COMMITTEE OF EXPERTS ON TERRORISM (CODEXTER)
CYBER TERRORISM — THE USE OF THE INTERNET FOR TERRORIST PURPOSES

CZECH REPUBLIC

July 2007

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.

The Government of the Czech Republic, with the aim of maximising the potential of the modern information and communication technologies, decided to find a new definition of its objectives in the area of the so-called information society and in the area of telecommunications - and to formulate a new state strategy for the future.

Contrary to the previous approach, where the two concepts were elaborated separately (see the documents "State Information Policy: Toward Information Society" and "National Telecommunication Policy"), the Government decided to respect their close interconnection and the general trend towards the convergence of both areas, and to create one common strategic document, entitled "State Information and Communication Policy: e-Czech Republic 2006". The name of the document itself also reflects the transformation of the former telecommunications branch into the electronic communications branch.

The four main areas of the activity of the Government of the Czech Republic were set out:
- available and secure communication services;
- information education;
- modern public services on-line;
- dynamic environment for the electronic enterprises.

With the goal of strengthening information security in the sphere of the communication and information infrastructure of the Czech Republic and in compliance with Section 4 (1b) of Act No. 365/2000 Coll., on public administration information systems, strategic documents were drafted in the sphere of the protection of public administration information systems of the Czech Republic, explicitly mentioning also the possible threat of a terrorist attack. These are in particular:

- "National Strategy of Information Security of the Czech Republic", which sets tasks in the sphere of building trustworthy information and communication systems in the setting of the Czech Republic.
- "Concept of Transfer of Classified Information by the Czech Republic's Public Administration Communication Infrastructure" which responds to the constantly increasing requirements for transfer of certain, especially classified, information determined by legal regulations. The document proposes a solution via the integration of the information systems into a universally usable secure public administration communication system providing access to the networks of other countries of the European Union.
- "Proposed Protection Levels for the Information Systems Necessary for the Functioning of the Critical Infrastructure of the Czech Republic".
- Amendment to Act No. 101/2000 Coll., on personal data protection and on changing some laws, as amended by later regulations (439/2004 Coll.), Section 13 (2), which says that the...
administrator or processor is obliged to process and document the adopted and realised technical and organisational measures for ensuring personal data protection in compliance with the law and other legal regulations.

- "Strategy of the Fight against Information Technology Crime", subsequently elaborated by the Ministry of the Interior and approved by the Minister of the Interior on 5 June 2001. This document is based on the outcome of police work in this area.

Both qualitative and quantitative analyses of these forms of crime indicate their apparent dangerous character for society, as there is not only a danger of material damage in individual cases, but also the danger of consequences in the form of a threat to the unstable and uncontrolled environment of the information and communication dimension of society, which could lead to the development of modern society being hindered. Since information and communication technologies are increasingly being interlocked with individual areas of human activities, insecurity in these structures could lead to the social and economic system itself being destabilised.

The Strategy also represents a reaction to the task set out for the Minister of the Interior in the Updated Strategy of Combating Organised Crime approved by the Government of the Czech Republic in October 2000. The Minister of the Interior was charged (on the basis of the Schedule of Measures forming the annex to the relevant Government Resolution) "to continuously and in a strategic way address combating organised crime activities in the area of information technologies." The Strategy presented here is, however, of a more complex nature because information technology-related crime is not limited to organised crime activities.

The key starting point of the strategy is the opinion that the approach of the Government to this type of criminality should be: systematic; balanced in putting differentiated emphasis on each aspect of such crimes according to their danger to society; diversified in a desirable way amongst the ministries and within the ministries; and, at the same time, coordinated through intensive co-operation between all the departments of the state bodies involved and through the Government co-operating with non-governmental organisations and with foreign countries.

The most important objectives of the above-mentioned document are:

- To ensure conditions for the further development of the structures directly engaged in the detection of computer crime (high-tech crime), including material and personal development of specialised police units.
- To increase and support co-operation between the law enforcement agencies, intelligence services and NGOs involved in the fight against various aspects of computer crime (high-tech crime).
- To elaborate principles for the protection of state, and some strategically important non-state, information systems.
- To elaborate a project for an alert system in the area of computer crime (high-tech crime).
- To elaborate a project in the area of educating the personnel of law enforcement bodies, with special regard to the clarification of criminal activity in the area of computer crime (high-tech crime).
- To develop and to set up forensic standards for seeking and verifying electronic data during criminal investigations and criminal procedures.
- To support independent research, public relations and statistics activities in the area of the fight against computer crime (high-tech crime).
- To promote public awareness campaigns, focused on recommended behaviour in cyberspace.
- To monitor the respective activities of the international platforms in the area of the fight against computer crime (high-tech crime). To participate in the relevant conferences and workshops.

