The same procedure might be used for solving the problems of technical or legislative nature.

United States of America

U.S. law enforcement invests significant resources in information-sharing and training programs on electronic evidence and mutual assistance in many countries that request assistance. However, the effectiveness of these programs is ultimately determined by the domestic priorities and funding abilities of participating countries.

2. d. To what extent does your legislation, procedures and mutual assistance go further than the provisions of the Convention and its Additional Protocol?

Bulgaria

The provisions of Bulgarian Penal Code and Penal Procedure Code do not go further than the provisions of the Convention and Additional Protocol, but there is a number of agreements undersigned by the Prosecutor General and different official institutions in order to achieve more efficiency in the field of detection and investigation of serious crimes, including computer crimes.

Hungary

The Hungarian legal regulations are in complete harmony with the principles set by the Convention. In connection with Article 16 of the Convention, I would like to indicate that by virtue of the Hungarian regulations, it is possible to preserve data for a period exceeding 90 days. Paragraph (7) of Section 158/A of Act XIX of 1998 on Criminal Proceedings, declares that after issuing the order for reservation, the review of the affected data has to be started without delay, and depending on its

findings, and either order the seizure of the data by copying them to the computer system or other data medium, or terminate the order for their reservation. The seizure lasts as long as it is necessary in the interest of the procedure (with the exception of the compulsory cases of termination).

Romania

Romanian legislation on cybercrime was drafted considering the provisions of the Convention. Law No.302/2004 on international judicial co-operation in criminal matters is a very broad law, which regulates cooperation procedures including extradition and surrender based on European Arrest Warrant being compatible with the communitarian law and European standards.

Russian Federation

The Ministry of the Interior of Russia believes that there is no practical mechanism of creation and functioning of the 24/7 network, which may hinder exchange of urgent information and deteriorate its status. In order to raise efficiency of the 24/7 network the Ministry of the Interior of Russia has proposed to implement the “Clean connection” project put forward in April 2006 at the International practical conference on fight against cybercrime and cyberterrorism in Moscow.

Slovakia

We do not identified any significant overlap of the national provisions in comparison to the related provisions of the Convection. Please see reply above.

United States of America

In addition to legislation that fully implements the provisions of the Convention, domestic U.S. legislation, among other things, also criminalizes conduct related to identity theft (18 U.S.C. sections 1028 and 1028A); various types of extortion or threats communicated via the Internet (18 U.S.C. sections 875 and 1030(a)(7)) and some types of spam (unsolicited, bulk commercial email) (18 U.S.C. section 1037).

3. a. Which types of cybercrime are currently considered particularly serious by your State? Why?

Bulgaria

The law enforcement bodies in Bulgaria, in particular the General Directorate for Combating the Organized Crime (GDCOC), sector “Cybercrime” carry out prevention and detection of computer crimes i. e. computer fraud, identity theft, unauthorized access to computer networks and systems, child pornography on Internet, terrorist threats, intellectual piracy. All these crimes are considered as particularly serious when organized crime group at local and/or international level is involved.

Hungary

These are: computer fraud, the infringement of copyright and certain rights related to copyright and phising attacks.

Romania

According to the Article 2 of the Law no. 39/2003 on preventing and combating organised crime among the categories considered serious offence it is also the offences committed through computer or communications systems and networks.
For computer crimes committed by an organized criminal group the law provides a more severe punishment (up to 20 years imprisonment).
It can be also mentioned the maximum penalties provided by the law for some of the computer offences: illegal access to a computer system performed by infringing the protection measures (up to 12 years imprisonment); computer related fraud (up to 12 years imprisonment); child pornography through computer systems (up to 12 years imprisonment).

Russian Federation

Of all crimes committed with the help of information technologies the most serious offence, in accordance with the Criminal Code of the Russian Federation of 1996, is production and distribution of materials and objects containing pornographic images of minors (article 242.1 of the CC of RF).
The fact that the global network abounds with information and entertainment resources determines the users of such materials, the majority of which is young people and other individuals with unstable and unformed social views. In this respect distribution of materials admittedly aiming at undermining the moral foundations of the society and corruption of youth is considered one of the most serious threats to the public security.
Crimes classified in the Russian Federation Criminal Code article 272 as unlawful access to computer information and in article 273 as creation, use and distribution of malware for computers are extremely dangerous too. As a rule, such unlawful actions are the first step in more serious crimes, the consequences of which may pose a considerable threat to public and state security.

