PRAGUE MODEL UNITED NATIONS
PRAŽSKÝ MODEL SPOJENÝCH NÁRODŮ

Background report

Hospodářská a sociální rada (ECOSOC)

Kybernalita

KYBERNALITA

Úvod do problému

Bouřlivý rozvoj informačních a komunikačních technologií má bohužel i svou negativní stránku. Čím více se konkrétní technologie stávají nezbytnou součástí každodenního života společnosti i jedince, tím více se zvyšuje frekvence a dopady jejich zneužití. Tempo technologického pokroku je nezadržitelné (Mooreův zákon[1]) stejně jako vynalézavost nového druhu kriminálníků s ním spojených. Společnost je závislá na počítačových systémech téměř ve všech aspektech života, od průmyslu, dopravy, zdravotnictví až k národní bezpečnosti, a i malá závada (úmyslná či neúmyslná), může zapříčinit nedozírné ekonomické dopady[2] či dokonce ohrozit lidský život.

Podle „**Manuálu OSN pro prevenci a kontrolu počítačového zločinu**“[3] jsou předními orgány zabývající se touto problematikou především **OECD**[4], **Rada Evropy**[5] a právě **OSN**. Spojené národy v rámci v pořadí již **Osmého Kongresu OSN o prevenci kriminality a zacházení s pachateli**[6] v roce 1990 doporučily **Výboru pro prevenci kriminality a kontrolu nemocí**[7] při ECOSOC, aby se této nastupující hrozbě věnovala.

Vymezení pojmů

John Barlow, zakladatel Electronic Frontier Foundation, považuje za **kyberprostor** všechny existující počítačové sítě a vlastně veškeré telekomunikační sítě.

Kybernetiku lze podle Norberta Wiesnera, jejího zakladatele, možno chápat jako „vědu o řízení a komunikaci v živých organismech a strojích“[8].

Definovat konkrétněji pojem **kybernetické kriminality** (tzv. kybernality) není snadné. Ztěžuje ho velké množství možných přístupů a chápání. Nejobecněji ji můžeme rozumět jako kriminalitě, namířené přímo proti počítačům, jejich hardwaru, softwaru, datům apod., nebo v které vystupuje počítač či počítačová síť pouze jako nástroj pro páchání trestného činu[9].

Kyberterorismem rozumíme aplikaci a využívání informačních a komunikačních technologií pro teroristické cíle různých skupin[10].

---

[1] Mooreův zákon (1965, Gordon Moore – Intel) stanoví, že každých 18 měsíců dojde k zdvojnásobení výkonu mikroprocesoru za stejnou cenu nebo ekvivalentně pokles ceny na polovinu při nezměněném výkonu. (PAUKERTOVÁ, Veronika. Elektronická informační kriminalita. Ikaros. 2006, 10, 8 http://www.ikaros.cz/elektronicka-informacni-kriminalita#p1 In: www.zive.cz)

[2] Podle amerických výzkumů dosahuje průměrná výše škody každého kybernetického trestného činu přibližně 450 000 USD a roční ztráty všech amerických společností se pohybují kolem 5 miliard USD. (MUSIL, Stanislav Počítačová kriminalita, s. 204-205 ;<http://www.ok.cz/iksp/docs/256.pdf>.)

[3] International review of criminal policy - United Nations Manual on the prevention and control of computer-related crime. 1989. http://www.uncjin.org/Documents/EighthCongress.html.

[4] Organization for Economic Co-operation and Development; http://www.oecd.org/home/0,2987,en_2649_201185_1_1_1_1_1,00.html

[5] Council of Europe; http://www.coe.int/

[6] Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders; http://www.uncjin.org/Documents/EighthCongress.html

[7] The Commission on Crime Prevention and Criminal Justice; http://www.unodc.org/unodc/en/commissions/CCPCJ/

[8] JIROVSKÝ, Václav. Kybernetická kriminalita.2007. Chápání kyberprostoru, s. 17

[9] JIROVSKÝ, Václav. Kybernetická kriminalita.2007. Pět problémů kybernality, s. 19

[10] POŽÁR, Josef. Některé trendy informační války, počítačové kriminality a kyberterorismu, s .1; http://www.svses.cz/skola/akce/konf/bezp05/texty/pozar.pdf

Kybernetická válka pak představuje aktivity vedené nebo koordinované státem s cílem získat informační převahu nebo vyřadit technologickou infrastrukturu protivníka. Její součástí je tzv. **informační válka** neboli „válka o informace“ [11].

High-Tech hrozby

Do High-Tech hrozeb řadíme hrozby spojené s moderními technologiemi. Pro klasifikaci kybernetických zločinů existuje mnoho různých přístupů. Můžeme je členit podle dopadu konkrétního skutku, z hlediska skutkových podstat, podle akčního plánu eEurope+, podle společenského významu chráněných zájmů, apod. My se budeme držet řazení podle mezinárodní dohody o kyberzločinu vypracované Radou Evropy[12], která třídí zločiny takto:

- Zločiny proti důvěrnosti, integritě a dosažitelnosti počítačových dat a systémů, jež se dále dělí na:
  - nezákonný přístup
  - nezákonné odposlouchávání
  - narušování dat
  - narušování systémů
  - zneužití prostředků
- Zločiny se vztahem k počítači, které jsou děleny na:
  - počítačové padělání
  - počítačový podvod
- Zločiny se vztahem k obsahu počítače, což je především dětská pornografie.
- Zločiny se vztahem k autorským nebo obdobným právům.