This agenda must be understood as being interconnected with other parallel intra-community activities in order to ensure appropriate relations between the personal and technical capacities
concerned. This especially applies to activities within the framework of the Security Research of the Ministry of the Interior for the years 2007-2010.

B. Legal framework

2. Does your national legislation criminalise the misuse of cyberspace for terrorist purposes, and
   a. are these offences specifically defined with regard to the terrorist nature or technical means of committing the crime, or
   b. is the misuse covered by other, non-specific criminal offences?
   How are these offences defined and which sanctions (criminal, administrative, civil) are attached?

In the Czech Republic, the respective acts are punishable as criminal offences within the framework of criminal law according to Act No. 140/1961 Coll., Criminal Code (hereinafter "Criminal Code").

The Criminal Code contains the constituent elements of a terrorist attack through which the implementation of the Framework Decision on combating terrorism was ensured. In the view of the Czech Republic, the described examples of behaviour might be prosecuted on the basis of this section. The constituent elements apply not only to a person committing an actual terrorist act, but also to a person who threatens to commit a terrorist act or who provides financial, material or other support (i.e. propagation, approval of or apologie of terrorist acts) to such an act. Imprisonment of five to fifteen years (under specific circumstances, even the exceptional sanction of life imprisonment) and, eventually, the forfeiture of property may also be imposed for these acts.

Furthermore, the Criminal Code contains provisions concerning public provocation to commit a crime and approving a crime. However, these crimes are of a general nature - they refer to all types of criminal behaviour, not only to terrorist offences.

Under Section 164 of the Criminal Code providing for the crime of instigation, anyone who publicly incites other persons to commit a crime or not to fulfil en masse an important duty imposed by law, shall be sentenced to imprisonment for a term of up to two years. This crime may be committed orally, in writing or in any other way possible.

Under Section 165 providing for the crime of approving of a crime, anyone who publicly approves a crime or publicly praises the perpetrator of a crime shall be sentenced to imprisonment for a term of up to one year.

Furthermore, if the above-mentioned examples of conduct are intended to support racially- or ethnically-motivated terrorism, they may be punished as the crime of incitement of national and racial hatred (Section 198a of the Criminal Code). The constituent elements consist in a person publicly inciting hatred of another nation or race or calling for the restriction of the rights and freedoms of other nationals or members of a particular race and may be punished.

At constitutional level, freedom of expression is provided for in Article 17 of the Charter of Fundamental Rights and Freedoms of the Czech Republic. According to its paragraph 4, it is possible to limit the freedom of expression and the right to information by a law adopted by Parliament, if it is necessary in a democratic society for the protection of the rights and freedoms of others, state security, public security or the protection of public health and morals.

As far as the legislative process is concerned, no serious problems were encountered as regards the adoption of anti-terrorism legislation with respect to the freedom of expression in the Czech Republic.¹

¹ Following 11 September 2001, several cases of the apologie of terrorism (verbal, printed or posted on the Internet) have been recorded, usually associated with extremist groups (extreme left/right wing groups and fundamentalists). Some of these incidents
It has been possible to prosecute all the relevant cases (except cases involving the distribution of bomb- or explosives-making expertise) as criminal offences. Since there are no doubts that this is a criminal offence, the police have not registered any serious problems (except for lengthy procedures) with the prosecution of suspected criminals who are considered to have committed their crimes in the Czech Republic.

The Criminal Code does not provide specific regulations covering the transmission of bomb- or explosives-making expertise, preparation of attacks, hostage-taking or other actions related to the commission of a terrorist offence. However, such conduct may be punished according to its general provisions, namely the provisions on participation in a crime might be used in this relation. Section 10 of the Criminal Code provides that a participant in a completed crime or an attempted crime is a person who intentionally organises or directs the commission of a crime (the organiser), instigated another person to commit a crime (the instigator) or grants another person assistance in committing a crime, particularly by providing the means for committing such crime, removing obstacles, giving advice, strengthening the person's intent, or promising assistance after the commission of the crime (an assistant). The criminal liability and liability to punishment of a participant are governed by the provisions on the offender's criminal liability and liability to punishment, unless the Criminal Code provides otherwise.