Slovakia

United States of America

U.S. law enforcement evaluates possible criminal conduct with respect to the applicable evidence sufficient to support conviction. U.S. sentencing guidelines place particular emphasis on the degree of damage or harm caused by the perpetrator's conduct. In addition, statutory penalties vary based on the specific conduct involved, and the harm caused. Specifically, the U.S. treats cybercrime that involves significant financial harm, damage to computers or computer data, serious physical harm to persons, threats to critical infrastructure such as emergency telephone and air traffic control systems, online child exploitation and child pornography, and intellectual property rights violations as particularly serious. The deleterious effect of this conduct often has an impact beyond the specific case.

3. b. Which cybercrimes have been identified as areas of growth and a likely future threat?

Bulgaria

According to the conducted analysis at present as in the future a growth in the financial frauds, the distribution of child pornography on Internet and the intellectual piracy is expected. The financial

frauds and more precisely the bank frauds cause serious damages to the Bulgarian economy. The problem is likely to have greater impact in the future due to the fact that in perpetration activities are often involved criminals from the former republics of the Soviet Union which hinders the investigation and sometimes makes it even impossible.
The intellectual piracy is a problem which engages perpetual repressive actions from the part of the law enforcement bodies.

Hungary

The branches described under the reply to Question 3.a can be considered the most dangerous in the future as well as it is the number of these criminal acts that is rising the most quickly.

Romania

According to the Romanian Strategy of Integrated Management of Romanian borders the strategic place of Romania makes the country a source, a transit area and a destination for criminal activities such as: illegal immigration and trafficking in human beings, weapons, drugs, and money laundering activities, or other aspects of economic crime.
Among the main tendencies identified that defines the evolution of the transnational crime in Romania it is also the increasing of the cybercrime, especially, the illegal access of computer data in order to obtain computer data from public institutions and make use of them.
 The most common cybercrimes: internet fraud and electronic payment instruments fraud in view of fraudulent use.

Objective factors that have favoured cybercrime in Romania :
- increasingly wide access to fast and modern equipment and connections (in the past 2 years);
- anonymous connections, non-cooperation by service providers, cyber cafés that are private or are located in university campuses or neighbourhood networks;
- the lack of legal provisions on automated retention of data over a determinate period of time, or the absence of appropriate sanctions for service providers who cause delays in the course of criminal investigation;
- the relative easiness with which one is able to carry out some of the acts specific of cybercrime;
- the delay in the response by the authorities and the little use of special investigative means, other than the interception of telephone conversations, which is totally inefficient in relation to internet cafés or neighbourhood networks.

Factors that subjectively favour cybercrime:
- the overnight enrichment of persons who commit internet fraud or fraud with electronic payment instruments
- the perpetrators' perception and belief that the acts they commit are "business", and their perception about their own selves, as they see themselves acting more as true business opportunists, never thinking of themselves as criminals

Russian Federation

Crimes connected with unsanctioned access to and creation and distribution of malware will gain momentum as demand for information, especially, closed for public grows. Emergence of new telecommunication, information, economic and household services is likely to bring about an increase in the number of unlawful intrusions in local networks and systems, unsanctioned access to resources governing critical processes related mainly to financial flows.

Development of the multimedia services market is likely to lead very soon to a new type of crimes – intellectual raids in the multimedia sphere involving attacks on universal multimedia portals and acquisition of digital intellectual property products.

Slovakia

Reply to question a, and b,
Whatsoever attacks against computer data, safety of their transmission and attacks against the whole computer systems in general. Another acts movement to derogation or abusing records and computer files or procuration or access code.

