CZECH REPUBLIC

April 2007 www.coe.int/gmt

CYBERNETIC THREATS: CHALLENGES FOR THE MODERN SOCIETY

Summary

The paper deals with the role of the information technologies and to them related criminal phenomenon in the modern society. It discuss also the possibilities of the misuse of the cyberspace from the side of crime, describes the motives and socio-psychological profiles of the perpetrators of the cybernetic crime and basic typology of the illegal activities within the cyberspace.

It also handles with the perspectives of the information technologies in conducting the cyber-war in the global cyberspace and the misuse of the information technologies by the terrorist groups.

The paper also analyses the cybernetic threats in the Czech Republic and the level of the protection against them (framework of the respective activity, organisational measures). Finally are listed some proposals of the measures for solving the actual situation and the possible ways of how to put such an ideas into the life.

1. Role of the modern technologies in the modern society[1]

Basic technological breakout, connected with the respective agenda, was the invention and spreading of the personal computers itself (with special regard to the creation of the computer networks that enables the distant access to the respective databases). For the modern society are typical following facts:

- There is reported constant growth of the extent and importance of the elaborated, transmitted, shared a stored data.
- Potential collapse of the computer industry would endanger the further development of the world economy at all.
- Internet is used not only as a working instrument, but becomes a part of the daily life of the modern man.
- The governments in the modern world are interested in the creation of the equal conditions and opportunity for social inclusion of the all group of the inhabitants into the society. It is described as a concept of so called e-inclusion (use of the modern technologies for realization of the equality of opportunities principle).
- Almost every employee, in various positions, are asked to be able to operate the modern computer and communication technologies.
- Modern technologies may cause the new opportunity for creation of the modern and efficient public administration (so called e-government).
- Modern society dependent on the information and communication technologies.

[1] http://www.ftc.gov/bcp/conline/edcams/infosecurity/popups/safesurf_quiz.html (Are You a Safe Cyber Surfer?) http://www.ndu.edu/inss/actpubs/dcom/dcomcont.html (Libicki, M., C., Defending Cyberspace and Other Metaphors, NDU Press Book, 1997.)

2. How can be the modern technologies misused by the criminal structures?[2]

The rise of use of the modern technologies in the day to day life goes hand in hand with the misuse of such instruments:

- Ability of the criminals to recognise new opportunities for illegal activities, as well as their ability to use the modern technologies in general, is on the increase.
- Perpetrators misuse the modern technologies to reach the better level of cooperation and to extend the scope of their activities, or to reduce the risk of being disclosed.
- Act, that can be committed in some "traditional way", is also possible to commit with use of the modern technology, but with more devastating effect, with better probability of success.
- Cybernetic crime can be described as a typical "white collar crime".
- It is important to mention the high level of latency of such a type of crime.
- Many institutions prefer not to report the respective attack; being afraid of the withdrawal of the customers (it plays a role especially in the cases of financial institutions).
- Damages, caused by the cybernetic incidents, are possible to be estimated as a damages, caused by the large scale natural disasters.

3. Why is the cyber criminality so attractive?[3]

Modern (information and communication) technologies are characterised by many characters that represent advantages not only for the blameless user, but also for criminals (and mostly posses disadvantage for the specialised security forces):

- **They make possible global accessibility.** It helps to increase the distance between the criminal and victim and makes possible that an attacker could accomplish his activity from distant place.
- It makes possible to criminal groups very quickly transfer (copying, destruction, modification) of large amounts of data.
- **They ensure large scope of anonymity.**
- The prices of the computer facilities constantly decreases, so they are much more available for ever broader group of people. Such technologies also more and more user-friendly.
- **The asymmetry between the attackers and defenders is huge.** Attacker is always the one, who choices the target, as well as the moment and method of the attack. Respective countermeasures are, on the other hand, very expensive.

Computer and informatics crime is beside current searching procedures:

- Digital traces are highly voluminous, very variable and can be distributed on a large geographical area (they are "everywhere and nowhere ").
- Damages, caused by the cybernetic incidents, are hard to detect or figure out (especially according to the topic of intellectual property).
- Low level of acceptance of the digital traces is, unfortunately, one of the rules in the legal praxis.