Mezi nejaktuálnější a nejdebatovanější příklady hrozeb a protiprávních jednání mohu jmenovat:

- Warez
- Sociální inženýrství (+ „phishing“)
- Hacking x Cracking
- Dětská pornografie

Warez a digitální pirátství

Pod pojmem **warez** rozumíme výrobu nebo rozšiřování pirátského software[13]. **Pirátství** zahrnuje jakékoliv neoprávněné užití autorského díla, které přísluší pouze nositelům práv k těmto dílům[14]. Mezi tyto trestné činy patří především výroba, distribuce a prodej produktů porušujících ochranné známky, autorská a patentová práva a digitální pirátství (veškeré nelegální stahování hudby, filmu či softwaru). Jejich ekonomické dopady jsou nedozírné.

[11] JIROVSKÝ, Václav. Kybernetická kriminalita.2007. Kybernetické války a infoware, s. 152

[12] Analýza současného stavu a trendů vývoje trestné činnosti na úseku informačních technologií a internetu včetně návrhu řešení, Ministerstvo ČR, s. 3-4; http://aplikace.mvcr.cz/archiv2008/dokument/2006/informacni.pdf

[13] JIROVSKÝ, Václav. Kybernetická kriminalita.2007. Hackeři a crackeři, s. 68

[14] Česká protipirátská unie. Co je to pirátství a jaké tresty za něj hrozí; http://www.cpufilm.cz/piracy.html

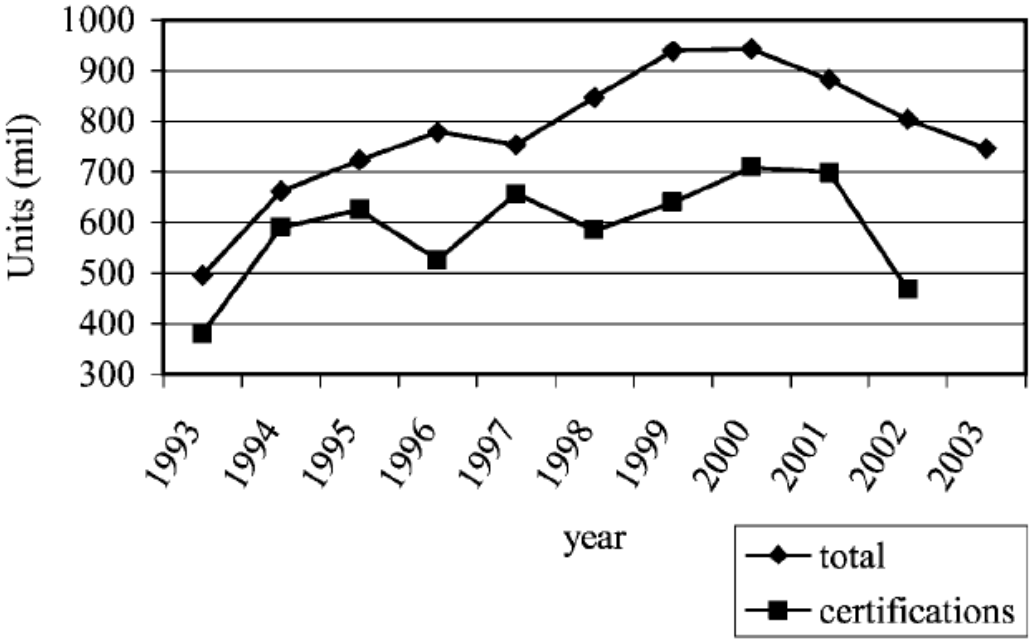


FIGURE 1.—Albums sold, 1993–2003

Graf zobrazuje poměr legálního počtu stažení hudby (certifications) s celkovým (total).[15]

[15] ROB, WALDFOGEL. Piracy on the high C´S; http://bpp.wharton.upenn.edu/waldfogj/jle_piracy.pdf

Studie OECD k padělatelství a pirátství, která byla spuštěna v roce 2005 uvádí, že od roku 2000 obchod s padělaným zboží neustále rostl a v roce 2007 dosáhl až k hodnotě 250 miliard USD[16]. Co se týká ztrát průmyslu způsobených nelegálním stahováním, v roce 2004 byly škody filmové sekce vyčísleny na 3,5 miliard dolarů a v roce následujícím už to bylo 5,4 miliard USD[17].

Rozšíření pirátského softwaru[18]

Země s nejnižší mírou:
USA (20 %), Japonsko a Lucembursko (21 %), Nový Zéland (22 %), Rakousko (24 %), Belgie, Dánsko, Švédsko a Švýcarsko (25 %)

Průměr:
Spojené arab. emiráty (36 %), Česko (38 %), Tchaj-wan (39 %), Francie (41 %), Slovensko (43 %), Itálie (48 %), Estonsko a Kypr (50 %)

Ti nejhorší:
Gruzie (95 %), Arménie (92 %), Ázerbájdžán a Moldávie (90 %), Pákistán, Venezuela (86 %), Vietnam a Irák (85%), Ukrajina (84 %), Černá Hora (83 %), Čína (80 %)
(Zdroj: BSA)

V zemích po celém světě jako je Indie, Austrálie, Čína nebo Mexiko probíhají kampaně na zvýšení povědomí veřejnosti o tomto jevu[19].
Uveřejňování nelegálních warez kopií dělá starost především organizacím na ochranu autorských práv. Mezi nejvýznamnější celosvětové organizace této oblasti kybernality můžeme jmenovat **Business Software Aliance** (BSA), která se snaží o prosazení legálního užívání software nebo **World Intellectual Property Organization** (WIPO), zabývající se především ochranou duševního vlastnictví[20]. Problematice se věnuje i Interpol a UNESCO[21].
Názory společnosti jsou ale značně benevolentnější a v mnoha zemích vznikají i politické strany s podporou pirátství na internetu[22]. Potlačení těchto trestných činů za účelem zachování specifických částí průmyslu se jeví jako jedna z nejpodstatnějších výzev nové počítačové doby.