Furthermore, the outlined behaviour could be considered as preparation of a crime under Section 7 of the Criminal Code. This section provides that conduct which threatens society and which consists in the organising of an especially serious crime (indeed, this category covers terrorist offences), the acquisition or adaptation of means or tools for the purpose of committing a crime or associating, assembling, instigating or giving assistance for such purpose, or other intentional creation of conditions for the commission of a crime shall be considered as preparation of a crime, even if such a crime is not attempted or committed. Preparation of a crime is punishable within the sentencing guidelines for the crime which was prepared unless the Special Part of the Criminal Code provides otherwise.

The police monitor web pages and other sources which provide readers with such information or expertise. However providing information and expertise on explosives-making is not defined as a criminal offence.

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

The legislative and other measures adopted by other countries against religiously-motivated hate crime are constantly monitored by the authorities. Especially the possibility of a more precise qualification of the activity, that could be considered as verbal approval of a terrorist attack, promotion of terrorism and incitement to terrorism, is being analysed.

The Czech Republic considers the above-mentioned legal regulation on the penalties for the propagation, *apologie* and glorification of terrorist attacks to be sufficient and there are currently no plans to amend this regulation.

With respect to the above, the Czech Republic holds the view that the current legislation is sufficient and no further specific legislation is required.

---

have been examined by the authorities to determine whether a crime has been committed under Section 164 of the Criminal Code (incitement) or Section 165 (advocating a crime). However, nobody has been convicted of a terrorism-related crime. The Police of the Czech Republic often face problems when the authorities are unable to prosecute activities that are considered as being dangerous to society (for example cases involving terrorist attacks being described "in a positive way") but these activities are difficult to prosecute as a criminal offence. The authors of such texts usually "react" to an official article concerning a particular terrorist attack. Their “comments” are published on “problematic” webpages. The comments are written in a sophisticated way, so the authorities are unable to prosecute these activities as a criminal offence. Theoretically, these activities could be prosecuted as minor offences, but in reality it is not possible because in such cases the police are not entitled to obtain the relevant telecommunications data.
However, some lacunae may be identified as an outcome of the Security Research of the Ministry of the Interior for the years 2007–2010.

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

   - Act No. 365/2000 Coll., information systems of the public administration, stipulates the conditions and limits of the transmission of data within the public administration. This Act does not have a direct impact on the prosecution of possible misuses of information or their dissemination by terrorists via the Internet.
   - Act No. 127/2005 Coll., on electronic communications, and amendment of some relevant acts, stipulates new conditions for access to commercial services via electronic communications. This act does not stipulate the responsibility of the subject who provides the service for the content of the information transmitted.
   - The limitation of access to the public electronic communications service is possible only on the grounds of a special act (Act. No. 241/2000 Coll., economic measures during a crisis situation).

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

   See the reply to question 4.

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

   Yes, for example the following sections of the Penal Code:
   152: Infringement of copyright;
   176: Forgery of official documents;
   239: Violation of the privacy of transmitted messages;
   250: Fraud;
   257: Damaging another’s property;
   257a: Damaging or misusing data carrier records;
   260: Support and propagation of movements aimed at suppressing citizens’ rights and freedoms.

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 or licence?**

   For the purpose of administering the domain *.cz, a Special-Interest Association of Legal Entities, CZ.NIC (http://www.nic.cz/), was established, in accordance with the provisions of Section 20f et seq. of the Civil Code by a Foundation Contract dated 21 May 1998. From the Rules for the registration of Domain Names in the *.cz domain:

   **14. Rights and duties of the cz.nic association**

   **14.1.** The CZ.NIC Association undertakes to register a Domain Name under the conditions specified by these Rules and to maintain that registration under the set conditions.

   **14.2.** The CZ.NIC Association undertakes to keep an entry on a registered Domain Name in the Central Register and the CZ Zone under the conditions specified by these Rules.

   **14.3.** The CZ.NIC Association undertakes to develop all possible efforts as may reasonably be required to secure the failure-free and problem-free operation of the Central Register and the primary name server.

   **14.4.** The CZ.NIC Association, based on its decision, is authorized to cancel registration of a Domain Name, providing:
14.4.1. Data kept in connection with a Domain Name in the Central Register is false or misleading;
14.4.2. The facts based on which a Domain Name was registered have changed. For example, the Holder ceased to exist without any legal successor or died without inheritors;
14.4.3. No approval of the Rules of Registration is granted according to the Rules of Registration;
14.4.4. Such a right derives from other provisions of the Rules of Registration.