United States of America

Cybercrime in general is an area of growth. Furthermore, it appears that theft and fraud will remain the driving force behind new kinds of cybercrime. For example, the Internet phenomenon of "botnets" drives record levels of financial fraud and identity theft. Similarly, virus and worm writing no longer simply has damage or "fame" as its goal, but also sophisticated schemes to defraud. Furthermore, perpetrators are organized increasingly into "criminal undergrounds" that are international in scope.

3.c. How does your State propose to deal with this growth of offences (e.g. setting-up a specialised body, additional training and equipment)?

Bulgaria

Currently the Ministry of Interior with then assistance of private and public organizations from Bulgaria and from abroad conducts specialized courses and seminars focused on countering cyber crimes. Specialized technical equipment to be in service of the IT Experts is assembled and distributed in the Cybercrime Section in GDCOC. This equipment is still unsatisfactory for the purposes of the investigators and computer experts who work in the Section.

In addition, the Public Prosecutor's Office provides periodically training for prosecutors, specialized in cybercrime cases with cooperation of the National Institute of Justice. National Institute of Justice its self, jointly with the Public Prosecutor's Office, the Academy of Ministry of Interior, the National Investigative Service, supported by Ministry of Justice of the USA and the Embassy of the USA in Bulgaria organizes and provides training for prosecutors, investigators and police officers about specific problems of combating the computer crimes.

In order to coordinate the efforts of public institutions and non-governmental organizations in combating the crimes against intellectual property rights, an interagency body was established in 2006 at the Ministry of culture – the Council for Intellectual Property Protection. With the support of various non-governmental organizations a number of training seminars for prosecutors, investigators and police officers were conducted.

Hungary

The independent organisational unit (the Department Against High Technology Crime of the National Investigative Office) was set up to prevent this.

Romania

The existent legislation and institutional capacity provide the framework and the tools to investigate, prosecute computer crimes.
In addition, the National Institute of Magistracy or other programs have provided special training for judges, prosecutors and police officers.

However, the reaction of some authorities has been fragile concerning the size of this phenomenon. The arrests made are few and sometimes short-lived, there are no fast sentences because of proceedings involving victims abroad, lack of sentences of imprisonment that are served (mostly of them been suspended) including for acts of the type of association in view of committing offences or organised crime, etc.
The sophisticated means to carry out substantive acts, both in the case of Internet fraud and in that of electronic payment instruments fraud, lead to feelings of sympathy from the media and even from certain members of the Judiciary for the defendants who are brought to justice. Thus the actual danger represented by such acts is belittled, namely the lack of security for electronic commerce, which has severe consequences upon capital movements and data circulation, and the lack of security in computer systems or networks that manage wide-ranging activities necessary to human communities.

Russian Federation

Unfortunately, at present the law enforcement bodies of different countries are not able to act in the current legal field with 100 % efficiency against criminals in global information networks, with which the main problems are connected. One of the biggest challenges in investigations of international IT-related crimes is anonymity. The process regulating the use of telecommunication networks is very slow. Therefore, results of investigations are often not up to public expectations: the international community has created by far too favorable conditions for criminals to conceal their traces in the virtual space, and the level of cooperation of different countries' law enforcement bodies is still very low.

Success in fight against cybercrimes can be achieved only if special methods of investigating IT crimes are combined with classical methods of investigating general crimes. This complex can include all law enforcement mechanisms: creation of new units, development of new training techniques, introduction of modern technologies and further legislative work. Partnership of the state, business, science and public will play a big role in this process.

Slovakia

For the time being setting-up of a specialized body or any other measures in that respect are not necessary.

United States of America

Both U.S. criminal and civil authorities pursue investigations and prosecutions in their separate spheres. U.S. law enforcement has a long-standing program both for prosecutors and investigators who receive specialized training for investigating cybercrime. For example, each of the 93 U.S. attorney's offices in districts throughout the United States has at least one prosecutor dedicated to cybercrime cases. In addition, nearly all U.S. investigative agencies now incorporate cyber units and officers with special training in computer evidence. U.S. law enforcement agencies also provide assistance and training in cybercrime and computer evidence to international partners. Promotion of the Convention is always a component of international outreach efforts. Finally, U.S. law

enforcement is actively engaged in industry-law enforcement partnerships that can leverage resources in both sectors to identify perpetrators and bring successful prosecutions.

