UNIVERZITA PARDUBICE

FAKULTA EKONOMICKO-SPRÁVNÍ

Globální informační společnost a rizika z toho plynoucí – vliv bezpečnostní koncepce a bezpečnostní politiku

Miroslav Kmec

Bakalářská práce

2009

Univerzita Pardubice
Fakulta ekonomicko-správní
Ústav systémového inženýrství a informatiky
Akademický rok: **2008/2009**

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Miroslav KMEC**
Studijní program:	**B6209 Systémové inženýrství a informatika**
Studijní obor:	**Informační a bezpečnostní systémy**
Název tématu:	**Globální informační společnost a rizika z toho plynoucí – vliv na bezpečnostní koncepce a bezpečnostní politiku**

Zásady pro vypracování:

1) Charakteristiky globální společnosti;
2) Vliv globalizace na konkurenční boj – detektivní a zpravodajská ochrana ekonomických zájmů podnikatelských subjektů a jejich aktivit;
3) Charakteristika globalizace v informační společnosti –informační válka, počítačová kriminalita;
4) Charakteristika globalizace v oblasti zločinnosti – korupce, drogová kriminalita, organizovaný zločin, kyberterorismu, terorismus;
5) Vlivy globalizace na bezpečnostní situaci (nebezpečí, rizika, hrozby, ohrožení);
6) Bezpečnostní analýza, bezpečnostní prognóza jako určující determinanty pro tvorbu bezpečnostních koncepcí a bezpečnostní politiku;
7) Provázanost bezpečnostních koncepcí státního, komunálního a soukromého bezpečnostního subsystému – vztah systému bezpečnostní politiky a institucionálního bezpečnostního systému;

Rozsah grafických prací:

Rozsah pracovní zprávy:

Forma zpracování bakalářské práce: **tištěná**

Seznam odborné literatury:

1) **MAGAZÍN SECURITY: časopis pro vaši bezpečnost. Č. 1 (leden/ únor 2007) Praha: FAMILy media, spol. s.r.o. 2007. Vychází 6x ročně. ISSN 1210-8723**

2) **MAGAZÍN SECURITY: časopis pro vaši bezpečnost. Č. 2 (březen /duben 2007) Praha: FAMILy media, spol. s.r.o. 2007. Vychází 6x ročně. ISSN 1210-8723**

3) **ISLÁM V EVROPĚ - obohacení, nebo nebezpečí? : sborník textů / Benjamin Kuras ... [et al.] ; editorka Dina Chmaitilliová. 1. Vydání. Praha: Centrum pro ekonomiku a politiku, 2006. ISBN 80-86547-53-1**

4) **FRYŠAR, Miroslav. Bezpečnost pro manažery, podnikatele a politiky. 1. Vydání. Praha: Public History, 2006 . ISBN 80-86445-22-4**

Vedoucí bakalářské práce: **doc. Ing. Pavel Petr, Ph.D.**
Ústav systémového inženýrství a informatiky

Konzultant bakalářské práce: **JUDr. František Brabec**
Ústav systémového inženýrství a informatiky

Datum zadání bakalářské práce: **6. října 2008**

Termín odevzdání bakalářské práce: **1. května 2009**

doc. Ing. Renáta Myšková, Ph.D.
děkanka

L.S.

doc. Ing. Jiří Křupka, Ph.D.
vedoucí ústavu

V Pardubicích dne 6. října 2008

Prohlašuji:

Tuto práci jsem vypracoval samostatně. Veškeré literární prameny a informace, které jsem v práci využil, jsou uvedeny v seznamu použité literatury.

Byl jsem seznámen s tím, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorský zákon, zejména se skutečností, že Univerzita Pardubice má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle § 60 odst. 1 autorského zákona, a s tím, že pokud dojde k užití této práce mnou nebo bude poskytnuta licence o užití jinému subjektu, je Univerzita Pardubice oprávněna ode mne požadovat přiměřený příspěvek na úhradu nákladů, které na vytvoření díla vynaložila, a to podle okolností až do jejich skutečné výše.

Souhlasím s prezenčním zpřístupněním své práce v Univerzitní knihovně.

V Rychnově nad Kněžnou dne 19. 8. 2009

Miroslav Kmec

Poděkování

Na tomto místě bych rád vyjádřil poděkování doc. Ing. Pavlu Petrovi, Ph.D. za poskytnutí cenných rad a odbornou pomoc při zpracování tématu. Dále bych rád poděkoval JUDr. Františku Brabcovi za poskytnuté materiály.

Souhrn

Bakalářská práce je věnována globální informační společnosti a rizikům z toho plynoucím. V úvodní části se zabývá pojmem a charakteristikou globální společnosti. Další část je věnována vlivu globalizace na konkurenční boj.

Následující části se zaměřují na globalizaci a její vliv na informační společnost, včetně počítačové kriminality a jejího členění. Další části popisují vliv na oblast zločinnosti, výčet nových typů trestné činnosti a jejich možné prevence. Poslední část práce je věnována závislosti globalizace a bezpečnostní situace a výčtu možných hrozeb z hlediska vývoje.

Klíčová slova

Informační globální společnost, globalizace, informační válka, počítačová kriminalita, terorismus, bezpečnostní politika, konkurenční zpravodajství, organizovaný zločin

Title

Global information society and the risks resulting from this – the impact of the security concept and security policy

Abstract

Bachelor's thesis is devoted to the global information society and their risks. The introductory part deals with the concept of global characteristics. Another part is devoted to the effects of globalization on competition.

The next sections focus on globalization and its impact on info-society, including cyber crime and its breakdown. Further description goes to continuing impact on area crime, new types of crime and their prevention. The last part is devoted to work, depending globalization and security situation and the list of potential threats in terms of time.

Keywords

Global information society, globalization, information warfare, cyber crime, terrorism, security policy, competitive intelligence, organized crime

Obsah

Úvod

Cílem bakalářské práce je seznámit čtenáře s globální informační společností, vlivem bezpečnostní koncepce, bezpečnostní politikou a riziky z toho plynoucími. Zaměřil jsem se na vlastní pojem globalizace, na vztah mezi tímto pojmem a naším každodenním životem. Je proto nutné zmínit charakteristiky globální společnosti, názory na jejich vliv na okolní svět a náš každodenní život.

Globalizace má však vliv na ekonomiku, nerovnováha v některém ze států se přenáší do států dalších, a z tohoto hlediska se zabývám konkurenčním bojem, který současně rozvíjí i jiné ekonomické aktivity, umožňuje rozkvět detektivních a zpravodajských služeb. Ty tak ochraňují ekonomické zájmy podnikatelských subjektů a současně umožňuje jejich rozvoj a tím pomáhají celé ekonomice.

S rozvojem moderních technologií, zejména pak počítačových a hlavně s rozvojem a rozšířením globální sítě internet, je nutné se zabývat i počítačovou kriminalitou, informační válkou a dalšími nebezpečími v informační společnosti.

Propojení světa a jeho zdánlivé zmenšení díky rozvoji dopravy a technologií působí i na rozvoj korupce a drogové kriminality. Tento posun v měřítkách pro vzdálenosti také zvětšil možnosti organizovaného zločinu.

Pozvolna dochází k posunu hranice organizovaného zločinu až na meze terorismu, za využití moderních technologií pak ke zdánlivě méně destruktivního kyberterorismu. To je však pouze zdání, díky velké penetraci informačních technologií do běžného života dokáže být kyberterorismus mnohem zákeřnější a účinnější, nežli terorismus, na který jsme byli do této chvíle zvyklí.

Globalizace zasahuje i do aktuální bezpečnostní situace. V čase se tak mění rizika dynamicky v závislosti na stupni ohrožení a hrozby a rizika se posouvají směrem ke stále nižší hranici vnímavosti. Rizika se tak s postupujícím časem transformují a tak považuji za vhodné se jimi z tohoto hlediska zabývat.

Proto, aby bylo možno těmto všem rizikům čelit, je nutné pracovat s bezpečnostními analýzami, bezpečnostními prognózami jako určujícími determinanty pro vytváření bezpečnostních koncepcí a bezpečnostní politiku, ať už se jedná o stát, nadnárodní korporaci či podnik.

Jak z výše uvedeného vyplývá, bezpečnostní koncepce jak státních, komunálních, tak i soukromých bezpečnostních subsystémů spolu úzce souvisí. Vzájemná provázanost je způsobena právě velmi úzkými vztahy globálních ekonomických prostorů, systémů a smluvních vztahů, vzájemných iterací mezi jednotlivými mezikontinentálními uskupeními a dohodami. Proto je nutné se globalizací zabývat a rozkrýt její souvislosti.

1 Charakteristika globální společnosti

V dnešní době je slovo „globální“ stále častěji skloňováno a není snad člověka na světě, kterého by se vědomě či nevědomě nedotklo.

Pojem globalizace vyjadřuje skutečnost, že kromě místní, regionální a národní úrovně organizace a integrace lidí se formuje i úroveň celosvětová, a to jako důsledek stále intenzivnější provázanost ekonomik (kultur a politik) – včetně správy a řízení procesů spjatých s globalizací. [1]

Další pojmy uvádějí, že „globalizaci“ můžeme také vnímat jako skutečnost, ve které jsme svědky vzniku celosvětové úrovně postupného a nezadržitelného procesu zcela nové kvality.

Jedná se o procesy, které směřují k rigidní celosvětové integraci a organizaci výroby – výrobních procesů, obchodu – obchodních procesů, bankovních a finančních operací, technologií a informací spjatých s fenoménem světové nadvlády nadnárodních korporací. Ty následně stále více ovlivňují a determinují globální politické procesy mezi aktéry světové politiky, zvláště pak bezpečnostní krize a rizika, světová migrace (ovlivněnou nejen populační explozí a prohlubující se nerovnováhou mezi Severem a Jihem), nová kvalita průmyslu organizovaného zločinu, řešení globální ekologické krize, akcelerující civilizační střety, úpadek dodržování lidských práv, kultury, morálek a náboženských systémů a dalších ne zcela subsidiárních problémů národních (státních), regionálních či místních systémů. [2]

Hlavním pohonem tohoto procesu je globalizace ekonomických aktivit, která zejména v posledních třiceti letech propojuje výrobu a trhy různých zemí z celého světa. Současná fáze globalizace je charakteristická nerovnováha mezi ekonomickou mocí národních korporací (ta působí na celosvětové úrovni) a jednotlivých společností: jak postmoderní společnosti jádra globalizace na Severu, tak v podstatě postkoloniální společnosti v semiperiferii a periferii globalizace na Jihu. Tyto společnosti jsou nyní organizovány u 197, suverénních „národních“ a mnohonárodních států.

Státy, které mají rozhodovací pravomoci předávat národním institucím, jsou velmi zdrženlivé. Odpor a nechuť k negativním aspektům globalizace stále více roste.

Mnoho teoretiků, kteří se problematikou globalizačních procesů v Evropě a ve světě zabývají, si uvědomuje, že vedle jejich pozitiv mají i možné negativní stránky a jistá úskalí. Např. ve svém článku Václav Bělohradský s odvoláním na sociologa J. Kellera píše: *“[...]*

příšera planetární globalizace tu zůstává, je stále dravější, nesrozumitelnější a krutější […] Globalizace pokračuje stále rychleji, neslouží žádné lidské potřebě, jen zhoubně roste. Lze tu příšeru udržet v nějakých hranicích?“. [3]

Ve zjednodušeném, zvulgarizovaném pojetí pak globalizace znamená „amerikanizaci“ kulturního života, je synonymem pro nadvládu nadnárodních koncernů a „normalizaci“ spotřební společnosti. Pozitiva a negativa globalizace a navrhovaná řešení jsou zřejmá z tabulky 1.

Tabulka 1 Pozitiva a negativa globalizace (zdroj: [2])]

Co je na globalizaci pozitivní	**Co je na globalizaci negativní**	**Navrhovaná řešení negativních dopadů globalizace[1]**
Roste nabídka a kvalita zboží	Světová ekonomika je daleko náchylnější k náhlým kolapsům (kasinová ekonomika)	Přísně regulovat činnost nadnárodních společností a bránit jejich dalšímu propojování
Klesající výrobní i prodejní ceny	Rozdíly mezi chudým Jihem a bohatým Severem jsou největší v historii a stále rostou	Omezit spekulativní toky kapitálu
Vznikají nové pracovní příležitosti	V chudých zemích bují hlad, války a nemoci více než dříve	Vybírat daně z kapitálových převodů a peníze rozdělit chudým zemím
Zvyšující se životní úroveň v rámci „konzumního způsobu života“	Reste ekonomická a politická migrace a xenofobie	Zrušit mezinárodní finanční instituce (MMF a SB) a nahradit je novým uspořádáním v podobě světového finančního parlamentu
Je daleko širší a svobodnější přístup k informacím (informační demokracie)	V zemích Severu se prohlubují rozdíly mezi nejvyššími a průměrnými příjmy (mizí „střední“ třída)	Zpřísnit pravidla pro ochranu životního prostředí a ekonomický růst podřídit pravidlům trvalé udržitelnosti
Rozšiřující se možnosti komunikace (informační a vzdělanostní společnost)	Zvyšuje se ekonomický a politický vliv nadnárodních společností (nedostatek legitimity globálních autorit)	Rozpoutat revoluci za svržení světového kapitálu
Tlak na globální spravedlnost a univerzalitu lidských práv	Zhoršuje se životní prostředí, rozšiřují se pouště	Atd.
	Akcelerují se civilizační střety (clash of civilizations)	
	Krize náboženských systémů	
	Umožňuje se globální zločin, roste terorismus, extremismus	

[1] Některá typická hesla „odpůrců globalizace“ při demonstracích v Praze ve dnech 26. – 28. září 2000 proti Výročnímu zasedání Mezinárodního měnového fondu (International Monetary Fund) a Skupiny Světové banky (World Bank Group).

2 Vliv globalizace na konkurenční boj

V současné době je stále aktuální téma efektivita a konkurenceschopnost české ekonomiky v podmínkách Evropské Unie a z pohledu její globalizace. Hlavní příčiny, zda je efektivní či neefektivní, konkurenceschopný či konkurence-neschopný, exportně-schopný či exportně-neschopný ekonomiky, závisí v samotném procesu řízení ekonomiky a jejich ekonomických zájmů. V tomto směru se hodně často zapomíná na soukromě-bezpečnostní ochranu ekonomických zájmů podnikatelských subjektů. [4]

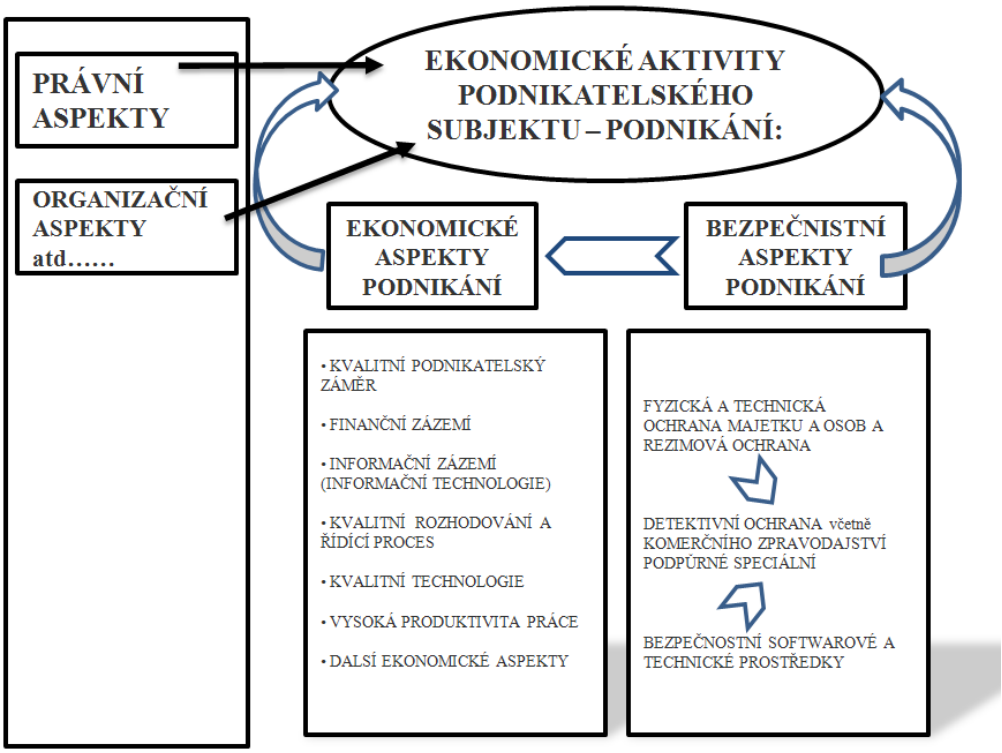
Všeobecně se dá říci, že konkurenční boj je ekonomickou válkou vedenou podnikateli, ale i národními ekonomikami, a to o zákazníky, o nové trhy a o vyšší zisky. Důležitou podmínkou úspěchu v konkurenčním boji vždy byla dobrá znalost konkurence a jejího trhu. V době kdy se konkurence odehrávala ve vymezených teritoriích, kde se konkurenti navzájem znali a kde platila neměnná pravidla, nebylo obtížné tyto informace získávat a využívat.

Dnes je však v důsledku globalizace pro kohokoliv dosažitelný jakýkoliv trh, segment zákazníků nebo obor podnikání. S tím roste množství příležitostí a hrozeb s tím spojených, složitost vztahů mezi aktéry na trhu a rychlost, s jakou se dění na trhu odehrává. Bez systematického vyhodnocování informací dnes již nikdo není schopen identifikovat využitelné příležitosti, reálné hrozby a důležité změny, natož adekvátně a včas reagovat. Proto je nezbytné se intenzivně věnovat „konkurenčnímu zpravodajství“ neboli „Completitive Inteligence“.

Pokud není podnikatelskými subjekty a jejich managementem zajištěna komplexní soukromě bezpečností ochrana a informační podpora, nelze se pak divit v jejich neúspěchy nebo malé efektivitě svých podnikatelských aktivit. Nejen podnikatelský subjekt se musí chránit proti úniku informací a hospodářské kriminalitě uvnitř svého podniku. Nejrizikovějším faktorem každého podniku je právě lidský faktor. Proto je nezbytné zajištění personální bezpečnosti. Pro svoji úspěšnost si musí podnikatelský subjekt vytvořit obranné bariéry v podobě systému komplexní bezpečnosti.

Pokud má podnikatelský subjekt nedostatek informací nebo v opačném případě nadbytek informací, jedná se o negativní vliv. Potřebuje kvalitní a relevantní informace, které jsou přeměněné ve znalosti. Aby byl podnikatelský subjekt úspěšný, potřebuje pro svou činnost management znalostí či znalostní management.

Mezi hlavní podnikatelské aktivity proto vedle ekonomických, právních, organizačních patří právě aspekt bezpečnostní (jak je znázorněno na obrázku 1).