4. Modern technologies and the terrorism or interstate conflicts[4]

---

[2] Brzybohatý, M., O terorismu; in: Brzybohatý, M. (ed.), Terorismus a my, Computer Press, Praha 2001, str. 15.
Hos, M., Terorismus a počítače; in: Brzybohatý, M. (ed.), Terorismus a my, Computer Press, Praha 2001, str. 54.
Jeger, D., Novodobé bezpečnostní hrozby; in: Computerworld, Speciál Bezpečnost, 2006, str. 10-12.
Požár, J., Trendy počítačové kriminality a kyberterorismu.
Rak, R., Trendy rozvoje technologicky orientované trestné činnosti v digitálním prostředí; in: Bezpečnostní teorie a praxe, 2 / 2005, str. 117-132.
Rak, R.; Porada, V., Charakteristiky a specifika digitálních stop; in: Bezpečnostní teorie a praxe, 1 / 2005, str. 71-84.
http://www.contactel.cz/script/2_servbasic.asp?rid=193 (Bezpečný Internet, kampaň firmy Contactel)

[3] Lewis, J., A., Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats, CSIS, 1 / 2002.
http://207.25.71.25/2000/tech/computing/01/02/cyberterrorism/ (Governments Ready to Fight Cyber-Crime in New Millennium, 2. I. 2000)
http://www.cs.georgetown.edu/~denning/crypto/cases.html (Denning, D., E.; Baugh, W., E. Junior, Cases Involving Encryption in Crime and Terrorism, 10. X. 1997.)
http://www.securityaffairs.org/issues/2005/08/weimann.php; http://www.usip.org/pubs/specialreports/sr116.html (Weimann, G., How Modern Terrorism Uses the Internet.)

During the last 20 years many companies introduced so called "Digital Control Systems" (DCS) a "Supervisory Control and Data Acquisition Systems" (SCADA), that serve to control key operation and function of cyberspace (that was necessary by then to do manually). DCS/SCADA use Internet for the data transmition more, than the networks for use of the individual households. **Collapse of the control system would imply immense consequences for "non-cyber" parts of critical infrastructures of many countries.** Large scale cybernetic attack can limit the possibility of use of the telephone network, including the emergency call services.

Handful of specialists can, with just a small expenses, to damage economy of technically advanced country to such extent that its recovery could require years. **Without cyberspace protection may vanish effects of many other partial security strategies**.

Cybernetic attack can simultaneously affect many victims on the distant locations in the world. Such an scenario is very attractive not only for terrorist groups but also for independently operating blackmailers.

Many countries already today intensively elaborate the concept of the information war. Some countries do know, that are unable to succeed in standard military conflict with most developed countries. Info-war is personally and materially relatively unpretending asymmetrical strategy whereas unidentified or surprising attack through the Internet could undermine striking power of the appreciably stronger and richer opponent.

Internet also provides equally quite extraordinary possibilities to extremists and terrorists groups and individuals, especially because of its ability to enable:

- Fast and relatively concealed communication.
- Spread of propaganda, acquisition and mobilisation of new followers and supporters.
- Information gathering, including the data about the potential targets of the respective attack.
- Distribution of the manuals for elaboration of the improvised weapons.

Internet and modern information and communication technologies generally enable for the terrorists creation of the global organization networks of new nature.

Almost all the terrorist group in the world run their web pages. Among them is possible to find the presentations, focused on women and children (e. g. fairytales or comics, describing the stories of the suicidal bombers). Frequently registered phenomenon of these days is so called "**self-radicalisation**" and "**self-training**" of individuals or small independently acting groups. Such person plan, prepare or commit attack (does not matter, whether of the "classical" or "cybernetic" nature), without directly contacting the ideological leaders of the network, they declared to be a part.

Monitoring of such a pages from the side of the law enforcement authorities is unimaginable expensive.

5. Basic characteristic of the current cybernetic criminality threat in the Czech Republic

The Czech Republic definitely can not be understood as a safe haven, unattached by the politically motivated cybernetic accidents. Domain ".cz" was in the recent years exposed to many