14.5. The CZ.NIC Association will cancel the Delegation of a Domain Name or registration of a Domain Name if it is requested by an executable judicial verdict or an award of an arbitration court. The CZ.NIC Association will transfer a Domain Name to a third person if it is requested by an executable judicial verdict or an award of an arbitration court.

14.6. The CZ.NIC Association is authorized to take all the measures that will be ordered by a preliminary measure, including limitation of the right to transfer a Domain Name.

14.7. As regards the pursuit of the CZ.NIC Association according to items 14.5 and/or 14.6, the CZ.NIC Association is not obligated to return any previously paid amounts.

15. Damage liability

15.1. The Holder acknowledges that a Domain Name, its registration, or its use may infringe on third persons’ rights to other Domain Names, trade marks, brand names, names, business companies or legal regulations concerning unfair competition, protection of personality, etc. By filing an application for registration of a Domain Name, the Holder confirms that they are aware of the potential infringement on the specified rights and legal regulations and he/she has developed all the possible efforts that may reasonably be required from him/her to make sure that his/her registered Domain Name does not infringe on those rights and legal regulations.

15.2. The Holder is liable for damages caused to the CZ.NIC Association by providing the CZ.NIC Association with wrong or misleading data or by using his/her Domain Name in a way that contravenes the Rules of Registration or infringes on third persons’ rights.

15.3. The CZ.NIC Association does not check the correctness of an application for registration of a Domain Name in terms of rights or rightful interests of third persons.

15.4. The Holder acknowledges that registration of a Domain Name does not constitute protection from third parties’ objections against registration or using a given Domain Name.

15.5. The CZ.NIC Association is liable neither for using or misusing a registered Domain Name, nor the manner of using a Domain Name. The CZ.NIC Association, therefore, is not liable for infringement on rights to trade marks, brand names, names or business firms of third persons arising from the registration or use of a Domain Name.

15.6. The CZ.NIC Association is not responsible for the functionality of name servers allocated to a Domain Name.

15.7. All the liabilities for all damages caused by the action or inaction of the CZ.NIC Association to the Holder in connection with one Domain Name is limited to an amount of CZK 250,000. ...

17. Solving disputes

17.1. The Holder is obliged to develop all the possible efforts he/she may reasonably be required to develop to peacefully settle disputes concerning Domain Names or their registrations, which may arise between the Holder and other persons.
17.2. If the parties in dispute do not solve a dispute peacefully, they are completely free to solve their dispute in the framework of valid legal regulations, which is to say, through arbitration or general courts.

17.3. If requested by all the parties in dispute, the CZ.NIC Association will act as a mediator in peacefully solving their dispute.

17.4. If a Holder and the CZ.NIC Association do not settle a mutual dispute concerning a Domain Name, any of the parties may submit the dispute for decision to an arbitrary court of the Economic Chamber of the Czech Republic and the Agrarian Chamber of the Czech Republic. The arbitration will be executed by three arbitrators in Prague, in the Czech language, in accordance with an order of the specified arbitration court. The arbitration award is final and binding for the contracting parties.

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

Some organisational activities are being prepared within the scope of the Security Research of the Ministry of the Interior for the years 2007–2010 (establishing of the CERT.cz, educational campaigns for public officials and the wider public, etc.).

C. International co-operation

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

The Czech Republic fully supports the idea of better co-operation between Council of Europe member states in the sphere of the fight against cybernetic threats.

The Czech Republic welcomes any activities that would enhance the fight against terrorism. The initiative “Check the Web”, kicked-off by the Federal Republic of Germany, is a good example of how to deal with the current problem of the misuse of the Internet by terrorists and how to coordinate and enhance the effectiveness of police work in this area.

The initiative of France to create platforms for reporting the presence of illicit content on the Internet is currently being discussed.

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?

According to the Council of Europe Cybercrime Convention, the police of the Czech Republic act as the direct international co-operation contact point. Since November 2004, the criminal police of the Czech Republic also act as the 24/7 contact point for international communication. In the course of 2005, there were 42 urgent cases requiring international co-operation (especially regarding phishing attacks – fake pages or advertisements from banks, etc.).