Obrázek 1 Ekonomické aktivity (zdroj: [4])

Přehlížet význam, vliv a úlohu soukromě-bezpečnostní ochrany ekonomických zájmů podnikatelských subjektů je velkou chybou.

Vývoj po roce 1989, kdy docházelo k přechodu od „plánovité ekonomiky“ k ekonomice tržní, byl charakterizován řadou skutečností [4]:

- zahraniční kapitál a zahraniční firmy do současné doby stále vstupují na český trh a do ekonomických vztahů a to se zázemím fungujících bank, soukromě-bezpečnostní ochrany ekonomických zájmů, informací podporujících podnikatelské aktivity, s podporou Competive Inteligence a Knowledge managementem (Konkurenční zpravodajství a management znalostí),
- čeští podnikatelé a české podnikatelské subjekty postrádali, a do jisté míry stále postrádají, zázemí fungujících bank, podceňují soukromě-bezpečnostní ochranu ekonomických zájmů, málo si uvědomují význam informací pro podnikání a význam

jejích ochrany, podceňují a málo využívají konkurenční zpravodajství jako nástroj k dosažení managementu znalostí.

Aby byla soukromě bezpečnostní ochrana ekonomických zájmů účinná a efektivní, musí být komplexní a zahrnovat [4]:

- režimová a organizační opatření,
- fyzickou ochranu – ochrana majetku a osob,
- bezpečnostně technickou ochranu – zabezpečovací technika, technika k ochraně informací, dat, komunikačních a počítačových systémů, softwarové bezpečnostní technologie apod.,
- vnitřní ochranu – detektivní a zpravodajská ochrana a činnost (konkurenční zpravodajství).

Významným prvkem je detektivní nebo zpravodajská ochrana a podpora ekonomických zájmů podnikatelských subjektů a jejich podnikatelských aktivit.

Podnikatelské subjekty a jejich management se mylně domnívají, že bezpečnost svého podniku (firmy, společnosti, organizace apod.) mají zajištěnou tím, pokud nechají namontovat elektronická zabezpečovací zařízení a zajistí své objekty hlídací službou – fyzickou ochranou. To je ale pouze jedna stránky věci. Významnější je právě vnitřní ochrana, a to detektivní nebo zpravodajská. Fyzická ochrana spolu s bezpečnostní technickou ochranou (zabezpečovací systémy, alarmy) může zabezpečit podnik proti útokům zvenčí. Nezabrání však úniku informací přes lidský faktor, nezabrání nekalým praktikám zaměstnancům a manažerům. Právě to je úkolem tzv. vnitřní ochrany, detektivní či zpravodajské ochrany a podpory ekonomických zájmů.

2.1 Vnitřní ochrana

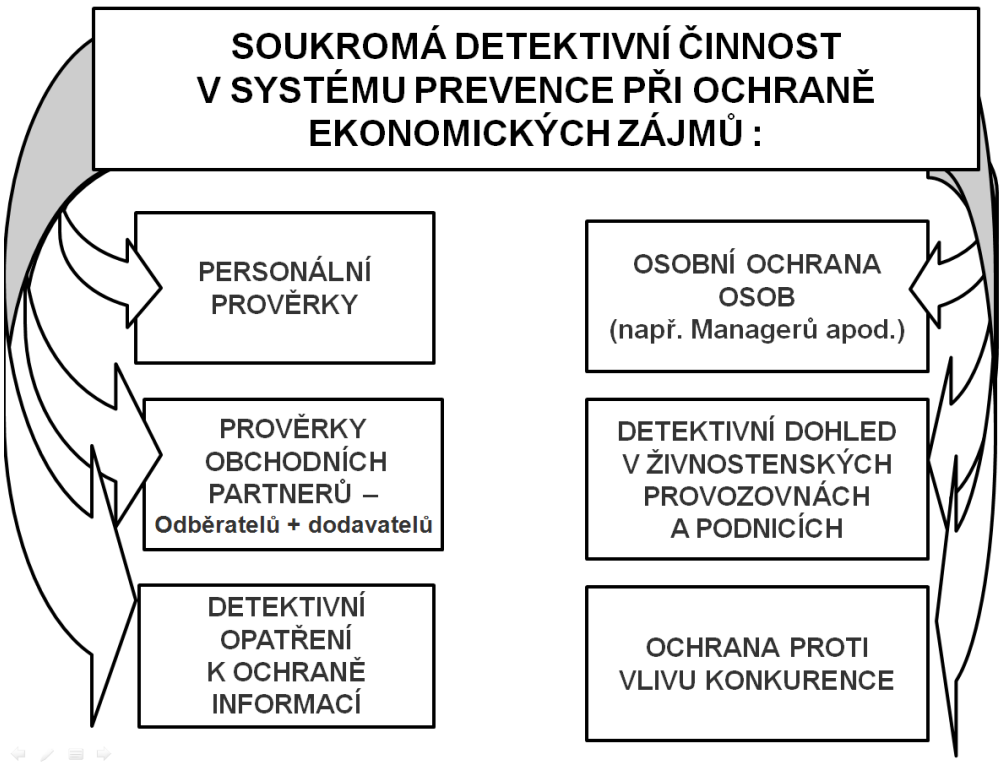
Detektivní a zpravodajská činnost na ochranu a na podporu ekonomických zájmů podnikatelských subjektů je uplatňována v několika rovinách, mezi které patří [4]:

- preventivní opatření,
- detektivní rozkrývání latentní ekonomické – hospodářské kriminality,
- shromažďování, třídění, analýza a syntéza informací.

Preventivní opatření

Preventivní opatření zpracovává interní normativní akty k zajištění organizačních a režimových bezpečnostních opatření, jejich realizaci a následné kontrole. Dále provádí detektivní prověrky pro personální bezpečnost, detektivní a zpravodajská opatření k zajištění informační bezpečnosti a detektivní a zpravodajská opatření k ochraně „KNOW HOW“, technologické bezpečnosti, provozní bezpečnosti a obchodní bezpečnosti apod. [4]

V rámci detektivní či zpravodajské ochrany ekonomických zájmů podnikatelských subjektů zaujímá velmi významné, a dá se říci, že prioritní, místo detektivní a zpravodajská prevence. Je výhodnější negativním vlivům směřující proti podnikatelským subjektům a jejich aktivitám předcházet, než následně odstraňovat vzniklé škody. Je velmi obtížné vymáhat pohledávky od dlužníků, kteří nechtějí zaplatit nebo nemají z čeho zaplatit. Naopak je velice výhodné těmto situacím předcházet prováděnou prevencí, v daném případě detektivní či zpravodajskou prověrkou budoucích odběratelů, obchodních partnerů apod. Do systému prevence ochrany ekonomických zájmů můžeme zahrnout činnosti uvedené na obrázku 2.



Obrázek 2 Systém prevence ochrany ekonomických zájmů (zdroj: [4])

Detektivní rozkrývání latentní ekonomické – hospodářské kriminality

Mnoho podnikatelských subjektů se domnívalo a někteří z nich se ještě stále domnívají, že vyhledávání latentní ekonomické – hospodářské kriminality v jejich podniku (společnosti, firmě, živnostenské provozovně, organizaci apod.) zajišťuje Policie ČR. To je samozřejmě mylná myšlenka. V podmínkách tržní ekonomiky si tuto činnost musí zajišťovat podnikatelský subjekt sám. Policie ČR řeší případy registrované kriminality a provádí odhalování a rozpracování těch případů ekonomické kriminality, které bezprostředně poškozují zájmy státu. Rozkrývání ekonomické kriminality v podniku, úřadu, instituci či organizaci je jednou z velmi složitých činností v rámci soukromě detektivních služeb. Spadá do oblasti ochrany ekonomických zájmů, ale samozřejmě zapadá i do komplexní ochrany představované konkurenčním zpravodajstvím. Vzhledem k její složitosti a náročnosti nelze při její realizaci spoléhat jen na získané zkušenosti, dovednosti a návyky. Jedná se o práci tvůrčí, a má-li být úspěšná, musí vycházet z poznání a analýzy složitých společenských a ekonomických vztahů a jevů. Proto také, pokud má soukromá detektivní činnost úspěšně působit v oblasti ochrany ekonomických zájmů a zejména pak v oblasti vyhledávání latentní ekonomické – hospodářské kriminality, musí vycházet z analýzy situací a jevů, které ekonomickou kriminalitu vyvolávají, způsobují a usnadňují, tedy od pramenů hospodářské kriminality, tj. podmínek a příčin ekonomické kriminality (trestné činnosti a jiných forem protiprávního jednání). Musí se opírat o obecné poznatky kriminologické vědy, i o kriminologickou analýzu v daném podnikatelském subjektu úřadu, instituci či organizaci. V návaznosti na to je nezbytné provést analýzu a zkoumat situace, jevy a procesy, které vznik ekonomické kriminality omezují, znesnadňují nebo dokonce znemožňují a o ty se v soukromé detektivní činnosti opírat. Soukromé detektivní kanceláře (soukromí detektivové) zpravidla zabezpečují nebo realizují informační proces (služby) týkající se zejména „sociálně a ekonomicky patologických „jevů, konfliktních procesů, nebo jevů, majíc znaky zločinnosti – ekonomické kriminality. Proto také úspěšnost jejich práce ve značné míře závisí na tom, jak budou využívat bohatých zkušeností, jež poskytuje kriminologie, jako nauka o podstatě zločinu (či jiné formy protiprávního jednání), jeho stavu, dynamice, struktuře, příčinách a podmínkách vzniku a existence, kriminogenních osobnostech a způsobech prevence ekonomické kriminality (trestné činnosti a dalších forem protiprávního jednání). [4]

Shromažďování, třídění, analýza, syntéza informací

Jedná se o informace potřebné pro podnikání a o důkazy pro soudní a správní kauzy.

Jestliže při rozhodování o státních zakázkách, dalších výběrových řízení, rozdělování dotací a strukturálních zdrojů, licenčních řízení, zavádění nové výroby, obchodních operací apod., nedokáže podnikatelský subjekt (společnost, firma, organizace, družstvo apod.), dostatečně kvalitně ošetřit subjektivní stránku tohoto procesu, musí počítat s tím, že s velkou pravděpodobností bude předběhnut a vyřazen konkurencí. Jedná se o zákonitost globálního světa s globalizovanou tržní ekonomikou. Zajišťování informací potřebných na ochranu a podporu podnikání nemůže označovat jako špionáž a kvalifikované lobování nemůžeme zaměňovat s korupcí.

Konkurenční zpravodajství (Completitive Inteligence) představuje komplexní zajištění ochrany a podpory ekonomických zájmů podnikatelských subjektů a jejich podnikatelských aktivit.

2.2 Konkurenční zpravodajství

Konkurenční zpravodajství můžeme chápat ve dvou rovinách. V širším a užším slova smyslu. [4]

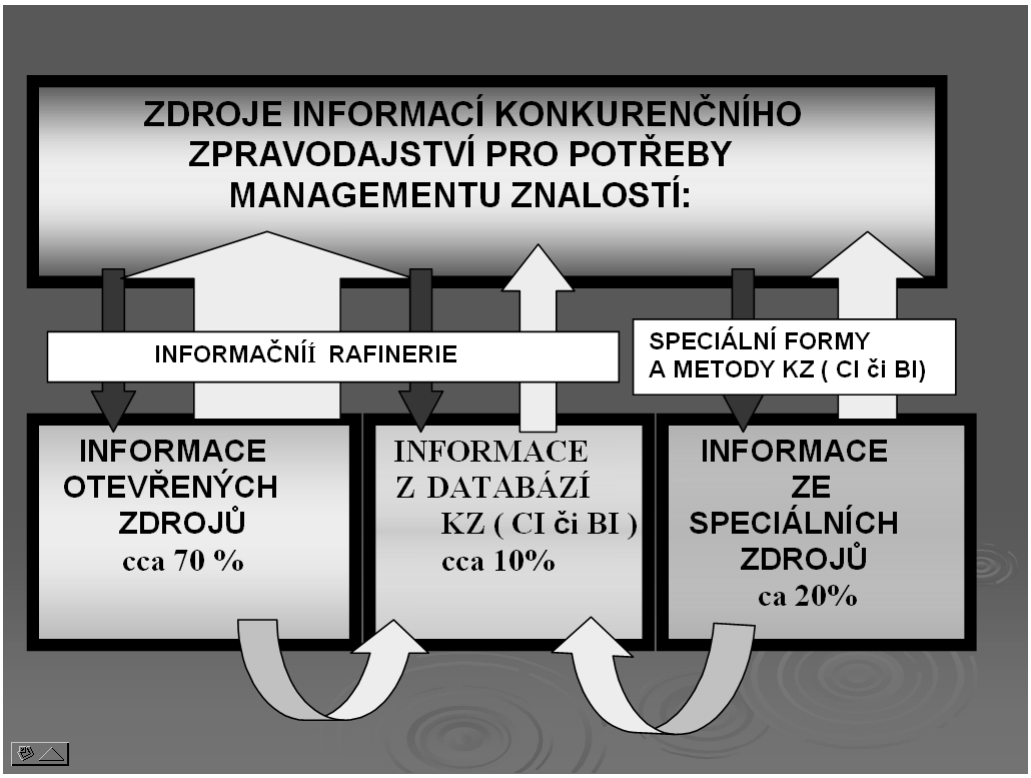
V širším slova smyslu

Konkurenční zpravodajství v širším slova smyslu lze definovat jako soubor aktivit zahrnující vyhledávání, analýzu a distribuci informací využitelných pro rozhodování ekonomických subjektů, jak definoval Tomáš Vejlupek, koordinátor SCIP pro Českou republiku.

Jedná se o souhrn informačních činností směřující k naplnění managementu znalostí (Knowledge managementu). Zpravodajství jako nástroj k prosazování mocenských a bezpečnostních zájmů, se bez prostředků špionáže úplně neobejde. Legitimní nástroj managementu firem se však musí od špionáže jasně distancovat. Pro odlišení klasického zpravodajství od zpravodajství prováděného za účelem získání konkurenčních výhod v legitimním konkurenčním boji firem se zavedl přívlastek konkurenční (Completitive Inteligence). [4]

Základem dosažení jakéhokoliv cíle je umění získat, zpracovat a využít informace – znalosti. U zpravodajství máme na mysli proces směřující k dosažení znalosti. Zpravodajství

musí dávat odpovědi – znalosti pro rozhodnutí operativního, taktického a strategického rázu. Zpravodajství je třeba chápat jako nástroj řízení. Jde o schopnost vyhledávat, filtrovat a interpretovat informace ve smysluplných souvislostech. Cílem je analyzovat a interpretovat všechny dostupné informace. Možné zdroje informací konkurenčního zpravodajství jsou zobrazené na obrázku 3.



Obrázek 3 Zdroje informací konkurenčního zpravodajství (zdroj: [4])

V užším slova smyslu

Konkurenční zpravodajství v užším slova smyslu, definujeme jako součást bezpečnostní, zpravodajská a bezpečnostní ochrana a podpora ekonomických zájmů podnikatelských subjektů a jejich podnikatelských aktivit, která představuje [4]:

- obranné zpravodajství,
- ofenzivní zpravodajství,
- vlivové zpravodajství (lobby).

Obranné zpravodajství

- zajištění personální bezpečnosti
- zajištění informační bezpečnosti
- zajištění bezpečnosti „KNOW HOW“, technologické a provozní bezpečnosti
- zajištění bezpečnosti obchodních vztahů apod.
- ochrana před ofenzivním a vlivovým zpravodajstvím konkurence

Ofenzivní zpravodajství

- zajištění informací potřebných pro podnikání
- zajištění informací marketingového charakteru
- získávání informací o konkurenci

U ofenzivního zpravodajství se jedná o systém získávání informací z dat, a to jednak informace potřebné pro podnikání, podnikatelské aktivity, tak i informace sloužící k ochraně vlastního podnikání před nežádoucím vlivem konkurence. Tyto informace jsou z oblasti ochrany vlastního podnikatelského subjektu před nežádoucími vlivy a z tzv. aktivní oblasti, tj. ve prospěch a k podpoře vlastních podnikatelských aktivit. Aby ochrana vlastního podnikatelského subjektu před nežádoucími vlivy a aktivní informační podpora vlastních podnikatelských aktivit měla smysl, musí projít procesem rozhodnutí, které musí být za pomocí vlivových (lobbyistických) opatření uvedeno v život. [4]

Toto ofenzivní zpravodajství se odehrává v nepřetržitém cyklu. Názorně je uvedeno na obrázku 4.

Obrázek 4 Cyklus ofenzivního zpravodajství (zdroj:[4])

Vlivové zpravodajství (Lobby)

Vlivové zpravodajství je detektivní a zpravodajská podpora rozhodnutí přijatých a realizovaných managementem znalostí.

O profesionálním lobování můžeme říci, že se musí opírat o cílené umístnění informací a vyvolání spolupráce založené na důvěře podložené praktickou zkušeností, oboustrannou výhodností a zainteresovaností. Tento proces vyžaduje velký objem kvalitních a relevantních informací, profesionálně a kvalifikovaně zpracovaných. Cílem lobování je zabezpečit takové rozhodování ekonomických, správních i politických subjektů a obchodních partnerů, ale i konkurenčních subjektů, které je v zájmu toho, v jehož prospěch se lobuje. Nedílnou součástí lobování je i ovlivňování veřejného mínění. [4]

3 Charakteristika globalizace v informační společnosti

Již několik let se projevuje velký rozvoj informačních a komunikačních technologii (ICT), tudíž se projevuje globalizace v informační společnosti[2]. V současné době se dá předpokládat, že rozvoj v této oblasti nás teprve čeká. Přičemž snaha o maximální využití ICT má, ale i své negativní stránky a důsledky. Člověk je zvídavý a proto se vznikem tohoto technického fenoménu se najdou lidé, kteří jej využijí k páchání trestné činnosti. Nejinak tomu je právě s rostoucím rozvojem ICT. Objevila se i počítačová kriminalita, která představuje nový druh trestné činnosti.

Tento kriminální fenomén má nejen národní, ale hlavně mezinárodní charakter. V dnešní době je možné již během několika milisekund napadnout rozsáhlé komunikační sítě a narušit jejich funkci a to z jakéhokoliv místa na světě, v jakoukoliv dobu, téměř anonymně.

Tomuto právě napomáhá Internet. Internet je souhrn všech počítačových sítí a počítačů vzájemně spojených přenosovým protokolem TCP/IP (Transmission Control Protocol/Internet Protocol). Každá síť a každý počítač, který je součástí Internetu, disponuje jedinečným doménovým jménem. Přidělování a správa doménových jmen jsou hierarchické: správce domény nejvyššího řádu (např..cz) rozhoduje o přidělování domén druhého řádu (např. mvcr.cz), správce domény druhého řádu rozhoduje o přidělování domén třetího řádu, aniž by toto přidělování konzultoval se správcem domény nejvyššího řádu atd. Komunikace mezi počítači probíhá na základě IP, ve kterém se počítače označují číselnými adresami (IP adresy). Před zahájením komunikace je vždy nutno zjistit, jaká IP adresa odpovídá zadanému doménovému jménu. Tomu slouží síť specializovaných počítačů, které na žádost obsahující doménové jméno zašlou odpověď s příslušnou číselnou adresou nebo naopak. Systém těchto počítačů se označuje jako DNS (Domain Name System).