4. a. How often has the 24/7 network been used since your State became a Party, in which types of cases and has it been successful?

Bulgaria

To the moment within the framework of the 24/7 network between 20 and 30 inquiries were addressed since the Bulgarian contact point is fully operational. The cases concerned involve identifying of e-mail boxes users and the used IP addresses; determination of persons posing terrorists threats through Internet; data preservation of contents and logs from web sites, containing illegal content or objects of intellectual property. In the majority of cases the initiated actions in response to the requests resulted in positive development.

Hungary

With view to the relatively short time since the setting up of the special organisational unit, there is not enough information at disposal to answer the question.

Romania

 The Directorate for Investigating Offences of Organised Crime and Terrorism (through the International Cooperation Office)

• the first half of the year 2007:

- 30 requests for mutual assistance transmitted to EU Member States, USA, Russia and Switzerland;
- only 7 requests have received replies.

- 45 requests for mutual assistance received from EU Member States, SUA and Turkey;
- 24 have been solved.

 The Service on cybercrime

- 4 requests for expedited preservation of computer data received from the USA;
- 1 request received from Germany;

2 requests for expedited preservation of computer data addressed to the USA initiated by the Service, one of them been followed by letters rogatory.

Russian Federation

The 24/7 network is used for international contacts to exchange information with other countries every day. This mechanism is very effective and efficient in receiving and sending information; it makes the information exchange much faster and easier in comparison with other alternative channels of communication.

Slovakia

In Slovak republic is the 24/7 network don't used, but it will be really good when this ability could be.

United States of America

The United States was a founding member of the 24/7 contact network, which has been in operation since 1997. Since becoming a party to the Convention, the United States has an expanded set of 24/7 contacts. The United States frequently uses its 24/7 network of contacts for both outgoing and incoming requests for assistance. U.S. agencies promote the 24/7 network as the primary vehicle for prompt requests for preservation and other assistance in emergency cases. Requests through the network have concerned cases ranging from financial fraud to terrorism to threats on the life of heads of states. In emergency cases, the network has proven to be both resilient and effective.

4. b. Please indicate if there have been any difficulties in obtaining mutual legal assistance in urgent cases.

Bulgaria

Hungary

Romania

In most cases the Romanian authorities send at least a request for information to foreign authorities, by using any of the accepted police channels but the reply time even for information exceeds 20-30 days.

Pre-trial investigation and than the trial take a long time, given the procedure for summoning persons who live abroad (the summoning takes place according to mutual assistance treaties concluded by Romania).

See also 4 a. and the study case.

Russian Federation

As a rule, there are no particular problems with information exchange and rendering assistance in urgent matters connected with serious threat to the state and the public. The main obstacle in creation of the mutual assistance mechanism is a sharp difference in legislative regulation of investigation and prosecution processes, as well as peculiarities in the structures of law enforcement bodies and in the systems of information flow and application of information.

Slovakia

There are no experiences in obtaining mutual legal assistance.

United States of America

There have been no difficulties in obtaining mutual legal assistance in urgent cases that can be attributed to either the Convention or the 24/7 network.

4.c. Please indicate whether the Convention has been used as a basis for expedited mutual assistance (e.g. including with States which have used the Convention as a model but which are not Parties).

Bulgaria

All States inquired which are parties to the Convention have followed the recommendations laid down in the Convention in particular granting urgent preservation of data and technical advice. In several cases inquires have been addressed to States which have not acceded the Convention, but have nevertheless observed it as legal ground and provided cooperation.

Hungary

Romania

Convention has been used as a basis for expedited mutual assistance with the States Parties to the Convention.

Russian Federation

Provisions of the Convention were applied for receiving or rendering assistance in information exchange or investigation of transnational crimes. Having signed many international mutual assistance agreements Russia has become an active participant in the process of countering transnational crimes (cybercrimes being just an individual case). However, there have been instances of preposterous refusals from our foreign partners to provide us with information under pretext that Russia has not joined the Convention.

Slovakia

Not , we don´t have any experiences.