---

[4] Americká policie varuje před digitálním Pearl Harborem; in: LN, 17. XI. 1999.
Jeden reálný scénář soudného dne Ameriky; in: HN, 8. II. 2006.
Lewis, J., A., Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats, Center for Strategic and International Studies, 2002.
Pacner, K., Teroristé mohou zničit elektronickou síť; in: MFD, 4. IX. 1999, str. 1.
Petráček, Z., Teroristé na Síti: Jaká rizika přináší Internet a jak se jim můžeme bránit; in: Respekt, 9. IX. 1996, str. 9.
Požár, J., Trendy počítačové kriminality a kyberterorismu.
Stöckl, P., CIA se obává elektronického úderu; in: MFD, 26. VI. 1998, str. 1.
Stöckl, P., Počítačoví piráti se dostali k satelitům; in: MFD, 23. IV. 1998, str. 8.
Vrána, K., Virtuální peklo, nebo ráj?: Počítačoví záškodníci útočí ze zábavy, kvůli penězům also politickým cílům; in: Týden, 26. III. 2001.
http://www.cs.georgetown.edu/~denning/crypto/cases.html (Denning, D., E.; Baugh, W., E. Junior, Cases Involving Encryption in Crime and Terrorism, 10. X. 1997.)

attacks (e. g. during the IMF/WB summit in Prague 2000, or NATO summit Prague 2002). As far as 50 % of authors of cyber crimes (especially hackers) declare more or less clean-cut political motivation of their activities. Some hacker groups as for example "Dark-Underground" or H131 declared political motivation of all their attacks.

Such an fact remains long time aside from the public concern. Already recent acquisitive-motivated incidents attracted the public attention to necessary investment into cyber security.

Current (November 2006) level of the endangerment of the Czech Republic from the side of cybernetic criminality is possible to describe following way:

- The perpetrators of the various types of crime misuse increasingly information technologies.
- Number of cybernetic accidents of all kind is on the increase in the Czech Republic (as well as of the hard figures and the seriousness of the cases).
- The number of the incidents, motivated by the increase of the "prestige" within the community of hackers (for example defacement) is decreasing. Among those on the increase are (or they are generally supposed to be) especially hidden profit motivated incidents.
- As well, the number of the high tech specialists, that are ready to be hired by the criminals, is on the increase.
- There is reported ever-increasing presence of the harmful or illegal content that is distributed via Internet (computer programs, movies, music, prohibited forms of pornography and extremist propaganda).
- Cases of the misuse of the phone lines for unauthorised re-dial of the Internet end-users are still being recorded.
- There is increase reported of the misuse of the Internet sale.
- There were cases recorded of the "sophisticated" misuse of the Internet banking (esp. "phishing", various forms of the unauthorised gathering of the sensitive data, "skimming" of the credit cards).
- All the above mentioned activities are one of the very latent nature. It is difficult to collect enough evidence to commence a trial in such cases.

6. Governmental strategies

The Government of the Czech Republic, with its aim to maximise the potential of the modern information and communication technologies, decided to find the new definition of its objectives in the area of the so called "information society" and in the area of telecommunication - and to formulate the new state strategy for the coming period.

As opposed to the former attitude where both concepts were elaborated separately (documents "State Information Policy: Toward Information Society" and "National Telecommunication Policy"), the Government now decided to respect the close interconnection and general trend of the convergence of both respective areas and to create one common strategic document, called **"State Information and Communication Policy: e-Czech Republic 2006"**. The name of the document itself also reflects the transformation of the former branch of *telecommunication* in the branch of *electronic communication*.

With the goal of **strengthening the information security in the sphere of 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 in the sphere of the protection of public administration information systems of the Czech Republic were drafted, even from the viewpoint of their possible menace by 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 conditions of the Czech Republic.
- Draft directive of the government for fulfilling tasks set by the "National Strategy of Information Security of the Czech Republic" on the part of public administration authorities and organisations and subjects of critical infrastructure.
- "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.[5] The document proposes a solution via integration of the information systems into a universally usable secure public administration communication system providing the access to networks of other countries of the European Union.
- "Security Policy of Transfer of Classified Information by the Czech Republic's Public Administration Communication Infrastructure" describing, in compliance with the Resolution of the State Security Council No. 84 of 18 November 2003, the security goals of the public administration communication infrastructure and the methods of their meeting, as well as the basic management structures of the system, their role and the area of responsibility during enforcing the afore-mentioned security principles. The content of the document is conceived so that the resulting system met security requirements of the EU communication system S-TESTA and the Czech Republic's crisis management information systems.
- "Proposal of Protection Levels of the Information Systems Necessary for 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.

7. Strategies of the Ministry of Interior

In October 2000 the Government of the Czech Republic approved **"Updated Strategy for Combating Organised Crime"**. Following the schedule of tasks specified in the Annex to the Government's resolution, the Minister of the Interior was assigned the task to "*implement an ongoing strategy for combating organised criminal activities in the area of information technologies*".