Sociální inženýrství, phishing

Dnes velmi populárním „sociálním inženýrstvím" jsou označovány „psychologické triky hrané na oprávněné uživatele systému za účelem získání přístupu do tohoto systému"[23]. Jedná se o webové stránky, na které odkazuje spam nebo například o tvz. **phishing**. U phishingu jde o typické e-

[16] Projekt OECD k padělatelství a pirátství. Ministerstvo průmyslu a obchodu, 2010; http://www.mpo.cz/dokument45250.html
[17] JIROVSKÝ, Václav. Kybernetická kriminalita.2007. Hackeři a crackeři, s. 74
[18] KORBEL, PERKNEROVÁ. Pirátství na internetu. Deník.cz, 2009; http://www.denik.cz/z_domova/internet_pirati20090513.html
[19] OECD. Piracy of Digital Content, 2009, s. 74-75; http://books.google.com/books?id=3tdCO_kv2iAC&printsec=frontcover&hl=cs&cd=1&source=gbs_ViewAPI#v=onepage&q&f=false
[20] MUSIL, Stanislav. Počítačová kriminalita, s.197-198 ;<http://www.ok.cz/iksp/docs/256.pdf>
[21] OECD. Piracy of Digital Content, 2009, s. 78; http://books.google.com/books?id=3tdCO_kv2iAC&printsec=frontcover&hl=cs&cd=1&source=gbs_ViewAPI#v=onepage&q&f=false
[22] Česká pirátská strana; http://www.ceskapiratskastrana.cz/, Pirátská strana (Švédsko); http://cs.wikipedia.org/wiki/Pirátská_strana_(Švédsko)
[23] JIROVSKÝ, Václav. Kybernetická kriminalita.2007. Sociální inženýrství, s. 196

mailové zprávy, kdy se pachatel vydává za bankovní instituci (za použití zfalšované adresy odesílatele) a snaží se
„vymámit“ z uživatele důvěrné informace (číslo kreditní karty, čísla účtů, přístupové kódy …). Následující obrázky jsou ukázkami takového phishingu v praxi:

První větší útok formou sociálního inženýrství v ČR. Zneužitím značky Citibank vymáhali pachatelé citlivé údaje klienta[24].

[25]

Hacking x Cracking

Ačkoli pohledy na věc se různí[26], „hacking“ a „cracking“ jsou dvě odlišné (i když související) aktivity. **Hackingem** míníme neautorizované pronikání do cizích počítačů, sítí nebo systému za

[24] Sociální inženýrství. Spyware.cz; http://www.viry.cz/go.php?p=spyware&t=clanek&id=48
[25] Phishing Activity Trends Report. Anti-Phishing Working Group, 2006; http://www.antiphishing.org/reports/apwg_report_May2006.pdf

účelem finančního zisku (např. prodejem dat) či cíleného poškození. Pojmem **cracker** je označován člověk, jehož prvotním cílem je prolomení softwarového zabezpečení. To bývá často spojeno s problematikou pirátství[27].
Mezi hackerské programové nástroje patří např. prolamovače hesel, trojské koně, backdoors, nástroje DoS a mnoho dalších[28].

Problémy kybernality

Prevence, vyšetřování a trestání pachatelů je velmi obtížné. Kyberprostor nabízí kriminálníkům anonymitu a rychlou ztrátu stop, zatímco první překážka vyšetřujících je už samotná obtížná definice kybernetických kriminálních činů. Nejpalčivější problémy, spojené s kybernalitou, můžeme rozdělit do tří základních skupin:

- Legislativa
- Policie a Justice
- Společnost a chápání bezpečnosti
-

Legislativa

Jak už bylo zmíněno výše, jedním ze základních problémů kybernality je **obtížnost konkrétní definice počítačového trestného činu a jeho dokazování**. Podle statistik USA je odhaleno jen asi 5% takových činů a z nich se pouze 20% dostane do soudního procesu[29]. Právní normy nejsou schopny zcela jasně vyjmenovat a konkretizovat jednotlivé zločiny, a proto jsou soudní řízení velmi nejasná a zdlouhavá, nehledě na **nedostatečnou kvalitu navrhovaných zákonů**[30]. Co je v jedné zemi trestné, může být v druhé akceptováno nebo nebývá v legislativě zahrnuto vůbec. Například tvorba a distribuce warez[31] je v západních zemí považována za nelegální činnost, zatímco země třetího světa ji tiše tolerují nebo uznávají za zcela legitimní[32]. Při globálním rozměru kybernality, kterou neomezují vzdálenosti ani fyzické hranice států, se pro řešení škody a pátrání po pachatelích nedostává potřebných nástrojů a vyšetřování se dostává do slepé uličky.