United States of America

U.S. authorities do not keep track of the specific basis of a request for assistance. However, the United States has sent numerous requests for assistance, and has received the same, from both Parties and States that have used the Convention as a model Some of these requests formally invoke the Convention. Requests for assistance have been received and sent primarily to countries that are members of the 24/7 network and/or have existing MLATs with the United States. U.S. authorities regularly promote the Convention as a solution for countries that are neither members of the 24/7 network nor have an existing MLAT with the United States.

Case studies and best practices

5. Please give details of the steps taken in cases which have arisen since your State became a Party and which could be usefully be included in the collection of case studies and best practices to be considered by the T-CY. For each case please follow the indications given below:

I. General Information

a. type of offence (e.g. child pornography, terrorist issues)

b. why expedited assistance was needed (e.g. number of victims or potential victims, risk to life, very large financial issues)

c. number of States involved

d. if this is the case please indicate the extent to which the case was successful (e.g. web-sites removed, persons punished, persons or money recovered). Please also indicate, where appropriate, why the case was not successful.

Bulgaria (the reply to I General Information and II Steps taken)

First Case

1. Terrorist threat directed by e-mail to the mass media.
2. The expedited assistance was needed, because of the fact that the life of a huge number of people staying in a Bulgarian ski resort was endangered by a threat of causing an avalanche.
3. One State involved
4. The IP address from which the e-mail containing the terrorist threat had been sent was identified. The e-mail was registered in a Russian post server. All the IP addresses from which the e-mail box had been accessed have been also located. The investigation was hampered due to the fact that the perpetrators had sent the threatening message from public Internet Café in the capital of Bulgaria.

Second Case

1. Detecting a Bulgarian citizen wanted for murder who threatened by e-mail to commit another murder
2. The expedited assistance was needed, because the Bulgarian citizen had accessed his e-mail box, using IP addresses of foreign ISPs. Immediate establishment of his relations in the foreign countries that he had visited was necessary.
3. Two States involved.
4. In cooperation with the respective police services the physical location of the IP addresses that the suspected had used were determined. The Bulgarian authorities issued an European Arrest Warrant and the detention of the person is forthcoming.

Third Case

1. Threat for murdering Bulgarian politicians, sent by e-mail.
2. The expedited assistance was needed because the threat was targeted to high level Bulgarian politicians.
3. Two states involved– one of the countries is not a Party to the Convention.
4. The IP addresses from which the emails originate have been identified after which request for mutual legal assistance was addressed to a country that is not Party to the Convention. In this

particular case the Convention was used as a legal ground for the request, and the responding country has provided full cooperation. The other cooperating State which helped detecting the users of the mail boxes established that the e-mail headers have been forged to include the domain trough which the e-mails have been sent from.
The investigation is still running and further information can not be provided at this stage.

Hungary **(the reply relates to all the remaining questions)**

In the application of the Convention, there emerge no criminal procedures with special significance from the aspect of the international practise.

Romania

It has been identified based on specific activities of data collection criminal activities carried out in Romania and abroad by a group of Romanian nationals.

The investigation have shown that in the area X, a group of individuals using the locations of Internet cafés as well as stand-alone computer systems, were systematically holding fraudulent auctions on various specialised websites, offering to sell fictitious goods, in order to unjustly collect the worth of such goods.

Working as branches several Romanian nationals have been identified in European countries (United Kingdom) and in the USA.

Group features:
- closed, joint action – Romania – United Kingdom – USA
- use of Romanian and British prepaid cards to communicate information within the group
- specialised one-way communications and periodic changes of prepaid cards
- use of Zapp internet services, private-owned internet cafés
- specialised knowledge of computing, programming and configuration of computer systems

The authorities gathered evidence about the following:
- fraudulently creation of user accounts (seller/buyer) on specialised online sales websites (e.g. eBay) or unauthorised access into existing user accounts
- send information about goods and technical data about them
- creation and use electronic of mail addresses for collection, which were checked by several group members
- e-mail messages received from the „winning" bidders, who were in fact deceived buyers
- identification data of electronic payment instruments (credit cards) transmitted with the intend of fraudulent use
- creation and use of fictitious escrow websites
- the involvement of some internet service provider's employees to secure anonymity of the connections
- British bank accounts accessible online, used for collecting the money resulting from fraud
- receipt/transmission/retransmission of identification numbers for money transfers made by the „winning" bidders by SMS
- generic identification of locations (..."at the office", private-owned internet cafés, with restricted access, as well as some of the individual computer systems)
- fictitious identities used for picking up the money
- the identity of the victims.