Počet uživatelů Internetu na světě již překročil magickou hodnotu jedné miliardy a jejich počet neustále roste. Mezi největší uživatele Internetu patří Čína (179.710.000, 18% z celkového počtu uživatelů) a hned za ní je v těsném závěsu USA (163.300.000, 16,2% celkového počtu uživatelů). Z Evropských zemí mají největší světový podíl uživatelů Internetu Německo a Velká Británie, které mají každý více jak 3,5% z celkového počtu. [5] V České republice bylo podle ČSÚ v roce 2007 připojeno k internetu 32% domácností. A

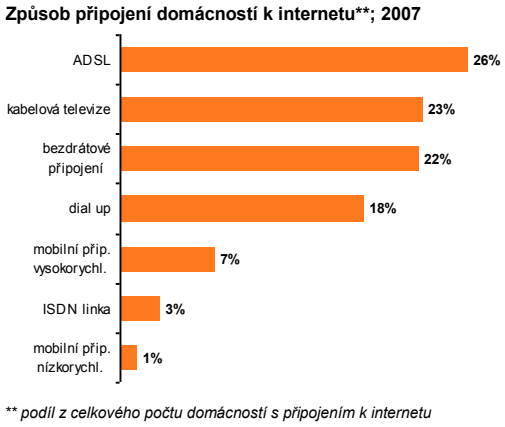
[2] Společnost založená na intenzivním využívání informačních a komunikačních technologií. Tato společnost pokládá vytváření, šíření a manipulaci s informacemi za určující část svých ekonomických, kulturních a společenských aktivit.

počet stále roste jak je vidět z obrázku 5. Jako nejčastější způsob připojení je ADSL (Asymetric Digital Subscriber Line).

%

	2003	2006	2007
Celkem	**14,8**	**26,7**	**32,0**
podle typu domácnosti			
domácnosti bez dětí		**16,0**	**19,0**
1 dospělá osoba bez dětí	.	10,3	12,0
2 dospělé osoby bez dětí	.	16,8	20,4
3 a více dospělých osob bez dětí	.	30,6	34,8
domácnosti s dětmi		**45,0**	**55,0**
1 dospělá osoba s dětmi	.	30,3	40,0
2 dospělé osoby s dětmi	.	48,5	57,1
3 a více dospělých osob s dětmi	.	45,9	55,9
podle typu lokality			
hustě zalidněná (velká města)	.	31,4	38,4
středně zalidněná (střední a menší města)	.	25,9	30,4
málo zalidněná (venkovské oblasti)	.	23,2	27,3
podle kraje			
Praha	29,3	36,7	46,2
Středočeský	15,5	28,7	32,0
Jihočeský	11,8	24,6	31,7
Plzeňský	11,6	27,5	25,9
Karlovarský	15,9	26,1	27,4
Ústecký	9,6	19,3	26,7
Liberecký	13,1	23,9	32,1
Královéhradecký	13,8	27,8	31,2
Pardubický	15,6	26,3	26,7
Vysočina	15,6	24,6	31,4
Jihomoravský	18,6	28,2	35,1
Olomoucký	8,9	23,9	21,8
Zlínský	14,8	19,2	29,8
Moravskoslezský	12,3	25,8	30,6

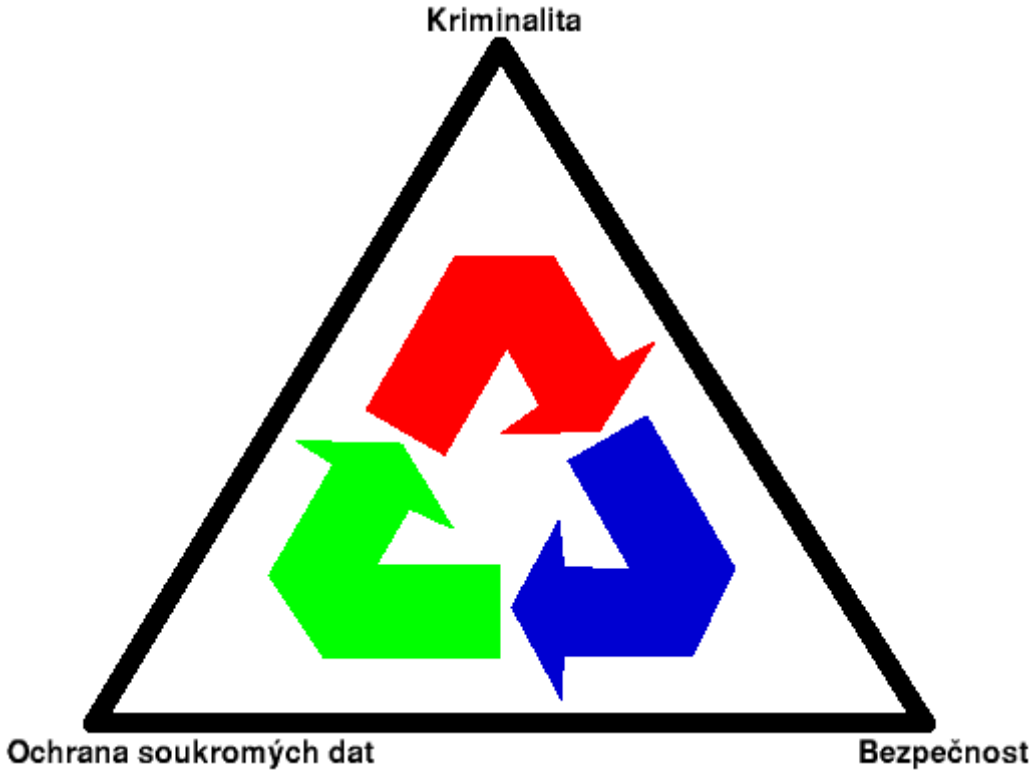
**podíl z celkového počtu domácností v dané socio-demografické skupině*



Obrázek 5 Počet uživatelů Internetu a způsob připojení (zdroj: [6])

3.1 Počítačová kriminalita

Počítačová kriminalita je výrazný jev dnešní doby. Jednoznačně definovat lze tento pojem jen velmi obtížně. "Počítačová kriminalita" je jakýsi "terminus technicus", jímž se označuje skupina trestných činů mající stejný charakter. Stejně tak jako je tomu u pojmů např. hospodářská kriminalita, násilná kriminalita, organizovaný zločin apod. Obecně lze říci, že počítačová kriminalita je mnohdy i přes své nesporné prvky moderních technologií jen jinou tváří různých standardních trestných činů. Jak je patrné z obrázku 6, můžeme v uzavřeném kruhu mimo jiné hledat slabiny implementace počítačových systémů, legislativní nedostatky nebo zájmy skupin a jednotlivců.



Obrázek 6 Uzavřený kruh (zdroj: [7])

Pokud chceme hovořit o počítačové kriminalitě, tak musíme tímto termínem obvykle označit trestné činy proti počítačům nebo trestné činy páchané pomocí počítačů. Toto jednání musí také naplňovat znaky skutkové podstaty některého trestného činu uvedeného v trestním zákoně[3] a nebezpečnost takového jednání musí dosahovat požadovaného stupně nebezpečnosti činu pro společnost.[4] Počítačovou kriminalitu můžeme definovat velmi obecně jako trestný čin namířený proti integritě, dostupnosti nebo utajení počítačových systémů nebo trestný čin, při kterém je požito informačních či telekomunikačních technologií. Vymezení počítačové kriminality lze dále citovat z výkladového slovníku *Ochrana dat* od Zelenky, Čecha a Naimana, kteří chápou počítačovou kriminalitu jednak jako *„[…] veškeré aktivity, které vedou k neautorizovanému čtení, manipulaci, vymazání nebo zneužití dat.“* Anebo také jako tzv. počítačovou defraudaci – jako jednu z metod počítačové kriminality založenou *„[…] na změně nebo jiné interpretaci dat s cílem získat výhodu, peníze na vlastní účet.“* [8]

[3] Zákon č. 140/1961 Sb., Trestní zákon, ve znění pozdějších předpisů.
[4] Čin, jehož stupeň nebezpečnosti pro společnost je nepatrný, není trestným činem, i když jinak vykazuje znaky trestného činu. Stupeň nebezpečnosti činu pro společnost je určován zejména významem chráněného zájmu, který byl činem dotčen, způsobem provedení činu a jeho následky, okolnostmi, za kterých byl čin spáchán, osobou pachatele, mírou jeho zavinění a jeho pohnutkou.

Státy Evropské Unie a Evropského parlamentu se dohodly na této definici počítačové kriminality: Je to nemorální a neoprávněné jednání, které zahrnuje zneužití údajů získaných prostřednictvím ICT nebo jejich změnu. Počítače v podstatě neumožňují páchat novou neetickou a trestnou činnost, poskytují jen novou technologii a nové způsoby na páchání již známých trestných činů jako sabotáž, krádež, neoprávněné užívání cizí věci, vydírání nebo špionáž.

Počítačová kriminalita má mnoho významných charakteristik, kterými je odlišná od kriminality klasické. Lze říci, že ve většině případů počítačové kriminality se neobjevují takové prvky, jako je násilí, použití zbraně, újma na zdraví osob apod. U klasické kriminality se měří doba spáchání určitého trestného činu na více jak minuty až na dny. Trestné činy v oblasti počítačové kriminality může být ale spáchán v několika tisícinách sekundy z jakéhokoliv místa na zemi. Pachatel trestného činu nemusí být tak na místě činu.

Mezi další významnou charakteristiku pro počítačové kriminality patří ve svém důsledku značné ztráty, a to buď v přímé podobě finančních částek, nebo v podobě zneužití získaných údajů. Počítačovou kriminalitu také provází určitá diskrétnost trestné činnosti. Z tohoto vyplývá, proč počítačová kriminalita bývá pro svou povahu označována jako kriminalita „bílých límečků“.

Za počítačovou kriminalitu budeme považovat trestné činy, jejichž objektem, eventuálně objektivní stránkou, bude informační technologie v plném slova smyslu. Jako jedno z možných členění počítačové kriminality přijala Rada Evropy úmluvu o počítačové kriminalitě [9], která byla publikována dne 23. 11. 2001, vstoupila v platnost 1. 7. 2004 a Česká republika ji podepsala 9. 2. 2005. Jejím smyslem je mj. sjednotit legislativu evropských zemí, nejen proto, že se jedná o problematiku počítačové kriminality, ale také z toho důvodu, že tato trestná činnost má mezinárodní charakter. Členění podle Rady Evropy je následující:

Do minimálního seznamu trestných činů jsou zahrnovány [9]:

- počítačové podvody,
- počítačové falzifikace,
- poškozování počítačových dat a programů,
- počítačová sabotáž,
- neoprávněný přístup,
- neoprávněný průnik,
- neoprávněné kopírování autorsky chráněného programu,
- neoprávněné kopírování fotografie.

Do volitelného seznamu trestných činů je zahrnuto [9]:

- změna v datech nebo počítačových programech,
- počítačová špionáž,
- neoprávněné užívání počítače,
- neoprávněné užívání autorsky chráněného programu.

Minimální seznam obsahuje taková jednání, která by měla být jako skutkové podstaty trestných činů zapracována do právních řádů jednotlivých zemí, aby bylo možné vést účinný boj proti počítačové kriminalitě. Ve volitelném seznamu jsou uvedena jednání, která by bylo vhodné kvalifikovat jako trestné činy, avšak není to nezbytné.

Srovnání legislativy v České republice a v Evropě uvádím v tabulce 2.

Tabulka 2 Srovnáni legislativy v České republice a v Evropě (zdroj: vlastní)

Rada Evropy	**Česká republika**
počítačové podvody	Podvod, pojistný, úvěrový - §§ 250, 250a, 250b tr. zákona
počítačové falzifikace	
poškozování počítačových dat programů	poškození a zneužití a záznamu na nosiči informací - § 257a tr. zákona
počítačová sabotáž	Sabotáž - § 97 tr. zákona, obecné ohrožení - §§ 179-180 tr. zákona, poškozování cizí věci - § 257 tr. zákona
neoprávněný přístup	neoprávněné užívání cizí věci - § 249 tr. zákona
neoprávněný průnik	neoprávněné užívání cizí věci - § 249 tr. zákona
neoprávněné kopírování autorsky chráněného programu	porušování autorského práva - § 152 tr. zákona
neoprávněné kopírování topografie	porušování autorského práva - § 152 tr. zákona, porušování průmyslových práv - § 151 tr. zákona,
změna v datech nebo počítačových programech	poškození a zneužití záznamu na nosiči informací -§ 257a tr. zákona, zkreslování údajů hospodářské a obchodní evidence - § 125 tr. zákona
počítačová špionáž	Vyzvědačství- § 105 tr. zákona, ohrožení utajované skutečnosti - §§ 106, 107
neoprávněné užívání počítače	neoprávněné užívání cizí věci - § 249 tr. zákona
neoprávněné užívání autorsky chráněného programu	porušování autorského práva - § 152 tr. zákona

3.2 Nové typy protiprávního jednání

V 21. století se s nástupem nových technologií objevují i nové druhy trestné činnosti. Jedná se o typy jednání, kde je obtížná klasifikace do výše uvedených příslušných paragrafů. Variant těchto deliktů existuje velká řada a zde bych uvedl ty nejběžnější případy, mezi které patří [10]:

- hacking,
- kybernetické výpalné,
- šíření materiálu se závadným obsahem,
- zneužití internetových stránek,
- sparing,
- warez,
- cracking,
- sniffing,
- cybersquatting.

Hacking

Hacking je považován za jeden z nejstarších deliktů, který v původním pojetí lze jen těžko označit za trestný čin, neboť nelze snadno vyčíslit škodu, která byla způsobena. Někdy ani sám správce systému neví, že do systému hacker pronikl. Motivací původního hackerské subkultury nebylo způsobení škody, ale pouze radost z osobního vítězství nad technikou, kdy se hacker naboural do systému, a tím získával obdiv hackerské komunity. [10]

V současném pojetí lze hacking definovat jako proniknutí do počítačového nebo řídícího systému jinou, než standardní cestou při obejití nebo prolomení jeho bezpečnostní ochrany. Právní úprava České republiky, která by postihovala hacking jako takový, je velmi obtížná. Bylo by možno použít ustanovení podle § 257a trestního zákona, který hovoří o poškození nebo zneužití záznamu na nosiči informací[5]. Skutková podstata tohoto trestného

[5] **§ 257a Poškození a zneužití záznamu na nosiči informací**
(1) Kdo získá přístup k nosiči informací a v úmyslu způsobit jinému škodu nebo jinou újmu nebo získat sobě nebo jinému neoprávněný prospěch
a) takových informací neoprávněně užije,
b) informace zničí, poškodí, změní nebo učiní neupotřebitelnými, nebo
c) učiní zásah do technického nebo programového vybavení počítače nebo jiného telekomunikačního zařízení, bude potrestán odnětím svobody až na jeden rok nebo zákazem činnosti nebo peněžitým trestem nebo propadnutím věci nebo jiné majetkové hodnoty.
(2) Odnětím svobody na šest měsíců až tři léta bude pachatel potrestán,
a) spáchá-li čin uvedený v odstavci 1 jako člen organizované skupiny, nebo
b) způsobí-li takovým činem značnou škodu nebo získá-li sobě nebo jinému značný prospěch.

činu je naplněna již tím, že pachatel získá přístup k nosiči informací v úmyslu způsobit účinek níže popsaného trestného činu. [10]

Mezi nejslavnější počítačové hackery světa je považován **Kevin David Mitnick** , nar. 6. října 1963. V 90. letech se ho obávaly tisíce Američanů a byl jednou z nejhledanějších osob v historii FBI. Po zatčení mu hrozil trest několika set let odnětí svobody, přestože nikdy nebyl obviněn z toho, že by měl z hackerství finanční prospěch. Soudním výrokem mu byl zakázán jakýkoliv přístup k počítači. Soud odůvodnil svůj rozsudek slovy: „Vyzbrojen klávesnicí je nebezpečím pro společnost“. Nakonec ve vězení strávil 5 let a po propuštění 21. ledna 2000 celý svůj život úplně změnil. Stal se nejvyhledávanějším expertem na zabezpečení počítačových systémů ve Spojených státech Amerických. Ve své knížce „Umění klamu“, kterou vydal, odhaluje tajemství svého „úspěchu“, popisuje, jak snadné je překonat zábrany a získat přísně tajné informace, sabotovat podniky, úřady či jiné instituce. Několiksetkrát tak učinil za pomocí důmyslných technik ovlivňování lidí. Dokazuje, jak klamná je představa bezpečnosti soukromých i služebních dat, ukazuje, jak obejít systémy za miliony dolarů zneužitím lidí, kteří je obsluhují. [11]

Kybernetické výpalné

Jedná se o nový typ trestné činnosti založený na strachu z prezentované hrozby průniku do spravovaného nebo vlastněného systému s následujícím zneužitím nebo zničením dat. I když ze strany vyděrače to mnohdy může být pouze využití neznalosti vydírané strany, je to zcela nová projekce klasického deliktu do počítačového prostředí, kterou se může rozmáhat zejména organizovaný zločin. Jedinou ochranou, kterou ohrožená strana může použít, je důkladná analýza rizik, spojených s narušením spravovaného systému a tomu odpovídající náklady na ochranu nebo vyplacené výpalné. [10]

Toto protiprávní jednání lze zařadit do trestného činu vydírání podle § 235 trestního zákona, s možností rozšíření o trestný čin, která již byl definován u hackingu.

Šíření materiálu se závadným obsahem

Tento trestný čin, zahrnující šíření pornografie, materiálů podporující extremismus nebo materiálů podobného obsahu, spadá spíše do trestní odpovědnosti poskytovatele obsahu, než do trestní odpovědnosti správce počítačového systému. Nejedná se o nový druh trestné

---

(3) Odnětím svobody na jeden rok až pět let bude pachatel potrestán, způsobí-li činem uvedeným v odstavci 1 škodu velkého rozsahu nebo získá-li sobě nebo jinému prospěch velkého rozsahu.

činnosti, ale spíše o nové médium pro její vykonávání. Je to jistá moderní projekce klasického trestného činu[6]. [10]

Zneužití internetových stránek

S velkým rozšířením elektronické komunikace dostal nový rozměr i jeden z nejstarších trestných činů – pomluva podle § 206 tr. zákona. S tou se setkáváme velmi často a definovat pomluvu není vždy jednoduché. Dříve se pomluva aplikovala za pomocí různých nápisů na veřejných místech. V dnešní době je právě velmi často využíván internet jako sdělovací prostředek. [10]

Forma spáchání takového trestného činu je při všeobecné dostupnosti internetu jednoduchá a může spočívat třeba v uvedení telefonního čísla spolu s osobní fotografií (která samozřejmě nepatří dotčené osobě nebo je výsledkem fotomontáže) na stránkách erotické seznamky. Jiný případ, který je velmi častý, je vytvoření internetových stránek, vyjadřujících názory jejich autora, často doplněné faktickými nebo smyšlenými komentáři třetích stran. [10]

K takové činnosti většinou láká falešný pocit anonymity na internetu, avšak pokud se nejedná o velmi promyšlený postup, autor může být vysledován. Zde pachatelům nahrává naše zbytečně složitá legislativa, která již pro sdělení koncového uživatele určité IP adresy vyžaduje vydat příkaz příslušný soudem podle § 88a tr. řádu.