Také **proces koordinace států** je velmi pomalý a neobejde se bez konfliktů. Případy masivních kybernetických útoků na klíčové body jednotlivých národů jako bylo například napadení Estonska před třemi lety[33], za kterým většina světa viděla angažování ruských expertů, ztěžují hladký průběh jednání. Tyto specifické útoky se nazývají „Kybernetické války“ a budu se jim podrobněji věnovat později.
Mezinárodním společenstvím také hýbe diskuze o **svobodě internetu**. Ten je často prezentován jako „nejdemokratičtější médium“, ale podle výzkumů z roku 2007 filtrovalo internetový obsah celých 40 ze 71 sledovaných států[34]. Například v zemích jako je Čína nebo Írán mají poskytovatelé internetu

---

[26] Například JIROVSKÝ ve své knize chápe hackera jako osobu se zájmem a vysokými znalostmi v programování, pohybujícího se v mezích zákona. Na druhé straně, cracker je podle něj ten, kdo zneužívá hackerských postupů ke způsobování škod v systémech za účelem finančního zisku. (JIROVSKÝ, Václav. Kybernetická kriminalita.2007. Hackeři a crackeři)

[27] ABERLE, Pavel. Budoucnost kybernetického terorismu. Masarykova univerzita, 2010, s. 106; http://is.muni.cz/th/342895/fss_m/Budoucnost.kyber.teror.Aberle.DP.pdf

[28] Pro získání podrobného popisu konkrétního jevu využijte zdroje a doporučenou literaturu na konci práce.

[29] MUSIL, Stanislav. Počítačová kriminalita, s.205 ;<http://www.ok.cz/iksp/docs/256.pdf>

[30] JIROVSKÝ, Václav. Kybernetická kriminalita.2007. Pět problémů kybernality, s. 25-26

[31] viz. 2.1

[32] PAUKERTOVÁ, Veronika. Elektronická informační kriminalita : Porušování autorských práv. Ikaros. 2006, 8, <http://www.ikaros.cz/elektronicka-informacni-kriminalita>.

[33] NAGORSKI, Andrew. Cyberwar is hell. Newsweek. 2010;<http://www.newsweek.com/2010/07/28/cyberwar-is-hell.html>.

[34] CHOVANEC, Ján. Internet je stále více cenzurovaný, tvrdí experti. Computerworld. 2009;<http://computerworld.cz/aktuality/internet-je-stale-vice-cenzurovany-tvrdi-experti-3660>.

nařízeno, na které stránky musí povinně znemožnit uživatelům přístup[35]. Díky podobným akcím a studiím vzrůstají obavy z pokusů konkrétních vlád kontrolovat svobodný projev v kyberprostoru.

Mezinárodní legislativní aktivity

Mezinárodní organizace v návaznosti na stoupající nebezpečí a frekvenci zneužívání informačních systémů začaly v tomto směru v posledních letech vyvíjet zvyšující se aktivity. V roce 1986 vytvořila **OSN** výše zmiňovaný **„Manuál OSN pro prevenci a kontrolu počítačového zločinu“**[36], který v roce 2001 prošel nezbytnou aktualizací. Země **OECD** inicializovali studii **„Computer-Related Crime: Analysis of Legal Policy“**[37], jenž vedla k tvorbě doporučení o bezpečnosti systémů pro členské státy[38]. V rámci plnění deseti bodů akčního plánu[39], dohodnutého na schůzce G8[40] v roce 1997, věnuje vysokou pozornost problému i **Evropská Unie**, která na jednom z posledních meetingů k tématu v roce 2010 zdůraznila potřebu sdílení informací a nadnárodní spolupráce[41]. Jejím klíčovým dokumentem, v uvedené oblasti je **„Akční plán pro bezpečnější internet“** z roku 1999-2004 a na něj navazující **„Bezpečnější internet plus“** pro období 2005-2008[42]. Tyto dokumenty vyvyšují především nutnost větší informovanosti veřejnosti. Za zmínku také stojí zavádění evropských platforem CERT/CSIRT, které poskytují službu a podporu v oblasti bezpečnosti počítačových sítí, a to především v oblasti řešení bezpečnostních incidentů[43].
Problematiku kybernality dále zkoumá také **NATO**[44].

Policie a justice

Kybernalita je páchána s použitím velmi vyspělých a specifických nástrojů, znalostí a postupů. Největší problém, s kterým se policie i justice potýká, je **nedostatek vysoce kvalifikovaných pracovníků** po stránce technologické i právní. Stopy v kyberprostoru mizí mnohem rychleji než u klasického trestného činu, na zajištění stop často není více času než pár minut. **Pomalost soudního procesu** poté může vést až k jejich úplné ztrátě a znemožnit dopadení pachatele.

Společnost a chápání bezpečnosti

Benevolentní vnímání kybernality společností je dáno především nehmotností produktů, anonymitou a neviditelnými následky. Je způsobeno také fenoménem tzv. zločinu **„bílých límečků“**[45], zatímco přímé převedení peněz z cizího účtu způsobuje většinou mnohem vyšší finanční ztrátu, společností