The group members, the relationship between them and the role they played within the group were identified.

The defendants and accused have been charged with the following offences:

- organised crime (Art.7 para. 1 in relation to Art.2 b) indent 18 of Law No.39/2003)
- continued swindling (Art.215 para.1,3 Criminal Code, also applying Art.41 para.2 Criminal Code)
- continued unauthorised transmission of identification data for electronic payment instruments (Art.27 para.1 indent 3 of Law No. 365/2002 also applying Art.41 para.2 of the Criminal Code)
- unauthorised access to computer systems (Art.42 of Law No.161/2003 also applying Art.41 para. 2 of the Criminal Code.)

For the preliminary stage before criminal prosecution and even for the actual action taken to eliminate the criminal group, the case was considered to be a success.

Russian Federation

a) A DDoS attack on an information resource in the Internet; blocking the work of a site, with which the money inflow is connected; further extortion in exchange for stopping the attack.
b) Botnet herders sent their e-mails with demands to pay ransom for stopping the attack from the territory of the Russian Federation.
c) The crime was committed in the territory of Russia, the attack victim was in the territory of another country, thus, the investigation was conducted by law enforcement bodies of two states.
d) The case was brought to court, which took place in the territory of Russia. Evidence necessary for the "guilty" verdict was collected and the court sentenced the criminals to imprisonment and payment of a large fine.

Slovakia **(no replies to further questions)**

United States of America

The U.S. handles a very large number of 24/7 requests for assistance every year. In most cases, the facts never become public. Following are some reduced details of cases in which the U.S. assisted (not necessarily since it became a Party).

1. Kidnapping of elderly woman in Country A. Ransom notes came exclusively via the affiliate in A of a U.S. Internet service provider and therefore the data was stored in the United States. Expedited assistance was necessary due to the threat to her health and perhaps life; two States involved; emails were successfully traced, she was released, and the perpetrators were arrested.

2. Young teenager went missing in Country B on a Friday. Her parents opened her email account to law enforcement in B. Her emails were sent through the affiliate in B of a U.S. ISP and the data was therefore stored in the United States. The emails indicated that she had been chatting with an older man and may have gone to meet him for the weekend. Expedited assistance necessary due to the threat to her health and life; two States involved; subscriber information for the man was provided within hours and the teenager was located.

3. The United States handles a very large number of foreign requests for assistance in phishing, fraud and intrusion cases every year. In a typical case, a transmission will come from an ISP in the United States into another State and law enforcement in that State will request preservation. U.S. authorities will issue a preservation letter and reply to the requesting state. Thereafter, the requesting State will send a mutual legal assistance request to obtain the evidence. Sometimes the U.S. will open a joint investigation with the requesting State, in which case evidence exchange is normally quicker. Most of these cases require quick assistance because of the potential money loss or threat to privacy and because the transmissions often require tracing through more than one

country. The rate of success in these cases varies; also, after it renders its assistance, the U.S. usually does not learn the final result.

II. Steps taken

Please indicate briefly and in chronological order the different steps which were taken and which led to the successful outcome or, in the case of an unsuccessful outcome, the problems which arose and whether steps can be taken in the future to avoid a recurrence of such problems.

Romania

1. The preliminary documentation activity (total length: 4 months)

Two letters rogatory have been sent to the United Kingdom, as well as requests for assistance were sent through the Interpol to the States whose nationals had been deceived. The IC3 was contacted through the FBI.

Authorisations were requested and obtained to intercept telephone conversations and to gain access into computer systems.

Total authorised duration: 4 months

Before the expiry of the 4 months of interception, intelligence activities were included in the plan of action, consisting of static and dynamic surveillance of the group of perpetrators.

