KYBERTERORISMUS: TERORISMUS INFORMAČNÍ SPOLEČNOSTI

Por. Ing. Michal JANOUŠEK

Anotace:

Terorismus ve světě představuje břečťan, který se v posledních letech „rozrostl" do nepředstavitelného množství odrůd a tvarů. Dnes již pojem terorismu neoznačuje pouze politicky motivovaný atentát či útok, ale odráží se v odporu vůči různým faktorům v mnoha různých úrovních lidského konání. A jelikož mírou moderní společnosti je schopnost využívání informací, objevuje se zde i velice specifický a nebezpečný druh skryté hrozby – kyberterorismus.

Již je to více jak 10 let, co se do České republiky dostal internet. Je to více jak 10 let, co mám v mozku začal vznikat nový systém přístupu a práce s informacemi, jehož důsledkem je existence tzv. „**informační společnosti**". Pojmem informační společnost se dnes v obecné rovině „*rozumí společnost, kde kvalita života i perspektiva sociálních změn a ekonomického rozvoje závisí na informacích a schopnosti jejich využití, tj. informace se stává klíčovým faktorem takového společenosti.*"[1]

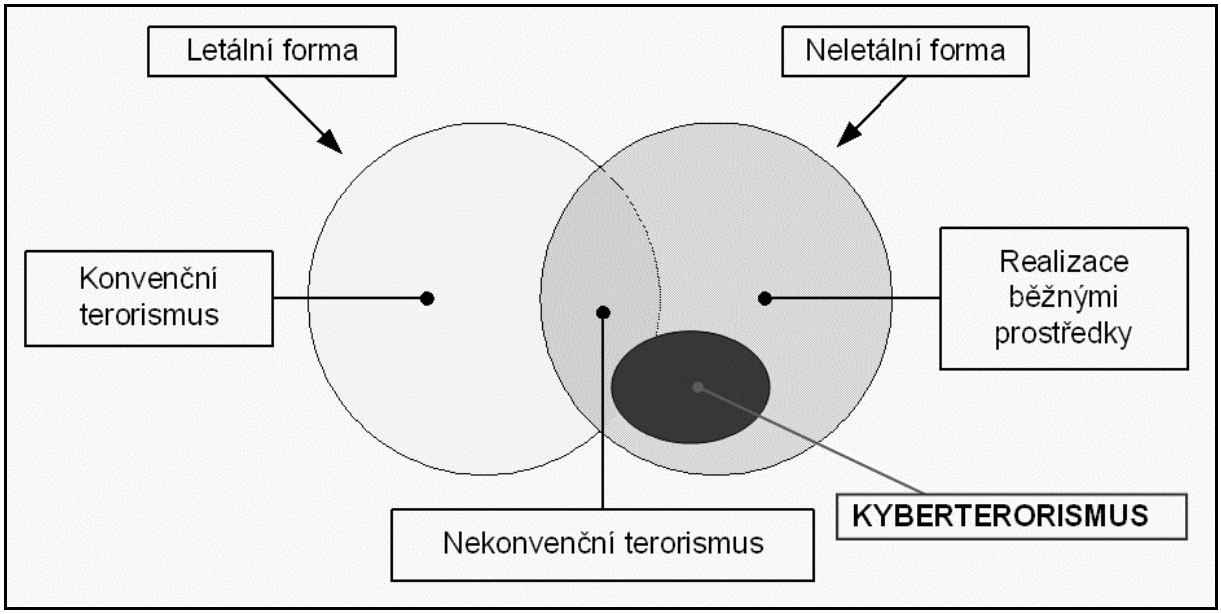
Současnou společnost je možné, i když s určitými výhradami, považovat v ideálním stavu za informační, protože téměř každé malé dítě zná internet a počítač, tudíž má přístup k informacím a dokáže je využívat. Bohužel, stále tu je slovíčko „téměř", které nás dělí od ideálního stavu a plnohodnotného označení „informační společnost".

Informační společnost se pohybuje v tzv. **kyberprostoru**, který byl definován panem Williamem Gibsonem z roku 1984 vymezuje takto: „*Konsensuální halucinace každý den zakoušená miliardami oprávněných operátorů všech národů, dětmi, které se učí základy matematiky. Grafická reprezentace dat abstrahovaných z bank všech počítačů lidského systému. Nedomyslitelná komplexnost. Linie světla seřazené v ne-prostoru mysli, shluky a souhvězdí dat.*"[2]

Dnes je pojmem kyberprostor označován svět virtuální reality, v němž se odehrávají různé, paradoxně reálné věci – např. telefonické hovory, mailová komunikace, apod. Běžný člověk může, z hlediska informatického, tento pojem zaměnit za mnohem rozšířenější pojem **internet**. Ten však zcela označuje určitou konkrétní část virtuální reality kyberprostoru.