That was the reason, why the Ministry of Interior elaborated document, called **"Strategy of the fight against information technology crime"**, based on the respective outcomes of the police work in the respective area. **The Minister of Interior approved the Strategy on 5 June 2001**. Currently is prepared the current wording of the Strategy.

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

- To ensure conditions for the further development of the structures those are directly engaged in the detention of high-tech crime, especially the specialised Police units.
- To spread and support the co-operation between the law enforcement agencies and the intelligence services and NGO's, involved in the fight against some aspects of the high-tech crime.
- To elaborate the principles of the protection of the state and some strategically important non-state information systems.
- To elaborate the project of the alert system in the area of the high-tech crime.
- To elaborate the project in the area of the education of the personnel of the law enforcement bodies in the area of the high-tech crime.
- To develop and to set up forensic standards for seeking and verification of the electronic data during the criminal investigation and criminal procedure.
- To support the independent research, public-relations and statistics activities in the area of the fight against high-tech crime.
- To promote the public awareness campaigns, focused on the recommended behaviour in the cyberspace.
- To monitor the respective international activities an to participate on them.

8. Organisational framework of the fight against computer crime (high-tech crime) in the Czech Republic.

Organisational framework of the fight against computer crime (high-tech crime) in the Czech Republic is possible to describe as follows:

[5] Quantity of these regulations and inconsistencies in their interpretation lead to projecting and developing many intentionally directed and interdependent systems.

During the year 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 of the Czech Republic, this group now being called the "Information Crime Group"

Within the years 1996 - 1998 the workplaces for the forensic technical expertise were established within all of the regional Criminal Police branches. This step was necessary because of the increase in numbers of the respective cases, which was interconnected with the ever increasing occurrence of the criminal misuse of the information technologies itself.

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

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

Another capacities, that are worth mentioning in this context, are the specialised academic and private facilities, able to ensure some forms of "service" or specific know-how for the security community of the Czech Republic (e. g. the activity of the court experts).

It is important to establish the links between all of the respective scientific areas that can be involved into the analysis of the cybernetic threats (especially the legal and sociological specialists). Important role in the abovementioned framework would also play so called Public – Private Partnership activities.

Aside of the personnel difficulties it is apparent that what is typical for the security community in the Czech Republic is:

- **Lack of specialised equipment** (specialised and certified software, modern specialised hardware, etc.).
- Fact that only a small number of the members of the Police of the Czech Republic who are educated in the area of information and communication technologies in general. Police educational capacities are far from coping with this problem as well.
- **Interconnection between numerous relevant intra-community databases is not sufficient.**
- The public sphere can hardly understand, how important is to invest into the security measures in the cyberspace.[6] Without exaggeration, it is possible to mention, that investing into the security of the cyberspace can anticipate several time larger costs (damages) in the future**.**
- *There does not exist some body (organisation), which can be understood as a neutral and trustworthy platform (counterpart) for the public sphere, able to provide required service for the respective security forces.*

9. Investing into the future of the Czech Republic

Remaining gaps in this area lie in the prevailing non-uniformity of the **above-mentioned academic and other facilities. This leads to a situation where a number of research institutions develop one and the same research area in duplicate forms. In spite of that the public sector (security community) is still in urgent need of a partner who can offer all of the advantages of the academic approach and who would at the same time be able to comply with the requirements resulting from the tasks that the security community has to face on the daily basis.**

From the structural and technical viewpoint (especially in the area of police investigation), most suitable would be that the issue of fight against computer crime (high-tech crime) is dealt with by experts that are in particular:[7]

[6] Only exception was the Y2K campaign in the ewe of the year 2000.
[7] With respect to the context of the material the section focuses predominantly on organisation area.

- well educated;
- technically equipped;
- able to identify the (potential and real) criminal act and ensure appropriate evidence that could be used in further proceedings;
- are able to identify the offender, arrest him of facilitate his arrest;
- are able to co-operate with the non-public sector and with the public sector itself;
- are able to co-operate with the foreign counterparts (on the precondition of their language skills, especially English).

Finding solutions to such a situation, even with the use of – for example – the police educational system – does not seem to be feasible (and not only because of the level of wages in the public sector). Top experts having interdisciplinary knowledge (from information technologies down to security information systems and law studies) are the area, which from the long-term perspective, the public sector in the Czech Republic will be prevailingly lacking.