Spamming

Pod pojmem spamming se rozumí zasílání nevyžádané elektronické pošty (email) obvykle s reklamním nebo propagačním obsahem. Jedná se o nepříjemný přímý marketing, který obtěžuje každého uživatele elektronické pošty. Velké množství nevyžádané pošty může některé firmě způsobit nemalé škody. Elektronické adresy se získávají nejrůznějším způsobem. Nejběžnější zdroje jsou právě www stránky, které prohledávají tzv. roboti, konference, inzeráty, ICQ aj. I když existuje celá řada programů, které spam dokáží odfiltrovat, jejich trvalá účinnost je pochybná, neboť spameři tento mechanismus znají a pro jeho obejití často mění adresu odesílatele. V poslední době jsou pro filtraci spamu používány zejména tzv. Bayesovské filtry[7], založené na vyhodnocení pravděpodobnosti spamu na

[6] Např. § 205 tr. zákona – Šíření pornografie, § 205a tr. zákona - Přechovávání dětské pornografie, § 198 tr. zákona - Hanobení národa, etnické skupiny, rasy a přesvědčení, § 198a Podněcování k nenávisti vůči skupině osob nebo k omezování jejich práv a svobod nebo § 260 tr. zákona a § k němu náležející - Podpora a propagace hnutí směřujících k potlačení práv a svobod člověka

[7] **Filtry založené na učení** využívají triky z oblasti umělé inteligence. V režimu učení se filtru předkládají dopisy explicitně označené jako spam a ham (ne spam), filtr z předložených dopisů extrahuje informace, které si

základě analýzy struktury přijaté zprávy. Také se ale může stát, že do spamu bude zařazená i pošta, která není nevyžádaná. [10]

Spam je velmi obtížný efekt spojený s elektronickou komunikací. K potlačení spamu směřovala již mnohá opatření a návrhy, nicméně jeho nárůst je téměř nezastavitelný. Některé zdroje uvádí, že v současné době lze očekávat až 90% objem spamů v elektronické poště.

Právní pohledy na možnost postihnout spamy se různí. V podmínkách České republiky se dá aplikovat zákonem o některých službách informační společnosti číslo 480/2004 Sb., který problematiku spamu upravuje a vyžaduje prokazatelný souhlas příjemce zprávy. Dohledem nad dodržováním zákona byl pověřen Úřad pro ochranu osobních údajů. Tento zákon byl postupně novelizován, a to v letech 2005 a 2006. [10]

Zákon byl vytvořen podle směrnice Evropského společenství číslo 2000/31/ES. Spam definuje jako obchodní sdělení, což jsou *všechny formy sdělení určeného k přímé či nepřímé podpoře zboží či služeb nebo image podniku fyzické či právnické osoby*. Zákon řeší nejen internetový spam, ale také jiné formy elektronické komunikace (SMS, telemarketing).

Podle zákona se *za obchodní sdělení nepovažují údaje umožňující přímý přístup k informacím o činnosti fyzické či právnické osoby nebo podniku, zejména doménové jméno nebo adresa elektronické pošty; za obchodní sdělení se dále nepovažují údaje týkající se zboží, služeb nebo image fyzické či právnické osoby nebo podniku, získané uživatelem nezávisle*.

Obchodní sdělení může prodejce zaslat, když [10]:

a) je adresátem jeho zákazník:
   - který zasílání podobných sdělení v minulosti neodmítl
   - sdělení se týká obdobného zboží či služeb,

b) adresát obchodníkovi poskytl informovaný souhlas.

Další možností boje se spamem, je použití ustanovení § 2 odst. 1, písm. e) zákona číslo 40/1995 Sb. o regulaci reklamy. Nevyžádaná pošta musí v tomto případě mít reklamní charakter a vést k nákladům na straně adresáta nebo jej obtěžovat. Porušení tohoto ustanovení

---

ukládá do databáze. Nejčastěji je dopis rozkládán na slova (popř. jiné úseky textu) a pro jednotlivá slova se statisticky zjišťuje pravděpodobnost, že dopis, který toto slovo obsahuje, je spam. V režimu rozpoznávání pak filtr využívá nashromážděné informace a testovanému dopisu přiřadí pravděpodobnost, že je to spam. Nejčastěji se pro výpočet pravděpodobnosti používá vzorec, který navrhl matematik Bayes. Velkou výhodou je, že filtr může učit i uživatel – laik. Učící se filtry jsou nejúčinnější, učí-li je přímo sami koncoví uživatelé podle svého individuálního názoru, co je spam a co ne. Přesto se bayesovské filtry používají i na serverech, kde učení probíhá pro všechny uživatele serveru společně.

je trestáno peněžitou pokutou, která může být na základě posouzení příslušného orgánu uložena až do výše dvou milionů korun.

Warez

Dnešní moderní počítačové pirátství, které je doprovodným fenoménem používání informačních technologií a rozmachu internetu, je z větší části skupinovou záležitostí. První část pracuje na prolomení ochranných prvků programových produktů. Druhá se specializuje na jejich šíření pomocí www serverů a získávání financí na jejich provoz umisťováním reklamy na pornografické servery nebo s erotickým obsahem na svých stránkách. [10]

Warezy jsou spíše pozůstatkem minulosti, dnes se spíše používají pro šíření tzv. cracků, neboli programů umožňujících zrušení ochrany u programových produktů, jejich plná verze je volně přístupná, avšak časově nebo jinak omezena. V současné době jsou daleko rozšířenější programy pro sítě P2P (peer-to-peer), které umožňují výměnu hudebních souborů, videa atd. Postihnutí nelegálního obsahu šíření v síti P2P je samozřejmě daleko složitější, než když je k šíření použit server warez. [10]

Právní posouzení je zde jednoduché a jednoznačné. Jedná se o porušení autorských práv, na které se vztahuje § 152 tr. zákona[8].

Cracking

Potom, co jsme si zde vysvětlili protiprávní jednání hacking a warez, je nutno uvést i formu, která je s těmito dvěma názvy neoddělitelně spjata. Jedná se o cracking, neboli o prolamování či obcházení ochranných prvků elektronických nebo programových produktů s cílem jejich neoprávněného použití. Cracking používá celou řadu metod od prostého debugování spuštěného programu, až po tzv. reverse engineering. Cracking je často používaná metoda při průniku do systému, kde cílem crackingu není „zprovoznění“ programu chráněného „softwarovým“ nebo „hardwarovým“ klíčem, ale zjištění informací důležitých pro umožnění neoprávněného přístupu do cílového systému. Nejčastěji se jedná o tzv.

[8] **§ 152 Porušování autorského práva, práv souvisejících s právem autorským a práv k databázi**
(1) Kdo neoprávněně zasáhne do zákonem chráněných práv k autorskému dílu, uměleckému výkonu, zvukovému či zvukově obrazovému záznamu, rozhlasovému nebo televiznímu vysílání nebo databázi, bude potrestán odnětím svobody až na dvě léta nebo peněžitým trestem nebo propadnutím věci nebo jiné majetkové hodnoty.
(2) Odnětím svobody na šest měsíců až pět let nebo peněžitým trestem nebo propadnutím věci nebo jiné majetkové hodnoty bude pachatel potrestán,
a) získá-li činem uvedeným v odstavci 1 značný prospěch, nebo
b) dopustí-li se takového činu ve značném rozsahu.

„password cracking“ – zjišťování hesla pro přístup do systému. Password cracking má širokou škálu metod, od snahy uhodnout heslo pomocí slovníku nejčastěji používaných hesel, použití hrubé síly při zkoušení všech možných kombinací znaků přicházející v úvahu, až po sofistikované algoritmy snažící se o zpětnou rekonstrukci odpovídající kombinace znaků ze zakódovaného řetězce hesla, uloženého v systémovém souboru s hesly. [10]

Trestní kvalifikace tohoto typu protiprávného jednání může být velmi rozličná. Obvykle se jedná o porušení autorského práva podle § 152 tr. zákona nebo poškození či zneužití záznamu na nosiči informací podle § 257 tr. zákona.

Sniffing

Sniffing je neoprávněné „odposlouchávání“ komunikace na síti, zdánlivě nevinná činnost, která má rovněž svoji trestní kvalifikaci. Obvykle dochází k ukládání, následnému čtení a odposlechu datové komunikace subjektem, který není jejím adresátem. Cílem této činnosti je získání přístupu k veškerému obsahu nešifrované komunikace, jako jsou např. přístupová hesla a jména, obsah e-mailů a další soubory posílané pomocí internetu. Tímto dochází k naplnění trestného činu porušování tajemství dopravovaných zpráv podle § 239 tr. zákona. V případě, že dojde ke zneužití takto získané informace, např. prozrazení třetí straně, pak dochází k naplnění trestného činu porušování tajemství dopravovaných zpráv podle § 240 tr. zákona. [10]

V této souvislosti bych dále uvedl jednu poměrně málo známou skutečnost. Internetové adresy, záznamy o provozu sítě a ostatní záznamy umožňující jednoznačně identifikovat osobu, ke které se vztahuje činnost na síti, jsou předmětem ochrany podle zákona o elektronických komunikacích[9] a zákona o ochraně osobních údajů[10]. Naivní správce sítě, který tyto údaje poskytne třetí osobě, se tak vystavuje postihu podle výše citovaného ustanovení trestního zákona. Jiným případem je úkon, kdy poskytnutí takových údajů požaduje policejní orgán. Zde je nutno rozlišit dva případy. V případě, že organizace, které patří síť, je poskytovatelem služby elektronických komunikací, ve smyslu zákona o elektronických komunikací, musí vyžadující policejní orgán předložit povolení soudu k poskytnutí takových údajů. Pokud organizace, které síť patří, není poskytovatelem služby

[9] zákon číslo 127/2005 Sb. zákon o elektronických komunikacích
[10] zákon číslo 101/2000 Sb. o ochraně osobních údajů

elektronických komunikací, pak se jedná o skutečnost, kdy je správce sítě povinen podat policejnímu orgánu vysvětlení na základě zákona o polici[11]. [10]

Cybersquatting

Cybersquatting se dá charakterizovat jako postup, kdy se vykupují oblíbená slova (názvy velkých podniků, institucí a produktů, a to zejména v oblasti farmaceutiky) a registrují se jako internetové adresy (domény), a to s cílem jejich prodeje s vysokým ziskem společnostem a vlastníkům ochranných známek. Pro mnoho společností to představuje závažný problém. Existují už i aukční servery, kde lze snadno prodat název domény nejvyšší nabídce. [10]

Právní kvalifikace v této oblasti je možná podle § 150 tr. zákona – Porušování práv k ochranné známce, obchodnímu jménu a chráněnému označení původu nebo podle § 149 tr. zákona – nekalá soutěž.

Množství problémů souvisejících se spory o doménová jména vede sdružení CZ NIC, které vydává pravidla k registraci doménových jmen v doméně CZ. V současné době je registrováno domén CZ – 534.694 (k 21. 3. 2009).

V globálním měřítku je Cybersquatting na vzestupu. Světová organizace duševního vlastnictví (WIPO) musela loni řešit 2.329 případů cybersquattingu, což byl osmiprocentní nárůst oproti roku 2007. Od roku 1999 řešila WIPO na 14 tisíc stížností, které se týkaly 26 tisíc doménových jmen. [12]

Phishing

Nakonec bych se zmínil o tzv. phishingu (rybaření), při kterém se podvody rozmáhají prostřednictvím emailové pošty. Dá se říci, že phishing většinou (není podmínka) začíná e-mailem, který se do posledního detailu tváří, jako by pocházel z nějaké instituce (častokrát nějaké banky apod.). V emailu je odkaz na stránku s podvodným obsahem, která se tváří jako skutečné stránky. Tam se od „oběti“ žádá vyplnění hesla, čísla kreditní karty, čísla účtů apod. Tyto údaje pak samozřejmě nejsou odeslány do banky ani do jiné instituce, ale přímo do rukou útočníků za jediným účelem – zneužití. Pravděpodobně poprvé se do České republiky dostal masivní případ phishingu v březnu 2006 v podobě falešného e-mailu od Citibank. Jednalo se o krátké oznámení, přijmu 2000 (v neurčené zahraniční měně) na váš účet. Abyste

[11] zákon číslo 273/2008 Sb. o Policii České republiky

potvrdili příjem této částky, máte podle instrukcí v e-mailu kliknout na uvedený odkaz a zadat vaše přihlašovací údaje, jak je uvedeno na obrázku číslo 7.

Obrázek 7 Případ CitiBank (zdroj: [13])

Po kliknutí na odkaz se skutečně otevře stránka Citibank, nicméně k tomu dojde přesměrováním z domény czechrepublic-online.com a kromě hlavního okna se skutečnými stránkami Citibank se otevře i vyskakovací okno, které však již nemá se Citibank nic společného. Zde jste pak vyzváni k zadání přístupových údajů do Citibank a tyto údaje jsou poté odeslány podvodníkovi, který může váš účet zneužít. Jediná cesta je nedůvěřovat, přemýšlet nad každou zvláštností a informace si ověřovat. Po útoku na CitiBank, nenechal phishing na sebe dlouho čekat a objevil se útokem na Českou spořitelnu, a.s, kdy nejen klienti České spořitelny, a.s. dostávali podvodný email, který se tvářil, jako by byl zaslán z banky.

3.3 Informační válka

Pojem informační válka (informatik war, infowar, informatik warfare) je v posledních letech stále častěji užíván i v českém jazyce a příležitostně zaměňován termínem kybernetická válka, který bývá vztahován ryze k válce na platformě výpočetní techniky a počítačových sítí. Její pojem není do současné doby ustálen a neexistuje jeho všeobecně přijatá definice. Jako jednu z definic tohoto pojmu zveřejnil Ing. Josef Nastoupil ve svém článku, který informační

válku definoval jako souhrn veškerých opatření a) pro ochranu vlastních informací a procesů na nich založených, jakož i pro ochranu informační techniky, b) pro působení na nepřátelské informace a procesy na nich založené, jakož i pro působení proti nepřátelské informační technice. [14]

Informační válku lze pak dále definovat ve dvou faktorech, kdy prvním faktorem prostředí, kde se válka odehrává. Pak je to válka pozemní, námořní, vzdušná, kosmická, světová, lokální apod. Druhým faktorem jsou prostředky vedení války. Jsou to např. zbraně konvenční, chemické, jaderné, letecké, bakteriologické a také informační apod. S tohoto logicky vyplývá, že informační válka je válka, která je vedena v oblasti informací nebo válka, v níž se bojuje informacemi. Zde je důležité podotknout, že „oblast informací“ neexistuje stejným způsobem jako země, moře, vzduch a vesmír. Podobně není informace zbraní ve stejném smyslu jako zbraň konvekční, chemická, jaderná nebo bakteriologická apod. Analogicky můžeme informační válku chápat jako válku o informace, tedy válku, kterou vedou lidé pracující s informacemi, případně válka, kterou charakterizují informace. [15]

Nejvýraznější vlastností prostředků informační války – infoware – je jejich dosah neboli potencionální schopnost útočníka na kterémkoliv místě světa, kde je dostupné připojení k síti (Internet), napadnout cíl na jiném a libovolně vzdáleném místě. Navíc, prostředky na přípravu a spuštění informatické zbraně jsou ve srovnání s potenciálními škodami, které by mohla napáchat, minimální. Takže potencionální útok je výrazně asymetrický. Útočník vystačí s minimálním vybavením, zatímco ochranné kroky se musí provádět plošně a ve velkém rozsahu, což vede k velkým nákladům na obranu. Obrana před informatickým útokem je i tak problematická. Za prvé je obtížné útočníkovi zabránit v dalších akcí a za druhé pozice útočníka nemusí být na území napadeného, což omezuje běžné prostředky obrany. S každým státem nemusí být sepsaná dostačující dohoda či spolupráce. [16]

Hlavním cílem informační války je oslabení pozice jiných států, podvrácení jejich státních základů a narušení státního zřízení pomocí informačního působení na politickou, diplomatickou, ekonomickou a sociální sféru společenského života prováděním psychologických operací a jiných demoralizujících a rozvracejících aktivit v kyberprostoru. Na vojenské úrovni jsou informační operace soustavou opatření, které se provádí v rozsahu vojenské moci státu podle rozhodnutí vojenských velení a jako součást strategických vojenských operací. Důležitým rysem informační války je, že mohou být použity jakékoliv vojenské a technické prostředky, které má stát k dispozici, ale zároveň musí být dodrženy právní, morální, diplomatické, politické a vojenské normy a zákony. Mezi důležité úkoly

informačních operací vojenských sil je působení na nepřítele v době, kdy teprve vzniká nebezpečí informační války. Zde má významnou úlohu zpravodajská služba. [16]

Informační válka se obvykle dělí do sedmi skupin, které jsou odděleně definované. Označuje se anglickými názvy příslušného infoware [16]:

- Command-and Control Warfare (C2W) – prostředky a válečná oblast zaměřená proti řídícím a velitelským centrům protivníka včetně komunikačních kanálů,
- zpravodajský (Intelligence) Warfare (IW) – prostředky skutečné informační války založené na syntéze a analýze informací, zde je hlavní úloha zpravodajských služeb,
- elektronický Warfare (PW) – elektronické zbraňové systémy zahrnující nejrůznější prostředky elektronické povahy, např. elektromagnetická děla nebo grafitové bomby, některé publikace zahrnují do této oblasti i kryptografické techniky,
- psychologický Warfare (PW) – psychologické metody manipulace veřejného mínění, mediální terorismus a ostatní metody psychologické války,
- hacker Warfare (HW) – metody a prostředky pro vojenské operace vedené hackerskými nástroji a postupy proti serverům a informatické infrastruktuře protivníka,
- ekonomická Informační Warfare (EIW) – ekonomické prostředky ovlivňující potenciál protivníka v ekonomické oblasti, vychází se z ekonomické hodnoty informace získané prostřednictvím IW,
- cyber Warfare (CW) – prostředky pro vedení kybernetické války.