2. Initiation of criminal prosecution (upon expiry of the duration of interceptions)

The field documentation covered 26 locations (domiciles, cafés) – field recognition operations in view of accurately establishing the data about the access to locations, the location of computer systems, the internet connections.

Authorisations were requested and received for domicile searches

- In this context, all the locations concerned : 19 in X, 1 in Y and 6 in Z were covered, which led to the identification of both the persons concerned and the computer systems, the instruments used to commit the acts, some of the amounts of money, documents, telephones, etc.
- One person was identified by specific means while in the road traffic. 11 persons were arrested in relation to this case and subsequently brought to court. Preventive arrest warrants were issued for a period of 29 days.
- The public prosecutor considered that with regard to 7 other accused persons it was appropriate to take the measure of obliging them not to leave the country
- An overall number of 30 persons were heard

The main activities after the arrests

- Authorisations were requested and received to perform searches in computer systems
- The searches of computer systems showed, as expected, actual computer data regarding the commission of the offences of swindling, unauthorised access to computer systems, transmission of identification data for electronic payment instruments (credit cards)
- The recorded telephone conversations were certified
- The defendants and accused were interviewed, as well as the witnesses
- Documents were seized

- Witnesses were heard
- Replies were received to the rogatory letters sent to the United Kingdom (the first partial reply was received three months after the date when the rogatory letters were sent; the final reply was received 1 year and 2 months from the date when the rogatory letters were sent)
- Complaints were received from the victims, through the Interpol, through the FBI Liaison Officer Bureau, directly (the collection of complaints lasted for almost one year). After approximately 4 months, the law court considered that it was appropriate to release the detained persons.

Although this measure was appealed against by the prosecutor, the court decided that the defendants were not a real danger to the public order and dismissed the appeal.

Russian Federation

Actions taken in course of the investigation:

1. Receipt of a request with information on supposed crime.
2. Preliminary check-up of that information, request for additional data pointing out to unlawful nature of actions by suspects towards victims.
3. Organization of close cooperation of the affected party and that country's law enforcement bodies with the investigation authorities of Russia.
4. Record of evidence of unlawful actions, analysis of the information provided by foreign partners or obtained in course of the investigation.
5. According to a preliminary agreement, a situation was set up when the blackmail victim fulfilled all demands made by the perpetrators in their e-mail, while the law enforcement recorded the sender and the recipient of the letters.
6. After all evidence had been collected, a decision was taken to arrest and prosecute the suspects.

III. The main methods used in course of the investigation:

1. Timely exchange of information between the law enforcement bodies of two states.
2. Coordinated record of crime evidence in both countries.
3. The case was conducted by Russian law enforcement officers in the Russian territory and observers from the other country were constantly informed about the course of investigation.
4. Actions were jointly planned and coordinated.

Cooperation of all companies and organizations that could provide any assistance in that criminal case was engaged.

United States of America

In examples 1 and 2, foreign law enforcement contacted the U.S. 24/7 contact point and U.S. authorities contacted the U.S. ISP. The ISP provided the necessary information quickly and the U.S. authorities passed it back to foreign law enforcement. Re example 3, see answer above.

III. Best practices

Please give details of any procedure which was used and which could be used by other States in order to fight cybercrime more efficiently (e.g. investigative manuals, standard formalized procedures)

Bulgaria

In 2005 in implementation of a project of ABA/CEELI in Bulgaria an interagency working group was established where the Supreme Cassation Prosecutor's Office, the Ministry of Interior, the Sofia City Investigation Service and Computer Technology Institute were represented. As a result a Practical manual for assisting the detection and investigation of cyber crimes was elaborated. Furthermore, the experts from the working group provide consultancy and support on particular cyber crime cases to the law enforcement bodies in the pre-trial stage of criminal proceedings.

In addition to this a Practical manual for prosecutors intended for internal use only in order to provide guidance in their work on crimes infringing intellectual property rights was issued in 2007. It was result of the common efforts of various state institutions /Public Prosecutor's Office, Ministry of Culture, Bulgarian Patent Office/, united management organizations of intellectual property rights and the Association of Bulgarian Prosecutors supported by the USA Ministry of Justice and the USA Embassy.