[35] Novinky.cz, 2009; http://www.novinky.cz/internet-a-pc/182443-francouzska-ustavni-rada-schvalila-zakon-o-pocitacovem-piratstvi-na-internetu.html
[36] viz. [3]
[37] JIROVSKÝ, Václav. Kybernetická kriminalita.2007. Kyberprostor a právo, s. 90
[38] OECD Guidelines for the Security of Informatik Systems, 1992; http://www.oecd.org/document/19/0,2340,en_2649_34255_1815059_119820_1_1_1,00.html
[39] Analýza současného stavu a trendů vývoje trestné činnosti na úseku informačních technologií a internetu včetně návrhu řešení, Ministerstvo ČR, s. 48; http://aplikace.mvcr.cz/archiv2008/dokument/2006/informacni.pdf
[40] Group of Eight; http://www.g8.utoronto.ca/
[41] Council conclusions concerning an Action Plan to implement the concerted strategy to combat cybercrime, 2010; http://www.enisa.europa.eu/media/news-items/council-cyber-crime
[42] Mezinárodní spolupráce v boji proti informační kriminalitě, Ministerstvo vnitra ČR, s. 4; http://www.mvcr.cz/docDetail.aspx?docid=21232226&doctype=ART&
[43] KROPÁČOVÁ, Andrea. Bezpečnostní týmy CERT/CSIRT, 2009; http://www.nic.cz/files/nic/doc/prezentace/IT09_Kropacova.pdf
[44] North Atlantic Treaty Organization; http://www.nato.int/cps/en/natolive/index.htm
[45] Podle amerického kriminologa Edwina H. Sutherlanda rozumíme pojmem „zločinci bílého límečku“ kriminálníky, kteří jsou relativně více chráněni před trestním stíháním díky svému vyššímu společenskému postavení. (DIVIŠ, Zdeněk. Trestná činnost tzv. bílých límečků, 2005-2006,s. 5. Bakalářská práce. Masarykova univerzita;<http://is.muni.cz/th/108605/pravf_b/Trestna_cinnost_tzv._bilych_limecku.pdf>.)

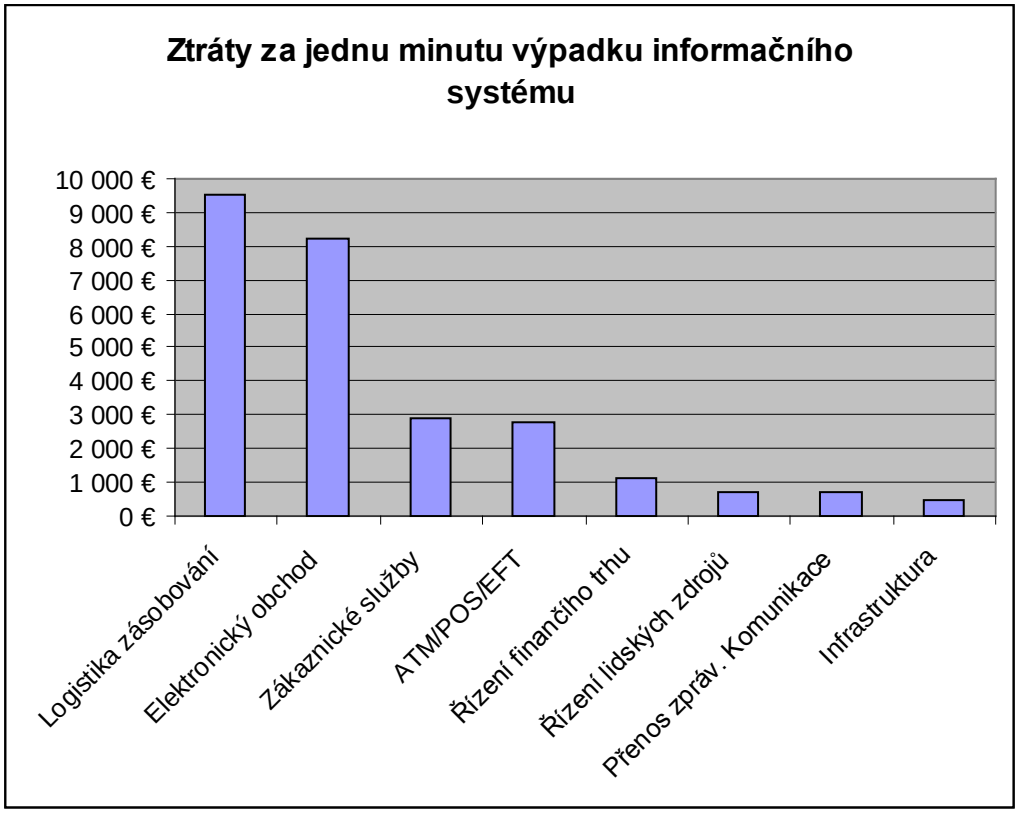
je posouzeno mnohem volněji než násilné ozbrojené vloupání do banky. **Softwarové pirátství** pak lidstvo neodsuzuje téměř vůbec, velká část obyvatel i firem dokonce nelegální software vlastní a obhajují si krádež faktickou nehmotností ukradené věci.
K všeobecně laxnímu přístupu také přispívá značná **neúspěšnost vyšetřování a trestání.**

Aby se dosavadní smýšlení lidí změnilo, je potřeba zvýšit **gramotnost a informovanost** běžného uživatele v této oblasti a dosáhnout co nejvyšší možné **bezpečnosti systémů.**

Kyberterorismus

Jako nejpoužívanější definici jevu známého jako kyberterorismus si můžeme zvolit tuto: „ Kyberterorismus spojuje terorismus a kyberprostor. Chápeme ho jako úmyslný útok proti počítačovým sítím a kritické infrastruktuře za účelem zastrašit nebo donutit vládu a obyvatele k plnění požadavků a cílů teroristické skupiny.“[46]

Ekonomické dopady této odnože terorismu se mohou vyšplhat až k obrovským hodnotám. Například vyčíslení škod po viru **Code Red**, který ohrožoval americké servery, se podle studie nevládní výzkumné organizace „Computer Economics“ v roce 2001 vyšplhalo až k hodnotě 2,6 miliardy dolarů[47].
Na následujícím obrázku můžeme vidět odhadované ztráty způsobené jednou minutou výpadku informačního systému, děleny podle typických segmentů trhu. Právě vyřazení serverů protivníka často bývá cílem kybernetických útočníku.