Such situation causes – on the one hand – obvious burdening of the respective bodies and, – on the other hand – their incapability to deal with all cases, be them the most serious. What arises as a result of this situation is often undesired media publicity of particular cases (for example in the area of child pornography), where it is especially Police of the Czech Republic who is groundlessly accused of inactivity, etc.

To ensure, that the fight against computer crime (high-tech crime) will be successful, it is also important to ensure appropriate legislative, organisational and technical framework for such activities (including the respective International co-operation).

Above mentioned facts (personal, material and technical weaknesses, complications in implementation of the relevant domestic and international documents, splitting of existing capacities of the public and academic sphere, other obstacles, etc.) are closely interconnected. That is why a complex and comprehensive approach in finding solutions would be more than welcome.

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

In the Czech Republic there is a number of academic or private research facilities already existing that are engaged in the area of the fight against computer crime (high-tech crime). The co-operation between such platforms with the public counterparts can be helpful for all the sides involved.

The Czech Republic is a homeland of many top experts, but also have to pay attention whether the respective experts don't give precedence to the more honesty engagement abroad.[8]

[8] Reference: Počítač pozná, jakou řečí mluvíte; in: Hospodářské noviny, 23. II. 2006
Špión z brněnské techniky; in: HN, 5. VI. 2006, str. 17, 21.
Čechová, Š., Mladí čeští vědci slaví úspěch na mezinárodní scéně; in: ČRo 1 – Radiožurnál, 10. VII. 2006.
Bednářová, Š., VÚT v Brně uspělo s programem na rozeznávání hlasu; in: ČT 24, 10. VII. 2006.
Fila, M.; Malý, P., VÚT v Brně uspělo s programem na rozeznání hlasu; in: ČT 1, 10. VII. 2006.
Petrucha, D., Vědci z Brna vyvinuli program na rozpoznávání identity mluvčího; in: ČTK, 10. VII. 2006.
"Kdopak to mluví?", to vědí v Brně; in: LN, 12. VII. 2006.
Program nejlépe na světě pozná, kdo volá; in: Rovnost - Brněnský deník, 11. VII. 2006.
Poznají hlas člověka v telefonu mezi desetitisíci volajících; in: Právo, 11. VII. 2006.

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

Such a step (creation of a Centre) is the basic outcome of the document, elaborated within the framework of the Ministry of Interior, called **"The Analysis of the Actual Level of Securing Cybernetic Security of the Czech Republic"**, that was discussed at the inter-ministerial level and currently is prepared for the discussion within the National Security Council.

Activities of the Centre will not be primarily focused on the "**passive**" defence of the cyberspace and databases (it means the waiting for the certain attack against secured networks, operated by the public authorities). Proposed Centre is understood as a **proactive platform** (that will not in fact analyse the "security" but "in-security", including the applied research, competition for supranational grants, simulation of even hypothetical scenarios of cybernetic attacks, etc.), that provides logistic service also for the subjects outside the public sphere.

All the agenda has to be understood as interconnected to other parallel intra-community activities, especially:

- Activities within the framework of the *Security Research of the Ministry of Interior* for the years 2006 – 2010 (especially sub-projects II.7: "Overcoming of the Language Barriers, Complicating the Investigation of the Financing of Terrorism and other Serious Crime"; II.21: "Information Support in the Latent Internet Crime Prevention and Detention"; XXII.: "Agenda of the Cybernetic Threats from the Perspective of the Security Interests of the Czech Republic").
- Other activities (activities in the area of the fight against extremism and the fight against child pornography, or commercial sexual exploitation of children as such).
- In the international context it is important to mention the European Union initiative, called "Check the Web".

It is important to invest into the cybernetic security of the Czech Republic. Other attitude would surely cause large scale losses, including the possible endangerment of the state economy.

Such a step has to be understood as a very likely as a returnable investment. It also can play a role according to the possible utilising of the European Union sources (esp. within the framework of the newly created priority budgetary chapter "Security and Space", that is strongly supported).

Investing into the measures, focused on the fight against cybernetic threats against the interest of the Czech Republic is without hesitation one of the most crucial and most returnable investment step in the security area of the Czech Republic at all.

Doc. Ing. Václav Jirovský
Charles University, Faculty of Mathematics and Physics, Charles University

RNDr. Václav Hník, CSc.
Ministry of Interior of the Czech Republic, Security Policy Department

Mgr. Oldřich Krulík, Ph.D.
Ministry of Interior of the Czech Republic, Security Policy Department