Romania

The mechanisms and procedures set up by the Convention in order to investigate and prosecute computer crimes, procedural provisions on interception of content data, preservation of stored computer data and preservation of traffic data, search of a computer system etc. and also the investigative methodologies.

United States of America

In general (not with specific reference to the cases above), the U.S. relies heavily on systematization to address cybercrime. For example – this is not an exhaustive list – most of the U.S. federal agencies with cybercrime jurisdiction have internal investigative guidelines and they often write manuals for the public or for other investigators. Some of these cybercrime organizations, though headquartered in Washington, D.C., have sub-units specializing in cybercrime in other American cities. The Computer Crime and Intellectual Property Section of the U.S. Department of Justice, which is composed of prosecutors, publishes several manuals at its website, www.cybercrime.gov. CCIPS also collaborates with, and provides training and advice to, a network of specialized cybercrime prosecutors in the 93 federal judicial districts in the United States.

IV. Other suggestions

Please make any other suggestions or remarks that may be helpful for the future work of the T-CY.

Romania

Considering the challenges entailed by the fight against cyber crime, the ever-increasing diversity of types of offences perpetrated through computer systems, and also the need to create the proper legal framework at both nationally and internationally level, there is a need for special tools in order to combat this phenomenon that should take into account the complexity and the need for a totally different approach to computer crimes.

Council of Europe Convention is a valuable instrument for:
harmonizing the domestic criminal substantive law elements of offences;
providing procedural law powers necessary for the investigation and prosecuting of such offences as well as other offences committed by means of a computer system;

establishing a framework for an effective and fast international cooperation.
In order to be effective it has to be promoted all over the world.

At the international level it should be also identified solutions for speeding up the mutual legal assistance procedures giving the fact that the necessary time to obtain the complaints and the documents requested by rogatory letters followed also by other inherent activities reduces the intended efficiency.

A model (form) of the request for expedited preservation of computer data generally accepted by the Parties would be very useful in practice.

Russian Federation

In accordance with Article 18.a. of the Vienna Convention on the Right of International Treaties of 1969 the Russian Federation will refrain from actions that would devoid the Convention on Cybercrime of its subject and goal. At the same time, Russia proceeds from the assumption that, in her opinion, the current wording of Article 32.b. of the Convention does not exclude such means of interpretation and application that do not correspond to its subject and goals, namely: goals and principles stated in the ninth and the tenth paragraphs of its preamble - and can damage the state sovereignty and national security of the member-states, as well as rights and legal interests of their citizens and entities.

The Russian Federation will make decision on her participation or non-participation in the Convention, considering also possible review of provisions of Article 32.b. in the manner prescribed in paragraph 3 of Article 46 of the Convention or in accordance with another procedure that can be used by the Parties to that end. At the same time, the Russian Federation is ready to cooperate with the Council of Europe member-states and other countries that have signed the Convention in order to solve this issue on the basis of respect and observance of its subject and goals.

The ambiguous wording of Article 32.b. provides for penetration to information networks of another state without its notification on the basis of someone's permission. However, it is not clear whose permission that is, which resources it extends to, what authorities that person has and how that permission was received. Proceeding from the experience of many years it should be noted that modern investigation of a computer crime is an intricate complex of interconnected measures taken by operative units and different structures in the public and private sectors. These measures are taken not only in the virtual space of telecommunication networks, but also among people living in a specific state and being subject of its jurisdiction. Therefore, it is not possible and even ridiculous to count on success in investigation of a computer crime through penetration to computer networks of another country.

The Ministry of the Interior of the Russian Federation believes that Article 32.b. contradicts internationally recognized norms of respect of sovereignty and human rights fixed in many international documents. It is advisable to ask for the member-states' opinion on that matter. We propose to make amendments to the text of the Convention that will be in line with common practice and modern requirements.

United States of America

The United States believes that it is most important that the T-CY emphasize full implementation by Parties and proselytizing to other countries rather than amendment of the Convention. A mechanism for this might be for Parties to volunteer to encourage other countries to become Parties – that is, if Country A has a historic or special relationship with Country B, A would volunteer to recruit B.