[48]

Na druhé straně se z řad veřejnosti ozývají i názory, že odhady finančních důsledků jsou, například ve srovnání s běžnými výpadky proudu, až příliš nadsazeny a medializovány[49].

[46] JIROVSKÝ, Václav. Kybernetická kriminalita.2007. Kyberterorismus, s. 130
[47] James. F. DUNNIGAN. Bojiště zítřka. 2002, s. 106;
http://books.google.cz/books?id=6fHVIqK5lo8C&pg=PA271&lpg=PA271&dq=kybernetická+kriminalita+mezinárodně&source=bl&ots=yk48K4v_Wo&sig=wy8sWn5UeBMKbkUVowIrvvpQdOE&hl=cs&ei=qkhhTOesK8StOJz89J8K&sa=X&oi=book_result&ct=result&resnum=10&ved=0CC4Q6AEwCThQ#v=onepage&q&f=false
[48] JIROVSKÝ, Václav. Kybernetická kriminalita.2007. Kyberterorismus, s. 131

Do kyberterorismu můžeme zařadit i specifickou ideologickou odnož, tvz. **mediální neboli psychologický terorismus**, kdy pachatelé využívají hromadných sdělovacích prostředků za účelem ovlivnění názorů populace či konkrétní cílové skupiny[50]. Typickým příkladem takového typu terorismu je případ z konce roku 2001, kdy se objevila alarmující zpráva o tom, že FBI implantuje do počítačů sledovací program s názvem **„Magic Lantern"** (tzv. Kouzelnou lampu) a že nutí antivirové společnosti, aby jej nezařazovaly do svých detekčních zařízení. Zvedla se obrovská vlna protestů ze strany ochránců autorských práv a rozhořčených obyvatel. Až později vyplynulo, že tato zpráva byla pouze smyšlenou fámou, která se nečekaně nafoukla, a že FBI takový software nikdy nenavrhla[51].

Jiný incident se udál 4. července roku 2009, kdy se cílem rozsáhlého útoku staly americké instituce nebo server newyorské burzy a útok proti jihokorejským vládním složkám, k němuž došlo o několik dní později[52].

Jedním z nejdiskutovanějších napadení kritické infrastruktury státu byl výše zmiňovaný útok ruských teroristů na důležité webové stránky Estonska[53]. V těchto případech, kdy panuje všeobecné podezření, že za teroristickou aktivitou stojí vláda nepřátelské země, se kyberterorismus často proplétá s tzv. „kybernetickou válkou", které se věnuje následující kapitola.

Věk kybernetických válek

Jak již bylo řečeno v úvodu, pojem **kybernetická válka** představuje aktivity vedené nebo koordinované státem s cílem získat informační převahu nebo vyřadit technologickou infrastrukturu protivníka. Její specifickou odnoží, informační **válkou**, pak rozumíme válku vedenou v oblasti informací, takovou, která informace využívá jako prostředek boje[54].

Zabývání se bezpečnostními otázkami je v kompetenci specifických orgánů OSN k tomu určených; jako je Rada bezpečnosti či Valné shromáždění. V rámci jednání v ECOSOC proto téma kybernetických válek nespadá pod diskuzní agendu a dostačuje mít pouze obecnou představu o dané problematice.

Informační boj je velmi oblíben, jelikož je to prakticky jediná možnost postavit se nepříteli, který má drtivou převahu vojenské i ekonomické síly. Je relativně nenáročný z hlediska materiálního i personálního. Paradoxně, nečekaný a překvapivý útok může podkopat jinak silnou obranyschopnost protivníka a zapříčinit škody mnohem větší než byly náklady na jeho uskutečnění.
Je známo, že některé státy už aktivně vyvíjí kybernetické prostředky pro špionáž, odposlech a samotný informační boj. Spojené státy americké a spojenci považují mezi potencionálními oblastmi nebezpečí především nepřátelské státy „osy zla"[55] (zejména pak Severní Koreu nebo Kubu), Čínu a Rusko, o kterých se všeobecně ví, že se technologiemi tohoto typu zajímají[56].

---

[49] James. A. LEWIS. Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats. Center for Strategic and International Studies, 2002, s. 9; http://www.steptoe.com/publications/231a.pdf

[50] JIROVSKY, Václav. Kyberterorizmus, bezpečnostní hrozba 21.storočia. 2008; http://www.eaq.sk/magazine/EAQ12_Tema_cisla_Jirovsky.pdf

[51] PŘIBIL, Tomáš. Kyberterorismus II, Vírusy.sk, 2003; http://www.virusy.sk/clanok.Itc?ID=403

[52] Přichází věk kybernetické války?. Magazín Emag, 2009; http://www.emag.cz/prichazi-vek-kyberneticke-valky/