D. Institutional framework

11. Please list the institutions that are competent for countering terrorist misuse of cyberspace.

During 1999, a specialised group for the fight against computer crime (high-tech crime) was created within the Office of the Service of the Criminal Police of the Police Presidium. This group is now called the "Information Crime Group" ("Skupina informační kriminality", SIK). The activity of the Group is especially focused on:
- detection and clarification of intellectual property crime (with the use of information technologies);
- detection and documentation of computer crime (high-tech crime), and initiation of criminal proceedings in the respective area;
- developing conditions for the police of the Czech Republic to fight these forms of crime;
- co-ordination of the regional units of the Criminal Police and Investigation Service and the provision of methodical support for such units;
- active steps in the area of educational activities for police officers at the regional and district levels and also within the framework of the special units of the police of the Czech Republic;
- co-operation with bodies involved in the fight against computer crime (high-tech crime) outside the Police;
- analysing the reasons and conditions leading to the commission of computer crime (high-tech crime) and submitting proposals for its reduction;
- serving as a national contact point for the computer crime (high-tech crime) agenda.

Between 1996 and 1998, workplaces were established in all of the regional Criminal Police branches for forensic technical expertise. This step was necessary because of the increase in the number of relevant cases, which was interconnected with the ever-increasing occurrence of the criminal misuse of information technologies.

This phenomenon is also investigated by the Police’s Unit for Combating Organised Crime.

The Forensic Institute Prague was the first place in the Czech Republic to deal with the agenda of computer crime (high-tech crime) in terms of securing evidence via forensic research. A workplace was established between 1990 and 1993 and was recently transformed into the Computer Expertise Department of the Forensic Institute.

The Police Academy of the Czech Republic is, in the context of its research activity, responsible for dealing with criminological issues in the detection, investigation and prevention of computer crime (high-tech crime). Within the framework of this activity the Police Academy also publishes expert journals and produces research studies related to the issue of computer crime (high-tech crime).

Other institutions worth mentioning in this context are specialised academic and private facilities which provide certain types of "service" or specific know-how to the security community of the Czech Republic (e.g. the activity of court experts). It is important to establish links between all of the respective scientific areas involved in the analysis of cybernetic threats (especially the legal and social science specialists).

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

It is important to state clearly that the fight against the numerous aspects of the cybernetic threats in the Czech Republic cannot be effectively won without the active participation of high-profile experts from the non-public sphere (especially academic).

A number of the academic and private research facilities already existing in the Czech Republic are engaged in the fight against computer crime (high-tech crime). Co-operation between such platforms with their public counterparts can be helpful for all the parties involved.

Some private and academic bodies are currently involved in research projects co-ordinated by the Ministry of the Interior (for the period 2007-2010). Some other similar projects are currently in progress (or are being prepared) by the police of the Czech Republic and by the intelligence services of the Czech Republic.

The most suitable systematic solution to the current situation in this area could be the establishment of a specialised "Centre for the Fight against Cybernetic Threats". Such a body would gather highly developed technical capacities together with qualified experts from various
areas of specialisation (IT studies, sociology, psychology, law studies, forensics, security studies) that relate to the issue of securing the cybernetic security of the State.

Aside from difficulties related to personnel, it is apparent that what is typical for the security community in the Czech Republic is (in most cases) the lack of specialised equipment (specialised and certified software, modern specialised hardware, etc.).

Only a small number of the members of the police (and of the intelligence services) are educated in the area of information and communication technologies in general. However, they can hardly acquire such knowledge, for various reasons (especially because of its specific nature), in an institution that does not fully reflect the needs of law enforcement authorities. Police educational capacities are far from coping with this problem either.

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.).

No such cases have been reported.

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 Ministry of the Interior is currently studying such topics within the framework of its research project. The results will not be available until the end of 2008.

The current (2007) level of danger in the Czech Republic related to cybercrime can be described in the following way:
- The number of incidents, motivated by an increase in the "prestige" within the community of hackers (for example defacement) is decreasing. Among those on the increase (or which are generally supposed to be) are especially hidden profit-motivated incidents.
- The number of high-tech specialists that are ready to be hired by criminals is also on the increase.
- An increase in the distribution of harmful or illegal content (computer programs, movies, music, prohibited forms of pornography and extremist propaganda) via the Internet has been reported.
- Cases of the misuse of phone lines for the unauthorised re-dialling of Internet end-users are still being recorded.
- An increase has been reported in the misuse of Internet sales.
- There were cases recorded of "sophisticated" misuse of Internet banking.
- One new phenomenon seems to be "phishing" (various forms of unauthorised gathering of sensitive data).
- The number of misused or forged credit cards and cheques, elaborated (originally issued) abroad, is steadily increasing. Also, the so-called "skimming" of credit cards is frequent.

All the above-mentioned activities are of a very latent nature. It is difficult to collect enough evidence to commence a trial in such cases.