Command-and Control Warfare

Podle amerického ministerstva obrany je C2W vojenskou strategií implementující informační válku na bitevním poli, jejíž součástí je fyzické zničení. Jedná se tedy o souhrn strategií informační války implementovaný ostatními prostředky informační války – elektronickými, zpravodajskými, kybernetickými a ekonomickými. V některé literatuře lze najít i označení C4I – Command, Control, Communication, Computer, Information Warfare. [16]

Pro provedení operace není nezbytné použít střelných zbraní, ale postačí použít prostředky působící v informační oblasti, jako počítačové viry, elektromagnetické zbraňové systémy nebo triviální přerušení dodávek elektrické energie. Dále jsou pak i situace, kdy ke zneškodnění nepřítele postačí zničení jedné osoby – vůdce organizace, strany anebo státu.

Podle RAND Corporation (Institut strategického plánování) existují tři základní typy operací pro odstranění vůdce [16]:

- operace zaměřená konkrétně proti osobě vůdce,
- operace zaměřené na iniciativu a přispívání k sesazení vůdce pomocí vyvolání vnitřních spiknutí a vzpour,
- operace přispívající k sesazení vůdce pomocí vnější vojenské invaze.

Zpravodajský warfare

Tyto zpravodajské prostředky jsou tzv. senzory umístěné v komunikačních kanálech. Zpravodajský infoware se zaměřuje na návrh, ochranu anebo potlačení systémů, které jsou zaměřeny na vyhledávání informací, na rozdíl od jiných infoware. Ty jsou určené k poškození informačních technologií. Senzor si můžeme představit nejen jako známé „štěnice“, ale i jako velmi komplexní systémy schopné např. napojení na systém řízení palby v reálném čase či zpracovat analýzu rozložení bitevního pole. [16]

Cílem zpravodajských prostředků je tedy získání informací nezbytných pro vedení vojenských operací a analýza situace a dezinformace nepřítele. Prostředky zpravodajského warfare můžeme rozdělit na prostředky útočné a prostředky obranné. [16]

Útočné prostředky infoware

Prostředky zpravodajské války patřící do oblasti infoware zpravidla vytvářejí rozsáhlé distribuované systémy, umožňující syntézu informací z mnoha kanálů. Tyto senzory je pak možné rozdělit do čtyř kategorií [16]:

- vzdálené senzory, kam můžeme zahrnout kosmické stanice, satelity se speciálním posláním a také seismické senzory nebo speciální akustické senzory,
- blízké senzory, které umožňují navádění a ovládání jako např. bezpilotní letecké nosiče (UMA, UAV[12]) vybavené specielními přehledovými technologiemi atd.,
- místní senzory, jedná se většinou o jednodušší zařízení pro detekci nejrůznějších změn okolí – akustické, gravimetrické, optické, atd.,
- zbraňové senzory umístěné přímo na příslušném bojovém prostředku nebo tvořící jeho součást – infračervený radar, atd.

[12] UMA – UnManned Aircraft, UAV – Unnanned Air Vehicle

V současné době není problémem zpravodajských prostředků infoware způsob získávání dat, ale problém co nejefektivnějšího zpracování získaných dat. Tyto systémy musí pracovat efektivně, rychle a spolehlivě.

Obranné prostředky infoware

Obranné prostředky slouží k ochraně „senzorů“. Hlavním řešením je znemožnění protivníkovi změnu senzoru, zjištění jeho funkce nebo, což je nejhorší případ, jeho zneužití ke klamání protistrany. Obranné metody se pak dají rozdělit do tří skupin [16]:

- fyzické zničení senzoru v okamžiku napadení nebo odhalení,
- vyřazení systému, které senzor používá, z provozu,
- utajování nebo klamání při umísťování senzorů – umístění rušivých elementů, falešné cíle nebo nástražné systémy, které se chovají podobně jako senzory, ale slouží pouze ke zmatení.

4 Charakteristika globalizace v oblasti zločinnosti

4.1 Korupce

Korupce je fenomén, který náš život, bohužel, provází denně. Podle průzkumu společnosti Gfk z 9/2006 více jak 56% populace v České republice považuje úplatek za běžnou součást života. V rámci Evropské Unie je Česká republika zařazené mezi státy s největší mírou korupce, podle hodnocení společnosti TI z 9/2005.

Korupcí, se podle definice z prezentace „Korupce a protikorupční politika ve veřejné správě“ rozumí: „takové jednání, kterým osoba v určitém kvalifikovaném postavení (volený zástupce, úředník zaměstnaný ve veřejné správě, zaměstnanec veřejného sektoru, ale i osoba na určité pozici v soukromém sektoru) zneužívá svého postavení k osobnímu obohacení nebo obohacení třetích osob, přičemž z tohoto jednání mohou mít přímý užitek osoby, které korupční jednání vyvolají a vždy vzniká škoda do různé míry určitelné skupině fyzických i právnických osob.“ [17]

Mezi hlavní příčiny korupce patří [18]:

- mocenský monopol,
- nekontrolovatelný rozsah možností mocenského (správního) uvážení,
- nízká úroveň veřejné kontroly.

A proto byla Ministerstvem vnitra České republiky přijatá pro rok 2006 až 2011, koncepce v boji proti korupci. Mezi hlavní principy boje proti korupci zařadila [18]:

- prevenci,
- průhlednost,
- postih.

Prevence

Z prevence vyplývá, že čím méně stát rozhoduje o životech občanů, tím menší je potřeba někoho korumpovat. V tomto bodu do své strategie MV zařadilo minimalizaci státních regulací, zásadní zjednodušení legislativy, snížení prostředků přerozdělovaných státem, debyrokratizace státní správy, omezení počtů zvláštních procesních pravidel (univerzální správní řád) a nakonec medializaci a veřejné odsouzení případů korupčního jednání. [18]

Průhlednost

Průhlednost při zadávání veřejných zakázek, čerpání prostředků z veřejných rozpočtů a rozhodování o právech a povinnostech občanů. V tomto bodu do své strategie MV zařadilo zprůhlednění systému zadávání veřejných zakázek, zprůhlednění systému čerpání prostředků z veřejných rozpočtů, zvýšení transparentnosti rozhodování veřejné správy, veřejná kontrola nad činností veřejných funkcionářů a jejich majetkovými poměry po dobu výkonu funkce, elektronizace agend veřejné správy a zřízení jednotné protikorupční linky. [18]

Postih

V posledním bodě, postih, je strategií MV ČR zpřísnění trestů v trestním zákonu i v zákonu o střetu zájmů. Zejména pak zvýšení trestů za prokázanou korupci změnou trestního zákona osobám odsouzeným za korupční jednání v souvislosti s veřejnými zakázkami, soutěžemi a dražbami, bude vždy vedle trestu odnětí svobody či peněžitého trestu uložen i trest zákazu činnosti, zavedení seznamu osob odsouzených za korupční jednání se zákazem účasti na veřejných zakázkách, tzv. „Černá listina“, zavedení principu odpovědnosti veřejných funkcionářů při správě cizího majetku, jako platí pro členy orgánů obchodních společností. Ten kdo způsobí škodu, bude za ni ručit celým svým majetkem. A v poslední řadě zřízení specializovaných justičních orgánů se zaměřením na korupci. [18]

4.2 Organizovaný zločin

Organizovaný zločin představuje závažné bezpečnostní riziko, ohrožující stabilitu světového hospodářského systému a v případě některých států i politický systém. Cílem organizovaného zločinu je dosažení maximálního zisku při vynaložení minimálních nákladů, a to zisku nejen materiálního, ale například i ve formě společenského a politického vlivu.

Organizovaný zločin je mimořádným bezpečnostním rizikem, ohrožujícím stabilitu světového hospodářského systému a v případě některých států i systém politický. Cílem organizovaného zločinu je dosažení maximálního zisku při vynaložení minimálních nákladů, a to zisku nejen materiálního, ale například i ve formě společenského a politického vlivu. Pro organizovaný zločin je typické soustavné páchání koordinované závažné trestné činnosti i aktivit, které tuto činnost podporují, zločineckými skupinami nebo organizacemi. Tyto organizace mají většinou vícestupňovou vertikální organizační strukturu.

Mezi základní znaky organizovaného zločinu patří [19]:

- trvající spolupráce více osob, z nich každá má pevně stanovené specifické úkoly,
- páchání závažné trestné činnosti s úmyslem získat prospěch nebo moc,
- vysoká profesionalita, tj. stabilita, koncepčnost, důkladná příprava akcí, konspirace disciplína, přísně stanovené normy chování a kontroly, dokonalé vybavení,
- koncentrace moci v rukou vůdce skupiny organizovaného zločinu,
- používání násilí nebo jiných prostředků zastrašováním uvnitř skupin, mezi skupinami i vůči okolnímu prostředí,
- využívání kontaktů na veřejné činitele, veřejnou správu, orgány zabývající se prosazováním práva, ekonomiku a sdělovací prostředky. Tyto kontakty slouží k zajišťování vlastních zájmů prostřednictvím spolupráce, kompromitování, korupce, nátlaku,
- snaha získat potřebné informace a využít je pro zvýšení zisků a snížení rizik,
- snaha o ovládnutí určité oblasti (geografické a/nebo určitého typu „podnikání“),
- aktivity na mezinárodní úrovni.

Organizovanou kriminalitu lze definovat jako druh skupinové trestné činnosti páchané organizovanou zločineckou skupinou nebo zločineckou organizací, vyznačující se dlouhou dobou trvání, dělbou činnosti, plánovitostí a orientací na vysoký zisk nebo na získání vlivu na veřejný život. Výjimečně mohou být zločinecké organizace motivovány také ideologicky (např. teroristické organizace). [20]

Ze statistických průzkumů vyplývá, že k nejčastějším kriminálním deliktům, do kterých je zapojen organizovaný zločin, nebo u kterých je patrný zárodek organizovaného zločinu, patří [21]:

- drogová kriminalita, včetně nelegálního obchodu s prekurzory,[13]
- finanční kriminalita,
- ilegální obchod se zbraněmi a výbušninami,
- imigrační kriminalita (pašování lidí přes hranice států),
- korupce na různých úrovních,
- krádeže a vykrádání vozidel, pojistné podvody,
- krádeže kulturních památek a obchod s nimi,
- kriminalita spjatá s nočním životem (prostituce, herny),

[13] Prekurzor – jedná se o výchozí chemickou látku včetně např. určitých léčiv nebo meziprodukt, z něhož vzniká výsledný produkt – droga.

- mezinárodní pornografie, využívající nezletilé osoby,
- (mezinárodní) terorismus,
- násilná trestná činnost, včetně nájemných vražd, únosů, loupeží, ozbrojených přepadení, vydírání,
- nezákonný obchod a podnikání,
- nezákonný obchod s ohroženými druhy flóry a fauny,
- obchod s lidmi (např. za účelem prostituce), s lidskými orgány,
- obchod se strategickým vojenským materiálem (obohacený uran, plutonium, chemické a biologické látky, technologické a počítačové komponenty atd.),
- organizovaný zločin,
- padělání měny, bankovek a platebních karet,
- padělání pasů a víz, úředních listin,
- počítačová kriminalita,
- porušování autorských práv, průmyslových vzorů, průmyslového a duševního vlastnictví včetně audio, video a softwarového pirátství,
- racketeering (vymáhání ochrany, „výpalného“) aj.

V současné době je rozvoj nových technologií na vrcholku, a to má do jisté míry dopad na organizovaný zločin a činnost bezpečnostních služeb. Nové technologie jsou vnímány ve dvou rolích [21]:

- Jako prostředek nebo cíl (předmět napadení) páchané trestné činnosti zločinci.
- Jako nástroj (prostředek) odhalování, prokazování a dokumentování spáchaných trestných činů.

4.3 Terorismus

Termín terorismus byl poprvé užit ve 14. století ve francouzštině, první známé anglické užití bylo zaznamenáno v roce 1528. Význam a užití jsou dobře popsány už v Machiavelliho Vladaři v roce 1513, samotný termín zde však zatím užit není.

Slovo terorismus se blízko dnešnímu smyslu objevilo poprvé v dodatku Slovníku Francouzské akademie v roce 1798 a v Encyklopedii Britanice v roce 1799. V průběhu druhé poloviny 19. a první poloviny 20. století jeho význam značně varioval. Byli jím např. označováni nepřátelé absolutistických zřízení, zejména anarchisté a jejich činy.

Terorismus a jeho charakteristické znaky lze tedy registrovat již v době před mnoha sty lety. Např. najatí vrahové v Persii a Sýrii za úplatu či společenskou výhodu vraždili kohokoliv, kdo byl mocnými označen a nebylo možno ho přesvědčit, aby změnil své názory či postoje. Velice často bylo zneužíváno přesvědčení věřících a náboženských fanatiků, jejichž prostřednictvím bylo uskutečňováno násilí a zastrašování. [22]

V druhé polovině 20. století, kdy zejména na Západě byla válka znemožněna jadernou hrozbou, se jeho význam dále posunul, často je přijímána definice, že je „ekvivalentem válečné zločinnosti v době míru“. [23]

V 21. století se problematika a nástroje proti terorismu dostala do popředí po útocích na New York a Washington ze dne 11. září 2001. V České republice je tato problematika aktuální i v současné době a to díky vyjednávání mezi USA a Českou republikou, v souvislosti s umístěním radaru protiraketové obrany USA v Brdech. V případě, že by došlo k výstavbě tohoto radaru, tak by se Česká republika stala, dle mého názoru, terčem útoku.

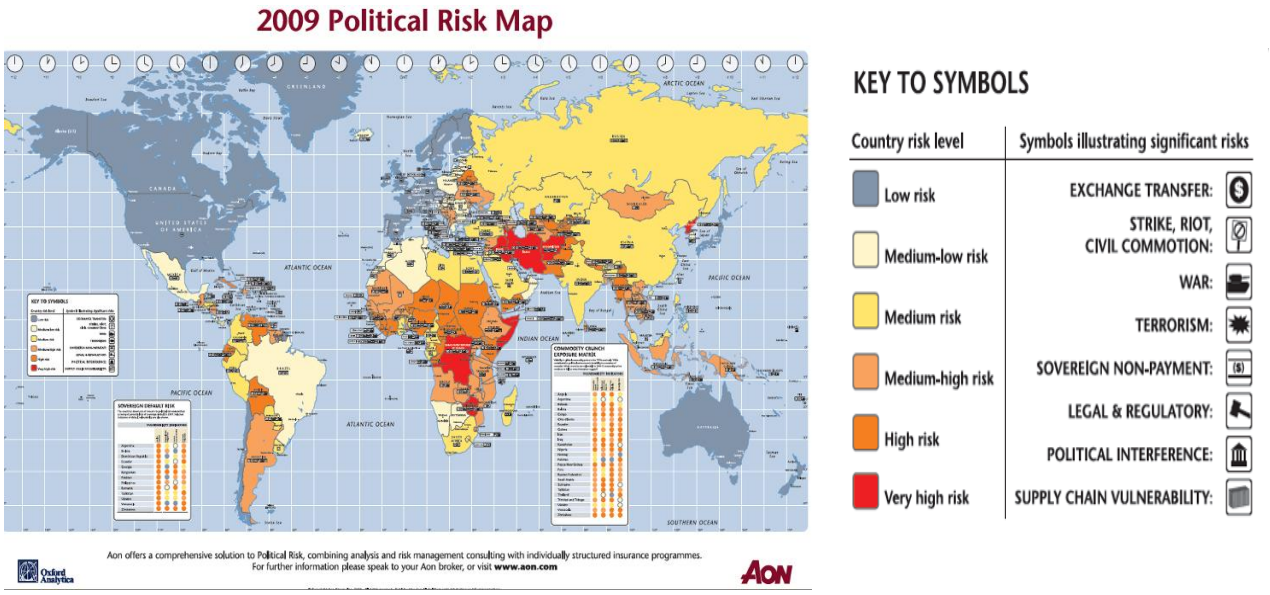
Terorismus lze definovat mnoha způsoby. Mezi často užívanou definici najdeme v americkém zákoníku a dalších amerických příručkách. Říká, že terorismus je předem vypočítané použití násilí nebo hrozby násilím k dosažení politických nebo náboženských a ideologických cílů prostřednictvím zastrašování, donucením nebo působením strachu, a tím způsobit velkou škodu nebo usmrtit osoby k dosažení cíle. [24]

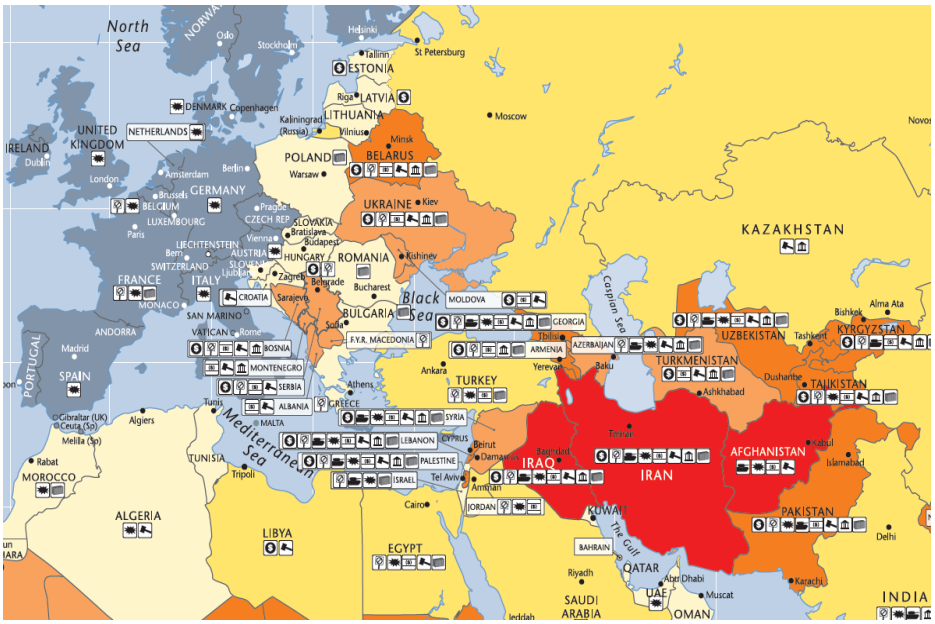
Jako další zajímavou definici terorismu bych uvedl definici FBI: *"Terorismus je nezákonné použití síly a násilí proti osobám či majetku se záměrem zastrašit nebo donutit vládu, civilní obyvatelstvo či jeho určitou skupinu, a tím dosáhnout politických nebo společenských cílů.“* [25]

Jednou za čas se v českých médiích objevují zmínky o prohlášení globálně působící pojišťovací firmy AON, které konstatují bezpečnostní prostředí v ČR z hlediska ohrožení terorismem. Česká republika patří mezi státy v Evropě s nízkým rizikem, jak je zobrazeno na obrázku číslo 8.

I když z obrázku 8 vidíme, že Česká republika mezi státy s nízkou rizikovostí, tak společnost AON zvýšila stupeň rizikovosti České republiky kvůli sídlu rozhlasové stanice Svobodná Evropa v Praze, blízkosti hranice Ruské federace a kvůli podpoře války v Iráku. V neposlední řadě se dá očekávat, že riziko se zvýší z důvodu již případné výstavby radarové základny v Brdech.