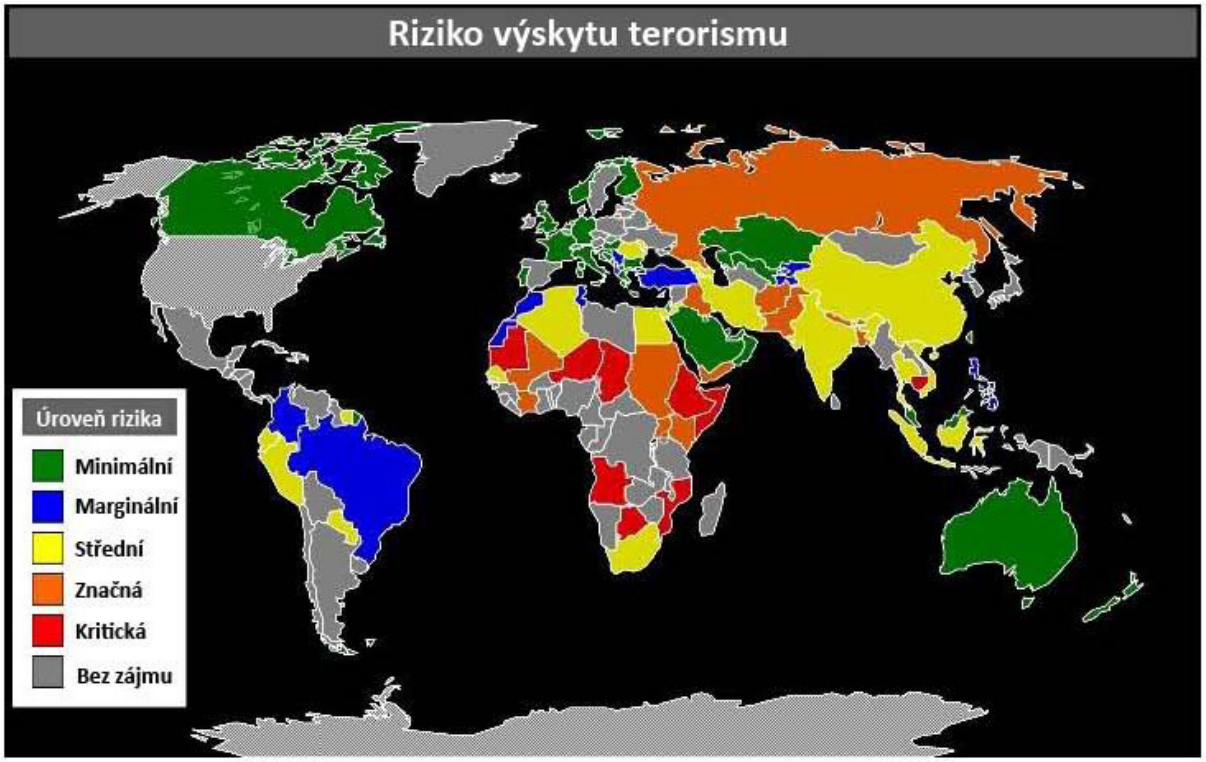
[53] viz. [28]

[54] viz. [11]

[55] „Osa zla" je původním termínem bývalého amerického prezidenta George Bushe pro státy, u kterých panuje podezření z napomáhání terorismu a vyrábění zbraní hromadného ničení. Mezi ně se řadí především Írán, Irák, Severní Korea, Kuba, Libye a Sýrie. Americká administrativa tento seznam vždy upravuje podle aktuálního mezinárodního dění. (http://cs.wikipedia.org/wiki/Osa_zla)

[56] JIROVSKÝ, Václav. Kybernetická kriminalita.2007. Kyberterorismus, s. 133

Následující obrázek znázorňuje některé oblasti s nejvyšším rizikem výskytu terorismu a nepřátelských akcí v kyberprostoru i mimo něj:



Zdroj: Institute for Intelligence Studies 2010. [57]

Závěr

Žijeme ve světě, kde rozhoduje síla informací. A právě informace bývají často zneužívány. Kybernetická kriminalita se tím stává jednou z nejpalčivějších a nejaktuálnějších otázek současnosti. K jejímu řešení je nezbytná nadnárodní spolupráce a koordinace trestního práva i boje proti ní. Neomezují ji vzdálenosti ani fyzické hranice států, a proto se její potlačení neobejde bez mezinárodní shody.

Zdroje a doporučené prameny informací:

JIROVSKÝ, Václav. Kybernetická kriminalita. Praha : Grada Publishing, a.s., 2007. 284 s.

DUNNIGAN, James F. Bojiště zítřka. Praha : Baronet, 2004. 359 s.

OECD. Piracy of digital content. OECD PUBLISHING. France, 2009. 133 s.

United Nations Manual on the prevention and control of computer-related crime; http://www.uncjin.org/Documents/EighthCongress.html

Ministerstvo vnitra České republiky. 2009. Výsledky projektů: Problematika kybernetických hrozeb. http://www.mvcr.cz/docDetail.aspx?docid=21232226&doctype=ART&; http://www.mvcr.cz/clanek/o-nas-bezpecnost-a-prevence-dokumenty-bezpecnost-a-prevence-dokumenty-kyberneticke-hrozby.aspx.

STEUER Petr. Počítačová kriminalita (bakalářská práce). Masarykova Univerzita, 2008/2009

[57] ABERLE, Pavel. Budoucnost kybernetického zločinu. Masarykova univerzita, 2010; http://is.muni.cz/th/342895/fss_m/Budoucnost.kyber.teror.Aberle.DP.pdf, In: Institute for Inteligence Studies 2010

PAUKERTOVÁ, Veronika. Elektronická informační kriminalita. Ikaros . 2006, 8, [cit. 2010-08-30]. Dostupný z WWW: <http://www.ikaros.cz/elektronicka-informacni-kriminalita>.