Jak se staví k problému bezpečnostní komunita České republiky? V této souvislosti je třeba definovat pojmy hrozba a riziko, jejich vzájemný vztah. Hrozbou se rozumí objektivní skutečnost, která může znamenat negativní dopad pro Českou republiku. Hrozbě lze čelit protiopatřeními, které jsou velice nákladná, a přitom není nikdy stoprocentní. Rizikem se výsledně rozumí „to, co stát podstupuje“, aby jeho snaha redukovat hrozby nepřekročila únosnou míru. Zde platí nepřímá úměra, že čím je který chráněný zájem střeženější, tím je úspěch útoku méně pravděpodobný.





Obrázek 8 Politicky bezpečnostní mapa (zdroj: [26])

Bezpečnostní komunita státu proto vyvíjí široké spektrum aktivit, s cílem přípravy a prevence celé řady možných ohrožení a rizik. Jakýkoliv zahraničně-politický vývoj byl a je neustále monitorován a vyhodnocován, se zvláštním zřetelem na následující faktory, které lze považovat za trvalé zadání všech zpravodajských služeb České republiky [27]:

- vývoj by mohl znamenat přímé vojenské ohrožení státu,
- vývoj by mohl znamenat aktivaci vojenských spojeneckých závazků České republiky,[14]
- vývoj by mohl ohrozit jednotky Armády České republiky v zahraničí, dislokované tam v rámci plnění humanitárních misí,
- vývoj by mohl ohrozit jiné občany České republiky (civilisty), nacházející se v prostoru konfliktu (turisté atd..),
- vývoj by mohl ohrozit personál zastupitelských úřadů České republiky,
- vývoj by mohl zapříčinit migrační vlnu, která by zasáhla i Českou republiku, nebo by Českou republiku nutila podílet se na jejím zvládnutí materiálně,
- vývoj by mohl aktivizovat určité kruhy v České republice v České republice do té míry, že by se staly vnitřní bezpečnostním rizikem (imigranti, extrémisté atd.),
- vývoj by mohl znamenat ohrožení určitých skupin, žijících v České republice (náboženské skupiny),
- vývoj by mohl z České republiky učinit pravděpodobnější cíl teroristického útoku nebo adresáta věrohodných výhrůžek útokem,
- vývoj by mohl poškodit hospodářské zájmy České republiky (bezprostředně: ztráta trhů/odbytišť/zakázek, nemožnost dovážet určité klíčové komodity nebo zvýšení cen těchto komodit v samotném důsledku akcelerace konfliktu; sekundárně: totéž, ale v důsledku diplomatických/politických kroků České republiky – zaujmutí politického postoje, který může být konkrétní zemí či zeměmi hospodářsky bojkotován).

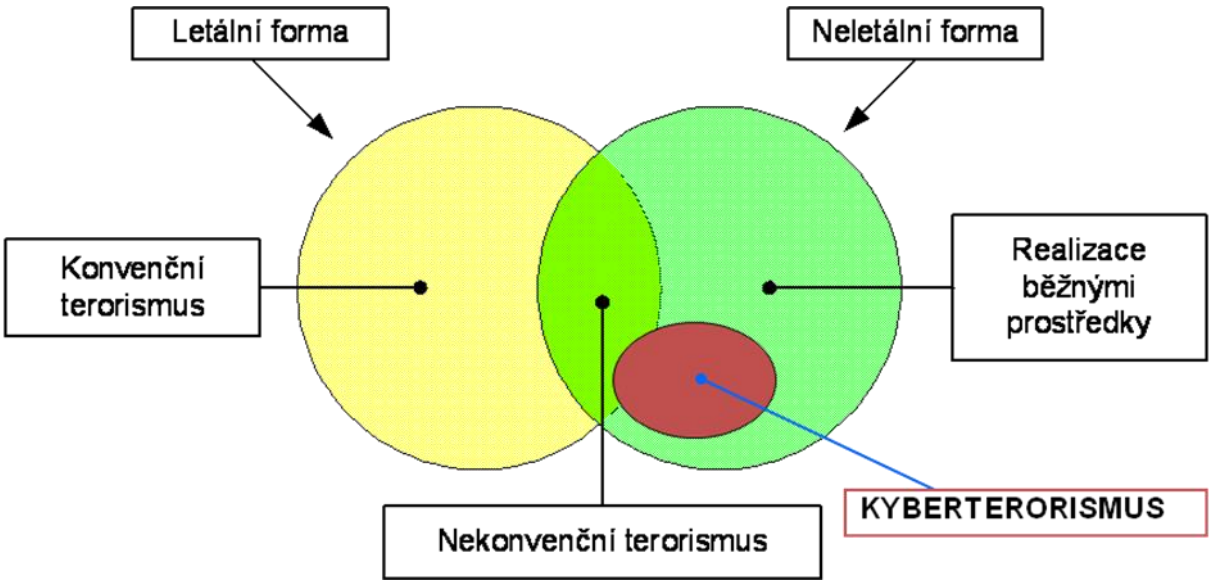
4.4 Kyberterorismus

V současné době jsme zaznamenali velký růst globalizace a centralizace informačních systémů a technologií a v důsledku roste logicky i jejich zranitelnost. Právě z tohoto důvodu je v popředí zájmu teroristů i pracovníků bezpečnostních sborů specifická oblast informačního terorismu – kyberterorismus (anglicky – cyberterrorism).

[14] Článek 5 Washingtonské smlouvy

Kyberterorismus je možné definovat jako zneužití počítačových technologií proti osobám či majetku za účelem vyvolání strachu nebo vydírání a vymáhání ústupků, zaměřené proti vládním institucím nebo civilní populaci, případně proti jejich segmentům, pro podporu politických, sociálních, ekonomických, případně jiných cílů, zaměřené na informační systémy používané cílovým objektem. [28]

Obecně lze říci, že jde o zneužití počítačových technologií proti osobám nebo majetku, za účelem vyvolání strachu nebo vydírání a vymáhání ústupků, kterou jsou nejen zaměřené na vládní instituce, ale i na civilní obyvatelstvo. Grafické začlenění pojmu kyberterorismu do množiny terorismu ukazuje obrázek 9.



Obrázek 9 Schéma začlenění pojmu kyberterorismu do množiny terorismu (zdroj: [29])

Jedná se o nový rys, který v budoucnu zaujme plošnost a brutalitu. Politický terorismus se až na výjimky zaměřoval na vybrané individuální cíle, představitelé státní a hospodářské moci. Tradiční terorista chtěl, aby hodně lidí přihlíželo, ale málo umíralo. Účelem útoku nového teroru je naopak zabít co nejvíce lidí, způsobit rozsáhlé materiální škody a hospodářské ztráty. Imperativem je vyvolat celospolečenskou paniku, strach a hrůzu, otřást psychikou společnosti, zviklat víru lidí ve schopnost vlády chránit své občany.

Obecně jsou známy dvě metody teroristických útoků [30]:

- cílem útoku je zničení protivníka informačního systému a systému závislých na informačních a komunikačních technologiích,
- informační technologie jsou využívány jako nástroj útoku pro manipulaci a zneužití cizích informačních systémů, ke krádeži nebo změně dat, případně přetížení a zahlcení informačních systémů.

Mezi hlavní možnosti k uplatnění kyberterorismu poskytuje své prostředí internet. Ten umožňuje teroristickým skupinám i jednotlivcům rychlou a anonymní výměnu informací, poskytuje prostor pro šíření jejich ideologií a názorů. Také umožňuje získávání nových sympatizantů a aktivistů. V dalších případech se internet stává bránou k průniku do počítačových sítí, a tak poskytuje příležitost k vedení kyberteroristických operací. Dosud je známým faktem, že teroristické skupiny využívají „zatím“ internet více ke své propagaci a ke vzájemné komunikace mezi sebou, než ke kybernetickým útokům. [30]

Formy kyberterorismu se dají shrnout do několika charakteristických bodů. Může se jednat o [30]:

- kriminální akce s cílem získání finančních prostředků z cizích bankovních kont. Všechny banky nepoužívají dokonalé bezpečnostní systémy a toho v mnoha případech využívají právě kyberteroristé, nezřídka i přímí zaměstnanci finančního ústavu.
- snahy o získání výhody v oblasti konkurenčního zpravodajství (competitive inteligence). V praxi lze přece zveřejnit negativní informace o představitelích společnosti, očernit je, napadnout nebo pomluvit. Obrana je zpravidla nemožná, což platí zvláště v případech anonymního útoku na internetu.
- možnost napadení či dokonce likvidace počítačového systému. Kebyrterorista pak provede útok na slabá místa informačního systému nebo zaměstnanci zaútočí na organizaci zevnitř. Z výzkumu vyplývá, že velká většina organizací nedostatečně chrání svá data a techniku.
- zájmy hackerských sdružení jsou další velkou oblastí kyberterorismu. Zpravidla bývá jejich záměrem dokázat světu, že mohou napadnout či zničit počítačový systém z internetu a dokázat si svou výjimečnost a nepostižitelnost. Finanční, ale i morální ztráty postižených organizací bývají vysoké, mnohdy na úrovni mnoha desítek milionů USD.

- snahy vlád některých zemí, které se intenzivně připravují na vedení kybernetické války určitým opatřením již nyní. Tyto státy organizují operace, které mají v praxi potvrdit úspěšnost jejich boje proti kyberterorismu, ale přitom svoji skutečnost utajují a maskují.
- další závažný problém při využití internetu k šíření extrémistických názorů, pornografie, návodů na výrobu jaderných zbraní, omamných prostředků, výbušin apod.

4.5 Drogová kriminalita

Drogová kriminalita patří k nejčastějším kriminálním deliktům, do kterých je zapojen organizovaný zločin, a která je hlavní zdrojem terorismu ve všech podobách. Pojem droga je velice těžké specifikovat a ani v Trestním zákoně České republiky nenalezneme ustanovení, které by obsahovalo pojem droga. Využíván je jen pojem návyková látka[15]. Na začátku 21. století dosáhlo zneužití omamných a psychotropních látek v globálním měřítku nevídaných rozměrů. Proto je nutné neustále přizpůsobovat zákony tomuto fenoménu zvané drogová kriminalita. Trestní zákon v současné době zakotvuje §§ 187, 187a, 188 a 188a tr. zákona, které vymezují kriminální delikty spojené s drogami.

Jako všude jinde, tak i česká drogová scéna se začala po roce 1989 řídit ekonomickými pravidly. Současná drogová scéna je již velmi dobře organizovaná. Zločinecké organizace působící na území České republiky zavedly dumpingové ceny a rozšířily sortiment nabízených drog na „evropskou“ úroveň.

Mezi významné faktory ovlivňující nelegální mezinárodní obchod s drogami na našem území patří [31]:

- strategická poloha ČR v centru Evropy, a tím i na hlavních tranzitních drogových trasách,
- vyšší propustnost a špatná kontrolovatelnost státních hranic ČR,
- rozvinutý a kvalitní chemický průmysl a zejména velice kvalitní báze ilegálních výrobců, kteří z lehce dostupných ingrediencí pro domácí výrobu pervitinu jsou schopni zásobit svou produkcí i zahraniční zájemce,

[15] § 89 odst 10 trestního zákona - návykovou látkou se rozumí alkohol, omamné látky, psychotropní látky a ostatní látky způsobilé nepříznivě ovlivnit psychiku člověka nebo jeho ovládací nebo rozpoznávací schopnosti nebo sociální chování.

- tradičně dobrý organizační a inteligenční potenciál obyvatel ČR, který vyměnil trestnou činnost v oblasti nelegálního směnárenství za perspektivnější obchod s drogami (stále více se mezi drogovými kurýry objevují i čeští občané),
- rozpad bývalého SSSR a bývalé SFRJ vedl k poměrně masivnímu proudu ekonomických a politických běženců i na území ČR. Této situace využily i profesionální zločinecké gangy, které se v ČR rychle zabydlely a působí zde jako mezičlánek velkých zločineckých organizací, nebo realizují svou nelegální aktivitu přímo na území ČR se zaměřením na české občany,
- významný podíl na mezinárodním nelegálním obchodu mají i čeští reemigranti, využívající k této činnosti svých prostředků, kontaktů i zkušeností získaných v cizině,
- ČR je stále označována za velice lukrativní stát pro „propírání“ peněz z organizovaného zločinu obecně, tedy i peněz z nelegálního obchodu s drogami (nedostatky v legislativních opatřeních upravujících pohyb financí usnadňují vytváření fungujících, ale i fiktivních zahraničních firem sloužících ke krytí jiné než povolené, případně i protizákonné činnosti),
- vzrůstající životní úroveň části populace má za následek nárůst kupní síly občanů disponujících dostatečnými finančními prostředky pro experimentování s drogami, případně pro přechod od aplikace levnějších druhů drog (marihuana, LSD) k dražším (extáze, heroin) s tím, že zejména mezi částí mládeže a podnikatelskou vrstvou je stále abúzus drog spojován s pojmem modernosti nebo dokonce s vysokým prestižním statutem (užívání drog je dokonce vnímáno jako míra svobody jednotlivce),
- nárůst abúzu drog souvisí také se zvyšujícími se požadavky na výkonnost a úspěšnost jedince na náročnějším trhu pracovních sil (nejen v podnikatelské sféře, ale zejména s obtížemi při zaměstnávání mladistvých bez kvalifikace) a často i s řešením případného nezdaru a selhání,
- specifickým problémem se stává abúzus drog mezi dětmi a mládeží z romské populace, kteří nemalé částky získané trestnou činností (obvykle z krádeží nebo vloupání do aut) utrácejí za drogy,
- nastupující éra internetu, který již zdomácněl i u nás, umožňuje každému, aby získal návody na výrobu drog, vyměnil si kontaktní adresy, případně další toxikomanické zkušenosti.

Jako zajímavý případ, který byl v poslední době pravomocně odsouzen a spadá do drogové kriminality šířené prostřednictvím veřejné sítě Internet, bych uvedl prodej rostliny s názvem SALVIA DIVINORUM (šalvěj divotvorná), která obsahu látku salvinorin A s halucinogenními účinky. Tu prodávali dvě fyzické osoby M. J. a M. J. prostřednictvím internetových stránek www.botanic.cz, provozované firmou M. J., se sídlem Praha 4, čímž umožnili prodej této vysoce halucinogenní rostliny teoretický kterékoliv osobě, která má přístup k internetu. Dle rozsudku Obvodního soudu pro Prahu 4, který nabyl právní moc dne 25. 11. 2008, jsou obžalovaní M. J. a M. J. vinni, že v přesně nezjištěné době, nejméně od 12. 12. 2006 do 17. 12. 2007 na internetových stránkách www.botanic.cz nabízeli k prodeji rostlinu SALVIA DIVINORUM (šalvěj divotvorná) včetně extraktů z této rostliny s tím, že zde popisovali účinky a způsob aplikace, kdy uvedená rostlina obsahuje látka salvinorin A, který má halucinogenní účinky, nepříznivě ovlivňuje psychiku člověka, jeho rozpoznávací a ovládací schopnosti, tedy sváděli jiného ke zneužívání jiné návykové látky než alkoholu a zneužívání takové látky šířili, taková čin spáchali veřejně přístupnou počítačovou sítí, čímž spáchali trestný čin šíření toxikomanie dle § 188a odst. 1, 2 písm. b) tr. zákona formou spolupachatelství dle § 9 odst. 2 tr. zákona a odsuzují se podle § 188a odst. 2 tr. zákona k trestu odnětí svobody v trvání jednoho roku a podle § 58 odst. 1 tr. zákona se výkon tohoto trestu podmíněně odkládá na zkušební dobu, podle § 59 odst. 1 tr. zákona v trvání dvou a půl let. [32]

Z důkazů pak bylo zřejmé, že obžalovaní museli vědět, jaké účinky nabízená látka má, když jejich účinky popisovali na webových stránkách jejich firmy. Jejich obhajoba, že zákazníci byli poučováni o tom, že produkt není určen k vnitřnímu užití (viz obrázek 10), je však nemůže vyvinit z žalovaného jednání, neboť museli předpokládat, že velký zájem o nákup rostliny není způsoben snahou o opakované zkoumání rostliny nebo přáním mít rostlinu v herbáři. Museli být si vědomi toho, že rostliny jsou zákazníky zneužívány nebo mohou být zneužívány a to především z řad narkomanů, ale i dalších především mladých lidí pokoušející se experimentovat. [32]

Na závěr této kapitoly bych odkázal na přílohu této práce, kde je ze statistiky drogové trestné činnosti v České republice za rok 2008 zřejmé, že drogová kriminalita zasahuje v globálním měřítku i zde v České republice.

Obrázek 10 Salvia divinorum (zdroj: [32])

5 Vliv globalizace na bezpečnostní situaci

V současné době lidstvo disponuje širokými možnostmi vědy a techniky, která svou dokonalostí na jedné straně dokáže lidské existenci ulehčit, na straně druhé však může působit destruktivně.

Pokud se zaměříme na hrozby, tak pod tímto označením můžeme chápat cokoliv, co nějakým způsobem může vést k nežádoucí změně informací, chování systému nebo ovlivnit jeho parametry. Sem se zahrnují osoby, prostředky, události nebo i myšlenky, které představují nějaké potencionální narušení důvěrnosti, integrity, dostupnosti nebo legálnosti použití systému. Útok je realizace hrozby. Ochranou proti hrozbě a útokům jsou pak veškeré fyzické mechanismy, definované politiky nebo procesy, které slouží k ochraně systému nebo obecně majetku před hrozbou nebo útokem.

Velmi důležitým momentem je zde riziko, jehož míru můžeme vztáhnout k hodnotě chráněného majetku. Riziko je pravděpodobnost, že dojde ke škodlivé události. Je závislou proměnnou a dá se odhadnout analýzou rizik. Je reakcí na hrozbu.

Hrozby se dají kvalifikovat jako úmyslné (např. průnik útočníka do systému) a neúmyslné, kdy ohrožení může např. vzniknout chybou operátora. Úmyslné hrozby se dále dají rozdělit na hrozby pasivní a hrozby aktivní.

Z hlediska bezpečnosti informačního systému můžeme hrozby rozdělit do čtyř základních skupin [33]:

1. **Únik informace** neboli případ, kdy informace důvěrného charakteru je prozrazena neautorizovanému subjektu nebo je jím odhalena. Únik informace pak může vést k přímým útokům se značným dopadem.
2. **Narušení integrity** zahrnuje porušení konzistenci dat, kdy může dojít k vytvoření nových dat či změně nebo vymazání stávajících dat neautorizovaným subjektem.
3. **Potlačení služby**, ke které dochází v případě, kdy je úmyslně bráněno přístupu legitimního subjektu k informacím nebo jiným systémovým zdrojům. Příkladem jsou,

známé útoky DoS[16], kdy úmyslné vytvoření vysoké zátěže zdroje nelegitimními a jalovými žádostmi vede k neúspěšným pokusům o přístup legitimních subjektů.

4. **Nelegitimní použití** znamená, že zdroj je používán neautorizovaným subjektem nebo neadekvátním způsobem. Příkladem může být průnik do systému a používání placených služeb, aniž by docházelo k faktickému vyúčtování a zaplacení služby.

5.1 Aktivační hrozby

Aktivační hrozby a jejich význam spočívá v tom, že jejich realizace vede k bezprostřednímu vytvoření základní hrozby, a i k přímému ohrožení bezpečnostních parametrů systému. Odtud také plyne jejich název, neboť aktivují základní hrozby. Dají se rozdělit na penetrační hrozby a implantační hrozby [33]:

Penetrační hrozby

- **Maškaráda** – případ, kdy se jedna entita (osoba nebo systém) vydává za jinou entitu. Toto je jeden z nejběžnějších způsobů narušení bezpečnostního perimetru systému, např. „login“ perimetru. Neautorizovaná entita v tomto případě „přesvědčí“ příslušný ochranný systém o tom, že je odpovídající autorizovaná entita a tak využívá všech práv a privilegií fiktivní autorizované entity. Hackeři používají maškarádu velmi často a slaví tak nejeden úspěch.
- **Obejití řízení** – v tomto případě útočník využije systémové nebo bezpečnostní slabiny, k získání neautorizovaných práv nebo privilegií.
- **Narušení autorizace** – spočívá ve zneužití autorizovaného přístupu ke zdroji pro neautorizované účely. Takový útok musí být veden zevnitř systému uživatelem, která má k danému zdroji přístup a nejedná se ani tak o selhání systémové jako o selhání personální.

Implantační hrozby

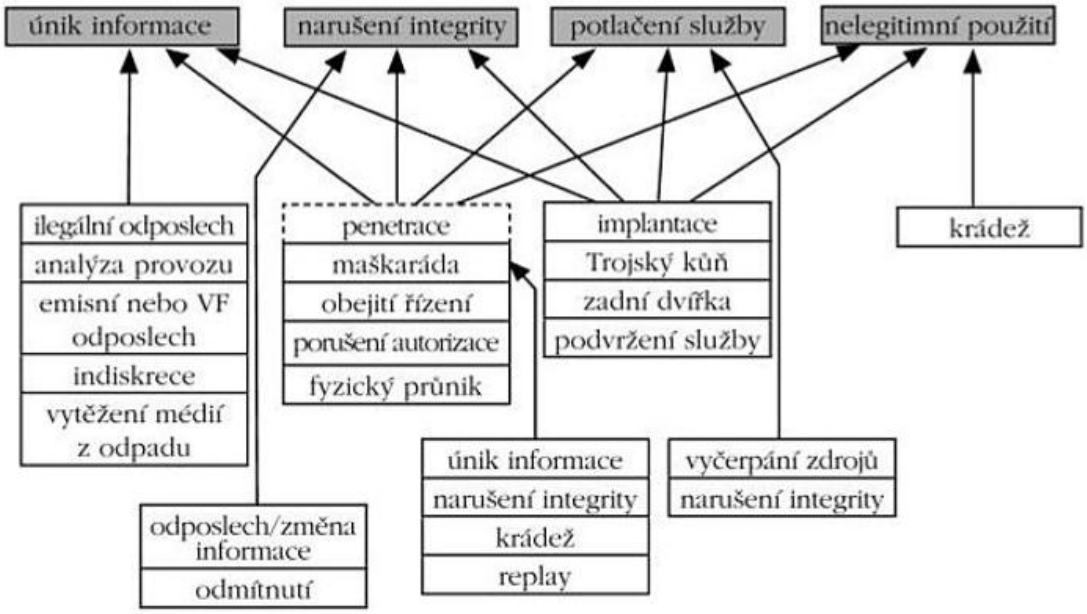
- **Trojský kůň** – jedná se o historicky nejběžnějším případem vložené hrozby, kdy software obsahuje neviditelnou nebo při běžném provozu nepozorovatelnou část, která po spuštění naruší bezpečnostní prvky systému. Příkladem může být např. běžný

[16] DoS – Denial of Service, způsob útoku v distribuovaném informačním systém, kdy jsou přenosové kanály zahlceny záplavou jalových informací generovaných útočníkem, což v důsledku vede k nedostupnosti informačních zdrojů.

program – textový editor, který umožňuje uložení informací o aktivitách uživatele, např. text, který uživatel napsal, ukládá do skryté části systému, odkud mohou být tyto informace vyzdviženy autorem trojského koně.

- **Zadní vrátka** – jedná se o část systémového software, která umožňuje při poskytnutí specifického datového řetězce na svůj vstup, obejít nástroje bezpečnostní politiky systému. Příkladem může být systém přihlašování uživatelů (login), kdy pro specifický identifikátor uživatel jsou vynechány všechny běžné kontroly hesel.

Analyzujeme-li základní a aktivační hrozby v nějakém systémovém prostředí, můžeme identifikovat některé hrozby, které mohou vést k realizaci i několika základních hrozeb. Hrozbám, které jsou podkladem pro realizaci z několika základních hrozeb, říkáme podkladové hrozby. Vztah mezi základními hrozbami a podkladovými hrozbami ukazuje obrázek 11. V tabulce 3 je pak popis jednotlivých hrozeb.



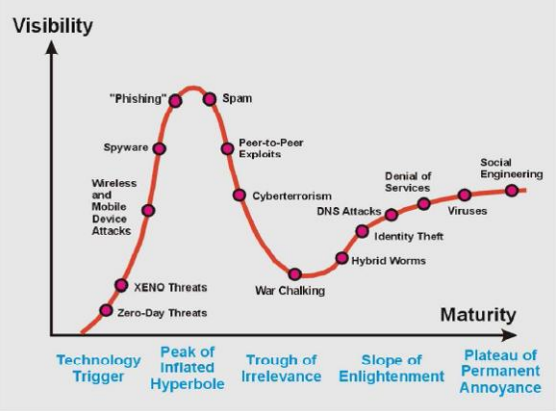
Obrázek 11 Vztah základních a podkladových hrozeb (zdroj: [33])

Tabulka 3 Popis jednotlivých hrozeb (zdroj: [33])

Hrozba	Popis
Porušení autorizace	Osoba, která je autorizována k použití zdroje pro jistý účel jej použije k jinému, neautorizovanému účelu.
Obejití řízení	Útočník využije bezpečnostních mezer v systému nebo jeho slabin.
Potlačení služby	Omezení legitimního přístupu k informacím nebo jiným zdrojům v síti.
Nezákonný odposlech	Informace je získávána monitorováním přenosového kanálu.
Emisní nebo VF odposlech	Informace je extrahována z vysokofrekvenčního vyzařování nebo emisí či jiných elektromagnetických jevů, ke kterým dochází při provozu elektronického zařízení.
Nelegitimní použití	Zdroj je používán neautorizovanou osobou nebo neautorizovaným způsobem.
Indiskrece	Autorizovaná osoba prozradí důvěrnou informaci neautorizované osobě z neopatrnosti nebo za úplatu.
Únik informací	Získání důvěrné informace neautorizovanou osobou nebo systémem.
Narušení integrity	Konzistence dat je narušena jejich neautorizovaným vytvořením, úpravou nebo vymazáním.
Změna dat při přenosu	Přenášená data jsou během přenosu informačním kanálem změněna, odstraněna nebo zcela vyměněna.
Maškaráda	Jedna entita (osoba nebo systém) se představuje jako jiná entita.
Vytěžení odpadových médií	Informace je získávána z magnetických nebo papírových médií, vyhozených do odpadu.
Fyzický průnik	Útočník získá kontrolu nad systém proniknutím k jeho ovládacím prvkům.
Replay	Zachycená kopie legitimní transakce je využita pro opětovný proces s nelegitimním úmyslem.
Popření skutečnosti	Strana zúčastněna ve vzájemné komunikaci později popře, že k takové komunikaci došlo.
Vyčerpání zdrojů	Jiný zdroj, např. port, je úmyslně natolik zatížen, že je znemožněno používání služby, která je na něj vázána, řádnými uživateli.
Podvržení služby	Podvržený systém nebo systémová komponenta, které se vůči uživatelovi chovají jako běžná součást systému, slouží k získání citlivých informací od důvěřivého uživatele.
Krádež	Kritický prvek bezpečnostního systému (např. přístupová karta) nebo veškerá citlivá informace jsou zcizena.
Analýza provozu	Informace je neautorizovanou entitou získána pomocí sledování provozu a výběrem podstatných jeho částí.
Zadní vrátka	Do systému je zabudována vlastnost nebo vložena součást, která při jisté konstelaci vstupních dat umožní obejít bezpečnostní mechanismus.
Trojský kůň	Software obsahuje zdánlivě nevinou nebo neviditelnou část kódu, který – pakliže je spuštěn – ohrozí bezpečnost uživatele.

5.2 Hrozby z hlediska časového vývoje

Dále se na hrozby můžeme podívat z časového vývoje, jak je znázorněno na obrázku 11, na svislé ose (y) diagramu, je vyjádřena míra výskytu dané hrozby (její „viditelnost“, publicita, věnovaná odborná pozornost). Na ose horizontální (x) pak je znázorněna vyspělost hrozby (u produktů vyspělost technologie, řešení). Jinými slovy se dá říci, že v levé části osy (x) nalezneme nové hrozby. V pravé části se nachází „ustálené“, velmi vyspělé hrozby. [34]



Obrázek 12 „Kybernetické hrozby ke konci roku 2004 znázorněné pomocí Hype Cyrcle diagramu společnosti Gartner“ (zdroj: [34])

Každá hrozba nebo produkt zpravidla ve svém historickém vývoji prochází postupně grafem zleva doprava. Nejprve se objevuje s nějakou novou technologií, aby se za nějakou dobu mohla ustálit a stala se tak stálou, vyspělou hrozbou, které je nezbytně nutné věnovat pozornost. Některé hrozby, ale nemusejí projít všemi oblastmi, mohou se ztratit, přestat existovat a v druhé polovině pravé části grafu se nemusejí pak již dále objevovat.

Křivka grafu z obrázku 12 je rozdělena do pěti základních, logických oblastí, které mají svá specifika [34]:

První oblast – technology Triger (technologičtí spouštěči) – jedná se o oblast zcela nových hrozeb, které se objevují s novými, perspektivními technologiemi, které se začínají objevovat na trhu. Obecně novinky na trhu nebo ve sledované oblasti. V době vydání grafu tam patřily hrozby typu.

1. „Zero-Day“ – cílené útoky na technologické chyby výrobců SW nebo HW produktů ještě předtím, než výrobce distribuuje opravné nástroje (např. SW patche).

V okamžiku, kdy někdo zjistí slabinu technologie nebo zařízení, začne ji ve velkém a cíleně napadat.

2. XENO (eXtendet Enterprise Networks Overseas) hrozby se začínají objevovat v důsledku outsourcingů v oblasti informačních technologií, kdy není dostatečně zabezpečená ICT bezpečnost, nejsou vyjasněny vztahy a odpovědnost mezi outsourcovaným a outsourcujícím subjektem.
3. Útoky na mobilní zařízení a bezdrátové (WiFi) produkty. V těchto zařízení se vyskytují viry podobně jako v klasické výpočetní technice.

Druhá oblast – Peak of Inflated Hyperbole („vrchol zvýšeného zájmu“) – jedná se o oblast, do které se řadí hrozby, o kterých se nejvíce hovoří, je jim věnována maximální odborná pozornost, směřováno maximální úsilí na ochranu. Oblast usilovných „marketingových“ aktivit výrobců ochranným prvků. Často jde i o záležitost určitých módních trendů, jejich oprávněnost se časem může zcela rozplynout. Mezi tyto hrozby můžeme zařadit.

1. *Spyware* (špionážní programy), monitorující chovatele uživatele, jeho činnost v počítači bez jeho vědomí a souhlasu. Krádeže znalostí nebo vlastnictví a jejich přenos k útočníkovi – soubory, technologická-know, průmyslová špionáž atd.
2. *Phishing* („rybaření“) – zcizování digitální identity uživatele, jeho loginů, hesel, či bankovních karet, účtů apod. za účelem jejich následného zneužití – výběr hotovosti z konta, neoprávněný přístup k funkcionalitám programů, datům atd.
3. *Spam* (zahlcování) – omezování prostoru, výkonnosti technologických zařízení, ztráta času uživatele nebo jiné negativní dopady, rozesíláním nevyžádané emailové pošty, datových souborů aj.
4. *Per-to-peer Exploits* („rovný s rovným“) – zneužívání slabin komunikace typu peer-to-peer.

Třetí oblast – Trough of Irrelevance („dno irelevantnosti či rozčarování“) - jedná se o oblast, kde hrozby nebo produkty ve světě komerčním, o kterých se již přestává mluvit, mají svůj vrchol pozornosti již za sebou. Dá se říci, že jejich hrozba již není v módě, kterou nelze stále podcenit. Zde patřily hrozby.

1. *Kybernetický útok* – po útocích na Světové obchodní centrum v New Yorku z 11. září 2001 se předpokládalo, že kybernetický terorismus se stane novou hrozbou zbraní útočníků. Nebyly ale zaznamenány žádné významné aktivity v této oblasti,

takže se o dané problematice hovoří méně. Ostražitost bezpečnostních specialistů v tomto případě neklesá a ani to není žádoucí.

2. *War Chalking* – skupina hrozeb průniků do bezdrátového WiFi počítačového spojení. Původně si hackeři ve městech označovali křídou (chalk) na chodníku místa, kde byl dobře zachytitelný WiFi signál, ke kterému měli bezproblémový přístup. V širším slova smyslu se pod tímto názvem dnes skrývá řada hackerských technik, pomocí kterých lze proniknout do nechráněné WiFi sítě. Technologie WiFi byla z hlediska možných odposlechů silně zranitelná a více jak 90% komunikace bylo otevřené. V současnosti se zabezpečení WiFi technologií věnuje velká pozornost, sítě jsou dobře zabezpečeny a War halking ustoupil z módy.

Čtvrtá oblast – Slope of Englightenment („svah znovuzrození, renesance“) – jedná se o oblast, kde hrozba nebo technologie se postupně, nenápadně stává běžnou realitou, začíná se denně vyskytovat ve velké míře. Ztrácí se módnost, nastupuje denní realita. Zde patřily hrozby.

1. *Hybridní červy* – specifické, těžko odhalitelné formy virů, které se dokáží skrývat a modifikovat sami sebe.
2. *Krádeže identity* – krádeže identity uživatele v digitálním prostředí. Pachatel pak vystupuje pod ochranou zcizené identity a minimalizuje odhalení své skutečné identity, která pak nemůže být spojována s jeho nelegální činností.
3. *Útoky DNS* (Domain Name systém) – útoky na distribuovanou datovou službu s replikací, zajišťující decentralizovaným způsobem překlad jména hostitele (počítače) na jeho IP adresu a naopak.
4. *Denial of Servise* (odmítnutí služby) – typ útoku proti počítačovému systému. Útok zabrání autorizovanému přístupu ke zdrojům nebo způsobí zpoždění časově kritických operací. Útočník zatíží server tolika požadavky, že dojde k vyčerpání všech volných zdrojů a následně k havárii služby nebo dokonce ke zhroucení celého serveru.

Pátá oblast – Plateau of Permanent Annoyance („rovina neustálých zlobičů“) jedná se o oblast, kde se hrozby reálně projevují v běžné praxi, je masově rozšířena a způsobuje závažné problémy, externě vysoké škody, svou vysokou technologickou nebo sociologickou vyspělostí. Jedná se o hrozby.

1. *Viry* – díky internetu se dnes šíří obrovskou rychlostí, za několik hodin dokáží zamořit celý svět. Způsobují obrovské ekonomické ztráty napadeným institucím i jednotlivcům.
2. *Sociální inženýrství* – je ovlivňování a přesvědčování lidí s cílem oklamat je tak, aby uvěřili, že sociotechnik je osoba s totožností, kterou předstírá a kterou si vytvořil pro potřeby manipulace. Jak jsem již uvedl v kapitole o hackingu, tak mezi největší lidi s tímto přesvědčováním patřil právě Kevin David Mitnick.

Závěr

Cílem práce bylo seznámit čtenáře s globální informační společností, vlivem bezpečnostní koncepce, bezpečnostní politikou, a riziky, které z toho vyplývají.

Nejprve jsem vyložil vlastní pojem globalizace, poukázal na charakteristiky globální společnosti, zdůraznil některé zásadní definice tohoto pojmu a také určitá zjednodušení a klišé, které se k pojmu globalizace vztahují a s ním asociují.

Dále jsem popsal působení globalizace na náš každodenní život. Zabýval jsem se vlivem globalizace na konkurenční boj, na snazší dostupnost světových trhů a s tím rostoucím množstvím příležitostí, ale i hrozeb. Zmínil jsem nutnost zavádění a důsledné dodržování bezpečnostních pravidel uvnitř organizací, a to jak po stránce právní, tak i organizační. Probral jsem jednotlivé úrovně opatření a ochran, které poslouží nejen zabezpečení ekonomických zájmů subjektů, ale i k ochraně jejich duševního vlastnictví. Neopomněl jsem důležitost rozkrývání latentní ekonomické kriminality jako samostatnou činnost ekonomického subjektu a jejich vazbu na zájmy státu. V souvislosti s tím je pak nutné správně pracovat s informacemi, shromažďovat je a třídit. V neposlední řadě pak takto získaná data správně interpretovat.

V tomto úhlu pohledu jsem se zabýval konkurenčním zpravodajstvím, které představuje komplexní zajištění ochrany a podpory ekonomických zájmů ekonomických subjektů. Můžeme ho tedy chápat jako souhrn aktivit, které zahrnují analýzu a distribuci informací využitelných pro rozhodování. Z toho je pak patrná jeho důležitost, protože správné rozhodnutí je v ekonomickém světě to nejdůležitější. Mnohdy je také důležité nejen se správně rozhodnout sám, ale podniknout kroky, aby se "správně" rozhodla i konkurence. Tím se zabývají jednotlivé složky konkurenčního zpravodajství, a to obranné, ofenzivní a vlivové neboli lobby, které jsem také popsal.

S rozvojem informačních technologií a s jejich průnikem do běžného denního života nelze opomenout vliv globalizace a její charakteristiky v informační společnosti. To zavdalo nutnost věnovat se i počítačové kriminalitě a jejímu mezinárodnímu charakteru. Ten je dán snadnou dostupností internetu a jeho návazností do všech oblastí ekonomického zájmu společnosti. Tím se dostává do popředí problematika ochrany osobních dat, otázky bezpečnosti a nalezení správného poměru mezi hranicí bezpečnosti a využitelnosti vzdáleně přístupných služeb.

Podíl využití výpočetní techniky na trestné činnosti stále roste a tak jsem shrnul kategorizaci těchto trestných činů v České republice a porovnal ji s obdobnou legislativou v zemích Evropské unie. Zabýval jsem se definicí a charakteristikou jednotlivých nových typů protiprávního jednání a jejich postižitelností podle stávající legislativy. Všechny výše uvedené typy protiprávního jednání lze současně zahrnout do seznamu prostředků, které lze využít při informační válce.