NAGORSKI, Andrew. Cyberwar is Hell. Newsweek, 2010. Dostupný z WWW: < http://www.newsweek.com/2010/07/28/cyberwar-is-hell.html>.

POŽÁR, Josef. Některé trendy informační války, počítačové kriminality a kyberterorismu. Policejní akademie ČR v Praze [online]. 2006, 8, [cit. 2010-08-30]. Dostupný z WWW: <http://www.svses.cz/skola/akce/konf/bezp05/texty/pozar.pdf>.

MUSIL, Stanislav. Počítačová kriminalita. In Institut pro kriminologii a sociální prevenci [online]. Praha : 2000 [cit. 2010-08-30]. Dostupné z WWW: <http://www.ok.cz/iksp/docs/256.pdf>.

ABERLE, Pavel. Budoucnost kybernetického terorismu [online]. Brno : 2010. 90 s. Diplomová práce. Masarykova univerzita. Dostupné z WWW: <http://is.muni.cz/th/342895/fss_m/Budoucnost.kyber.teror.Aberle.DP.pdf> .

James A. LEWIS. Assesing the risk of cyber terrorism, cyber war and other cyber threats. CSIS, 2002. Dostupné z WWW: <http://www.steptoe.com/publications/231a.pdf> .

OECD, 2008 [cit. 2010-08-30]. Malicious Software (Malware): A Security Threath to the Internet Economy. Dostupné z WWW: <http://www.oecd.org/dataoecd/53/34/40724457.pdf>.

United States Department of Justice : Computer Crime and Intellectual Property Section [cit. 2010-08-30]. Dostupné z WWW: <http://www.cybercrime.gov/index.html>.

Cybercrime. Euractiv [online]. 2002, [cit. 2010-08-30]. Dostupný z WWW: <http://www.euractiv.com/en/infosociety/cybercrime/article-117465>.

OECD Guidlines for the Security of Informatik Systems. OECD, 1992. Dostupný z WWW:<http://www.oecd.org/document/19/0,2340,en_2649_34255_1815059_119820_1_1_1,00.html>.
Council conclusions concerning an Action Plan to implement the concerted strategy to combat cybercrime. Council of European Union, 2010. Dostupný z WWW: < http://www.enisa.europa.eu/media/news-items/council-cyber-crime>.

Sociální inženýrství aneb nenechte se oblbnout. Spyware.cz. Dostupný z WWW: < http://www.viry.cz/go.php?p=spyware&t=clanek&id=48>.

Viry.cz. Dostupný z WWW: < http://www.viry.cz/go.php>

Projekt OECD k padělatelství a pirátství. Ministerstvo průmyslu a obchodu ČR. Dostupný z WWW: < http://www.mpo.cz/dokument45250.html>

What you should know about internet piracy. Guide to computer training. Dostupný z WWW: <http://www.guidetocomputertraining.com/tips-and-tools/internet-piracy>.

Software piracy – A challenge to E-world. SANS Institut. Dostupný z WWW: <http://www.sans.org/reading_room/whitepapers/basics/software-piracy-challenge-e-world_999>.
Česká protipirátská unie. Dostupný z WWW: < http://www.cpufilm.cz/>.

CHOVANEC, NOSKA. Internet je stále více cenzurovaný, tvrdí experti. Computerworld, 2009. Dostupný z WWW:< http://computerworld.cz/aktuality/internet-je-stale-vice-cenzurovany-tvrdi-experti-3660>.

Top partneři

GENERÁLNÍ PARTNER MODELU OSN

NADACE EDUCA

HLAVNÍ PARTNER MODELU OSN

G2 OD KOMERČNÍ BANKY

MODEL NATO IS CO-SPONSORED BY THE NORTH ATLANTIC TREATY ORGANIZATION

NATO OTAN

HLAVNÍ PARTNER MODELU EU

Zastoupení Evropské komise v České republice

UNIVERZITNÍ PARTNER

VYSOKÁ ŠKOLA EKONOMICKÁ V PRAZE VŠE

PARTNER ZAHÁJENÍ

interhotel AMBASSADOR ZLATÁ HUSA

PARTNER JEDNÁNÍ

KONGRESOVÉ CENTRUM PRAHA

PARTNERSKÉ MĚSTO

PRAHA PRAGUE PRAGA PRAG

Dodavatelé služeb

VYŠEHRAD

KONFES KONGRESOVÁ TECHNIKA www.konfes.cz

KONICA MINOLTA

zátiší group

kofola original

inspiro solutions

Hasičská vzájemná pojišťovna, a.s.

newton media

MOTOROLA

PEKAŘSTVÍ

3M

SUBWAY

Mediální partneři

RESPEKT

HOSPODÁŘSKÉ NOVINY

PARTNER CHRONICLE

ČTK

ÚSTAV MEZINÁRODNÍCH VZTAHŮ PRAHA iir

natoaktual.cz

METROPOLITNÍ UNIVERZITA PRAHA

Asociace pro mezinárodní otázky
Association for International Affairs

Zpracoval: Veronika Kadlecová
Redakční úprava: Sára Foitová, Kateřina Humplíková, Iveta Moravcová
Grafická úprava a tech. spolupráce: Šimon Ehrlich
Vydala Asociace pro mezinárodní otázky pro potřeby XVI. ročníku Modelu OSN.

Model OSN
Asociace pro mezinárodní otázky, Žitná 27, 110 00 Praha 1
Tel./fax: +420 224 813 460, e-mail: model.osn@amo.cz, IČ: 65 99 95 33
»www.amo.cz« »www.studentsummit.cz«