Informační válkou jsem se zabýval jak ve smyslu souhrnu veškerých opatření pro ochranu vlastních informací a procesů, tak i pro působení proti nepřátelské informační technice. Uvedl jsem jednotlivé skupiny členění informační války a jejich charakteristiku, z které vyplývá podstata a hlavní cíle takto vedeného boje.

Globalizace má ovšem dva vlivy – nepůsobí jen na rozvoj charakteristik vlastní zločinnosti, ale i podstatu zločinnosti jako takové. Umožňuje navzájem propojit oblasti dříve neslučitelné. Z toho důvodu jsem se zabýval také korupcí, která je závislá na stavu veřejné kontroly a možnostech mocenského uvážení a její prevenci. S korupcí úzce souvisí organizovaný zločin, jehož základní filozofii jsem uvedl, stejně jako terorismus a moderní kyberterorismus, který je s organizovaným zločinem mnohdy velmi úzce propojen.

Nemohl jsem opomenout rozvoj drogové kriminality, který je na globalizaci přímo závislý, neboť státy produkující drogu jsou od míst vlastní distribuce mnohdy velmi vzdáleny.

Všechna výše uvedená nebezpečí mají přímý vliv na bezpečnostní situaci a to jak globální, tak i jednotlivých kontinentů, oblastí a států. Probral jsem možné hrozby a jejich charakteristiky a vliv, jaký mohou na napadený subjekt mít. Zde nezáleží na velikosti subjektu, může jím být stát, stejně jako obchodní firma. Tyto hrozby se také mění v závislosti na čase. Uvedl jsem tedy jejich základní členění z tohoto hlediska a možné dopady na subjekt.

Jak je vidět, globalizace a zdánlivé zmenšování světa a zkracování vzdáleností není jen předností. I když si to mnohdy neuvědomujeme, mohou nám její doprovodné jevy přinést mnoho nebezpečí. Není však proto třeba globalizaci jako takovou zatracovat. Přináší s sebou celou řadu možností, které si před několika málo lety nebylo možné ani představit, umožňuje uskutečňovat řešení, spadající dříve do oblasti teorie. Nelze jí však brát na lehkou váhu a při využívání kladů, které nám dovoluje, je vždy nutné k nim přistupovat zodpovědně s vědomím možného rizika. Jen tak je možné nalézt rovnováhu, která posune celou společnost na vyšší úroveň. Na úroveň, kde budeme moci využívat další výdobytky civilizace, ale i stát před nutností čelit novým hrozbám, které s nimi souvisí.

Použitá literatura

[1] NOVÁKOVÁ, Šárka, et al. *Vize rozvoje České republiky do roku 2015* . 1. vyd. V Praze : GUTENBERG, 2001. 245 s. ISBN 80-86349-02-0.

[2] ZOUBEK, Vladimír. *Lidská práva – globalizace – bezpečnost*. 1. vyd. Plzeň : Vydavatelství a nakladatelství Aleš Čeněk, 2007. 510 s. ISBN 9788073800260.

[3] BĚLOHRADSKÝ, Václav. Vše trvalé se mění v páru, vše posvátné se znesvěcuje. Salon, literární příloha Práva, 12. Března 1998, [cit. 2009-02-28]. Dostupné z WWW: <http://www.sds.cz/docs/prectete/epubl/vbe_vtsm.htm>

[4] BRABEC, František. Efektivnost tržní ekonomiky závisí i na její soukromě-bezpečnostní ochraně. In *Bezpečnost v podmínkách organizací a institucí ČR*. Praha : Soukromá vysoká škola ekonomických studií, s.r.o., Linderova 575/1, Praha 8, 2005. s. 208. ISBN 80-86744-26-4.

[5] *PCWorld : Počet uživatelů internetu překročil miliardu* [online]. 28.1.2009 [cit. 2009-03-01]. Dostupný z WWW: <http://pcworld.cz/novinky/pocet-uzivatelu-internetu-prekrocil-miliardu-6530>

[6] *Český statistický úřad : Informační společnost v číslech* [online]. 25.4.2008 [cit. 2009-02-01]. Dostupný z WWW: <http://www.czso.cz/csu/redakce.nsf/i/domacnosti_a_jednotlivci>

[7] *Scycore: Počítačová kriminalita* [online]. 2003 [cit. 2009-02-25]. Dostupný z WWW: <http://www.scycore.com/papers/comp_crime.html >

[8] ZELENKA, J. – ČECH, P. – NAIMAN, K. *Ochrana dat : Informační bezpečnost – výkladový slovník.* Hradec Králové : Gaudeamus, 2002. 164 s. ISBN 807041197X.

[9] Úmluva Rady Evropy o počítačové kriminalitě, Budapešť, 23. listopadu 2001, Convention on Cybercrime - ETS no. 185. Dostupný z WWW: <http://conventions.coe.int/>

[10] JIROVSKÝ, Václav. *Kybernetická kriminalita : nejen o hackinngu, crackingu, virech a trojských koních bez tajemství*. 1. vyd. Praha : Grada Publishing, a.s., 2007. 288 s. ISBN 978-80-247-1561-2.

[11] MITNICK, Kevin, SIMON, William. Umění klamu. Vašta Luděk. 1. vyd. Polsko : HELION S.A., 2003. , 1. Nakladatelsví HELION S.A.. 330 s. ISBN 83-7361-210-6.

[12] *České noviny: Firmy i známí lidé musejí stále více bojovat o internetové domény* [online]. 16.03.2009 [cit. 2009-05-12]. Dostupný z WWW: <http:// www.ceskenoviny.cz/zpravy/firmy-i-znami-lide-museji-stale-vice-bojovat-o-internetove-domeny/365801 >

[13] *Lupa: Phishing po česku* [online]. 6.3.2003 [cit. 2009-02-25]. Dostupný z WWW: <http://www.lupa.cz/clanky/phishing-po-cesku/ >

[14] Ing. NASTOUPIL Josef, Informační válka: způsoby a průběh jejího vedení. [online]. [cit. 2009-02-24]. Dostupný z WWW: <http://www.army.cz/avis/vojenske_rozhledy/1999_1/info.htm>

[15] POŽÁR, Josef. Některé trendy informační války, počítačové kriminality a kyberterorismu. In *Bezpečnost v podmínkách organizací a institucí ČR*. 1. vyd. Praha : Soukromá vysoká škola ekonomických studií, s.r.o., Praha, 2005. ISBN 80-86744-26-4.

[16] JIROVSKÝ, Václav. *Kybernetická kriminalita : nejen o hackinngu, crackingu, virech a trojských koních bez tajemství.* 1. vyd. Praha : Grada Publishing, a.s., 2007. 288 s. ISBN 978-80-247-1561-2.

[17] Transparency International *ČR* [online]. 2005 [cit. 2009-04-20]. Dostupný z WWW: <http://www.transparency.cz/index.php?lan=cz&id=2680>

[18] Ministerstvo vnitra ČR*: Pilíř boje proti korupci* [online]. 20.11.2006 [cit. 2009-05-05]. Dostupný z WWW: <http://www.mvcr.cz/.../strategie-vlady-v-boji-proti-korupci-2006-2011-pdf.aspx>

[19] Marešová, A., Baloun,V., Cejp,M., Martinková, M., Zeman, P. *Kriminalita v roce 2005*. Praha : IKSP, 2006. 165 s. ISBN 80-7338-051-X.

[20] Ministerstvo vnitra ČR*: Organizovaný zločin* [online]. 14.6.2006 [cit. 2009-03-05]. Dostupný z WWW: <http://aplikace.mvcr.cz/archiv2008/bezpecnost/ozlocin.html>

[21] CHMELÍK, Jan, et al. *Zločin bez hranic*. Praha : Linde Praha, a.s., 2004. 185 s. ISBN 80-7201-480-3.

[22] NOŽINA, M. *Mezinárodní organizovaný zločin v ČR*. 1. vyd. Praha: KLP, 1997, 253 s. ISBN 8085917351.

[23] ZEMAN, J. *Terorismus: historicko-psychologická studie*. 1. vyd. Praha: Triton, 2002, 166 s. ISBN 8072543059.

[24] MAGAZÍN SECURITY: časopis pro vaši bezpečnost. Č. 1 (leden/ únor 2007) Praha: FAMILy media, spol. s.r.o. 2007. Vychází 6x ročně. ISSN 1210-8723.

[25] *Valka : Terorismus* [online]. 20.01.2001 [cit. 2009-02-12]. Dostupný z WWW: <http://www.valka.cz/newdesign/v400/show.asp?action=HTML&id=327>. ISSN 1803-4306.

[26] *Aon :Risk Management* [online]. 2009 [cit. 2009-03-15]. Dostupný z WWW: <http://www.aon.com/default.jsp >.

[27] MAGAZÍN SECURITY: časopis pro vaši bezpečnost. Č. 1 (leden/ únor 2007) Praha: FAMILy media, spol. s.r.o. 2007. Vychází 6x ročně. ISSN 1210-8723.

[28] BRZYBOHATY, M. *Současný terorismus* [online]. [cit. 2008-02-14]. Dostupný z WWW: <http://www.army.cz/avis/vojenske_rozhledy/2002_2/46.htm>

[29] JÍROVSKÝ, V. *Kyberterorismus. ICTfórum/PERSONALIS 2006.[předneseno27.9.2006]. Praha.*

[30] POŽÁR, Josef. Některé trendy informační války, počítačové kriminality a kyberterorismu. In *Bezpečnost v podmínkách organizací a institucí ČR*. 1. vyd. Praha : Soukromá vysoká škola ekonomických studií, s.r.o., Praha, 2005. ISBN 80-86744-26-4.

[31] Ministerstvo vnitra ČR *: Drogová kriminalita včera, dnes a zítra* [online]. 2008 [cit. 2009-04-13]. Dostupný z WWW: <http://aplikace.mvcr.cz/archiv2008/casopisy/kriminalistika/2001/01_04/drogy.html>

[32] KALUŽA, František, GAPAL, Peter, KUBERA, Petr. Soud rozhodl - šalvěj může i zabíjet. *Buletin*. 2009, roč. XV, č. 2.

[33] JIROVSKÝ, Václav. *Kybernetická kriminalita : nejen o hackinngu, crackingu, virech a trojských koních bez tajemství.* 1. vyd. Praha : Grada Publishing, a.s., 2007. 288 s. ISBN 978-80-247-1561-2.

[34] POŽÁR, Josef. Některé trendy informační války, počítačové kriminality a kyberterorismu. In *Pohled na bezpečnostní hrozby v informatice a telekomunikacích na přelomu roku 2004-2005*. 1. vyd. Praha : Soukromá vysoká škola ekonomických studií, s.r.o., Praha, 2005. ISBN 80-86744-26-4.

Seznam obrázků

Seznam tabulek

Příloha

Statistika drogové trestné činnosti v České republice za rok 2008

ČESKÁ REPUBLIKA - 2008

kraj	realizace	pachatelé	NP
hl. m. Praha	193	226	3
Středočeský	149	181	15
Jihočeský	160	189	1
Západočeský	170	211	5
Severočeský	354	430	6
Východočeský	121	141	3
Jihomoravský	299	375	0
Severomoravský	279	369	1
NPC [1]	36	105	0
OOZOK [2]	6	10	0
Celní správa [3]	121	89	39
CELKEM	**1888**	**2326**	**73**

z toho ve spolupráci PČR a CS	21	24

pohlaví	počet
muži	1993
ženy	333

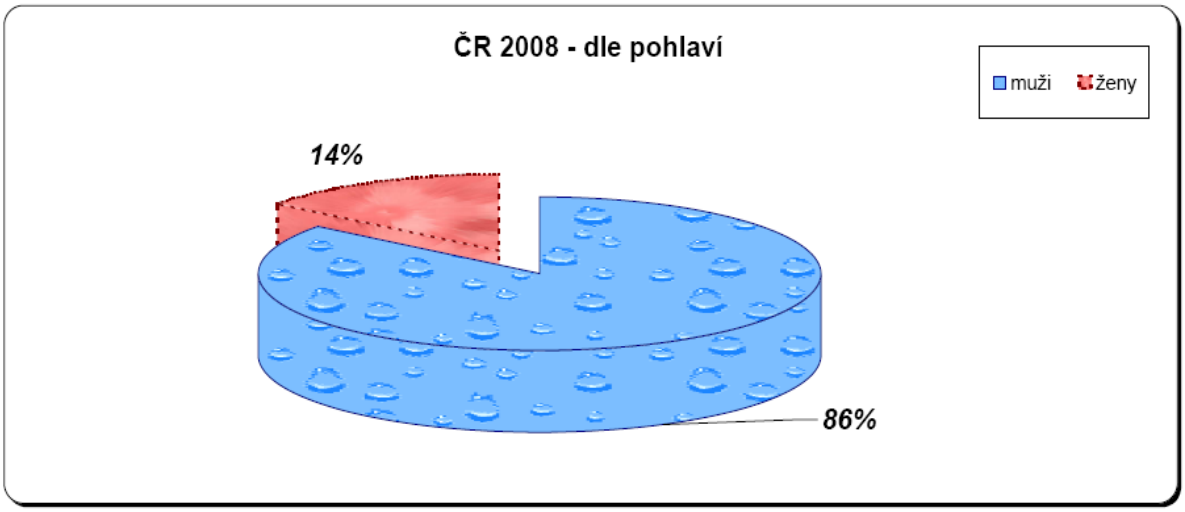
dospělí	2104
mladiství	162
nezletilí	60

národnost	počet
albánská	2
alžírská	1
americká	1
argentinská	1
běloruská	1
britská	2
bulharská	6
česká	2127
ghanská	1
chorvatská	1
irská	1
jugoslávská	3
kamerunská	1
makedonská	6
německá	1
nigerijská	8
nizozemská	1
polská	4
rakouská	1
rumunská	2
ruská	4
slovenská	21
srbská	4
turecká	1
ukrajinská	6
vietnamská	119

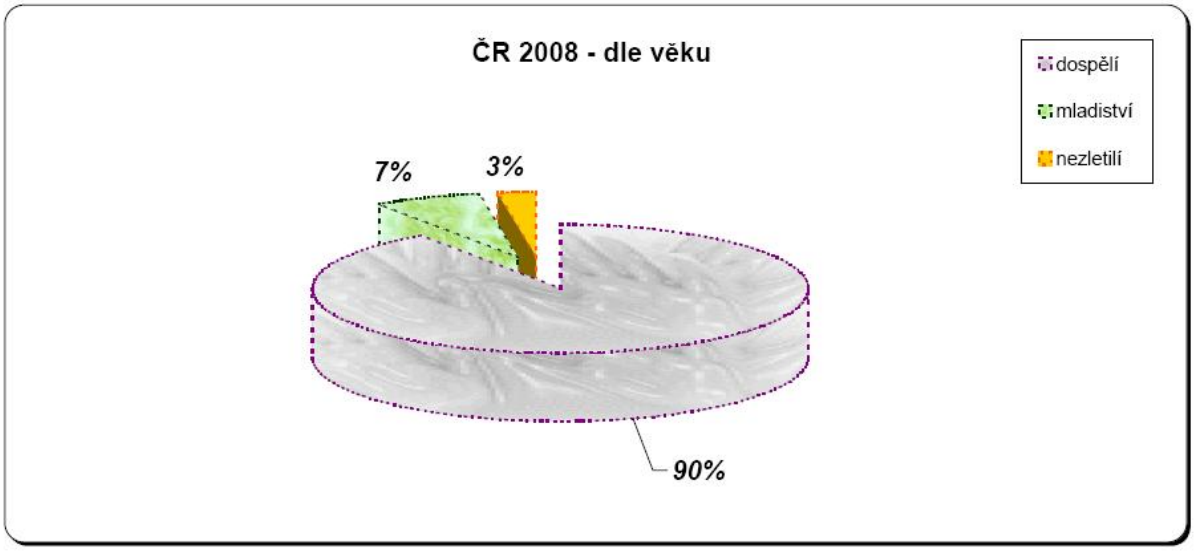
česká	2127
ostatní	199

[1] NPC SKPV se podílela na dalších realizacích v rámci celé ČR. Z důvodu vyloučení duplicity jsou tyto údaje započítány u příslušných okresů, s nimiž realizace proběhla.
[2] pouze samostatné realizace po linii TOXI, ostatní realizace, které proběhly ve spolupráci, jsou z důvodu vyloučení duplicity započítány u příslušných okresů, s nimiž realizace proběhla.
[3] pouze samostatné realizace, na kterých se nepodílela PČR

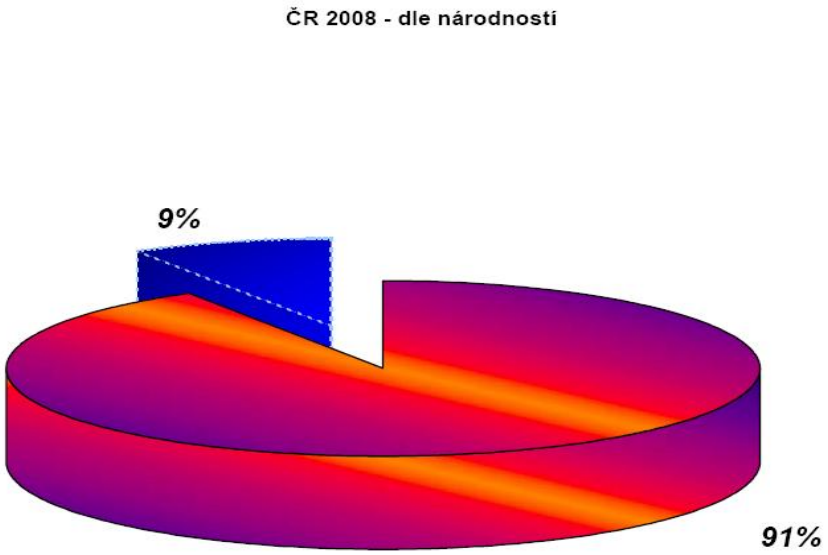
Česká republika celkem



Poměr zadržených muži/ženy



Rozdělení zadržených dle věku



Rozdělení zadržených dle národnosti

05 Východočeský kraj

okres	realizace	pachatelé	NP
Havlíčkův Brod	5	6	0
Hradec Králové	5	7	0
Chrudim	5	6	0
Jičín	11	10	1
Náchod	11	13	0
Pardubice	18	21	2
Rychnov nad Kněžnou	8	11	0
Semily	14	15	0
Svitavy	21	25	0
Trutnov	15	15	0
Ústí nad Orlicí	5	8	0
Správa Východočeského kraje	3	4	0
CELKEM	**121**	**141**	**3**

z toho ve spolupráci PČR a CS	***2***	***2***

muži	**126**
ženy	**15**

dospělí	**125**
mladiství	**9**
nezletilí	**7**

národnost	
česká	**138**
polská	**2**
slovenská	**1**

Východočeský kraj – dle původního rozdělení krajů

Zdroj: Výroční zpráva Národní protidrogové centrály 2008