Kyberprostor však čelí určitým hrozbám. Jednou z nich je kyberterorismus, který je možné vymezit jako neletální formu teroristické činnosti realizovanou skrze služby, které podporuje a sdílí daná informační či komunikační síť. Neletální forma je však pouze vnější skořápkou, protože sekundárním důsledkem kyberútoku může být právě fyzická likvidace konkrétního objektu nebo systému, což může vést i k ztrátám na lidských životech, ovšem většinou se nejedná o primární cíl takového útoku. Grafické začlenění pojmu kyberterorismu do množiny terorismu ukazuje obr. č. 1.

Oficiální definice kyberterorismu vyřčená D.E.Denningem zní následovně: *„Kyberterorismus je konvergencí terorismu a kyberprostoru obecně chápaný jako nezákonný útok nebo nebezpečí útoku proti počítačům, počítačovým sítím a informacím v nich skladovaným v případě, že útok je konán za účelem zastrašit nebo donutit vládu, nebo obyvatele k podporování sociálních nebo politických cílů."*[3]



Zdroj: JÍROVSKÝ, V. Kyberterorismus. ICTfórum/PERSONALIS 2006. [předneseno 27.9.2006]. Praha. (prezentace na konferenci – nepublikováno).

Obr. 1.: Schéma začlenění pojmu kyberterorismu do množiny terorismu

Bohužel, definice je poněkud zavádějící, protože chápe jako akty kyberterorismu útoky směrované proti kritické infrastruktuře, které mají za cíl získání informační nadvlády. Paradoxně častěji jsou na internetu zaznamenány útoky narušující funkci určité služby či jejích součástí, aniž by daný útok byl veden proti konkrétní společnosti nebo vládě s konkrétním účelem (např. vydírání).

Kyberterorismus dá dle svého působení dělit na dva směry:

- první směr je čistě propagandistický (informační) a inklinuje k negativní či odmítavé reakci na aktuální stav mezinárodní či národní politické situace (propagace jednotlivých teroristických skupin, propagace ideologií, apod.).
- druhý směr realizuje přímá napadení konkrétních informačních sítí a likvidace síťových služeb a je tudíž výrazně nebezpečnější, neboť ve své snaze útočník většinou paradoxně zničením sítě nebo její části zlikviduje i svůj operační prostor, což je k hlediska taktického jakési Pyrrhovo vítězství, ovšem z hlediska informační nadvlády je to maximální informační výhra - nejsou-li informace bude protivník dezorientovaný a nebude schopen reagovat na souběžné útoky na různá místa.

Díky tomuto dělení se dostáváme ke jakési obecné kategorizaci využití informační sítě pro teroristické potřeby, které můžeme rozdělit do tří úrovní:

- ***vnitřní řízení*** – teroristická skupina využívá informačních technologií k řízení svých lidských zdrojů, rozptýlených po celém světě. Sem typicky patří např. využití steganografie (skrytí textu do obrázků) pro předávání úkolů a reportů mezi jednotlivými členy skupiny.
- ***lokální kyberútok*** – samostatný přímý útok na konkrétní technologii či službu. Nebezpečnost tohoto druhu útoku je závislá na zkušenostech, cílech a možnostech dané skupiny. Pro vedení útoku jsou potřeba zkušení uživatelé síťových služeb a IT specialisté, kteří mají potřebné znalosti a zkušenosti v oblasti bezpečnosti počítačových sítí.

- ***souběžný útok*** – nejnebezpečnější varianta útoku, kdy dochází k několika paralelním útokům na konkrétní oblasti či cíle na různých úrovních. Kyberútok v této fázi je pouze jakousi přípravou pro napadení útočníka nebo přímou podporou pro jeho dezorientaci a likvidaci, která může být v přímé součinnosti s přímou akcí speciálních jednotek nebo např. leteckým bombardováním či dělostřeleckou přípravou. Může také docházet ke koordinaci několika různých druhů útoků (např. zajistit rozšíření nebezpečného malware pomocí zablokování určitých služeb sítě).

Tímto se dostáváme k tomu, abychom definovali jednotlivé programové prostředky, které se při kyberútoku nejčastěji používají. Jedná se tzv. malware, což je specifické programové vybavení sloužící v narušení funkcí jednotlivých prvků sítě nebo služeb, které poskytují. Malware se typicky dělí na počítačové viry, trojské koně, adware a spyware.

- Adware – speciální programové vybavení sloužící k podpoře úmyslného získání a odposlechu informací z jednotlivých koncových stanic počítačové sítě (např. odposlech přihlašovacích údajů k různým internetových službám, apod.).
- Spyware – speciální softwarové vybavení sloužící k utajenému odeslání údajů o uživateli. Metoda vznikla jako podpora cílené reklamy, ale v současné době již svou prvotní funkci výrazně překročila.
- Počítačové viry – speciální programové vybavení, které má za cíl likvidaci konkrétní služby či funkce jednotlivých prostředků počítačové sítě.
- Trojské koně – specifická skupina počítačových virů, které se navenek prezentují jinou funkci, než-li doopravdy realizují. Většinou se jedná o jakési ukryté viry (backdoors), které při splnění konkrétní podmínky (konkrétní datum, spuštění konkrétních aplikaci či služeb, apod.) spustí své „skryté“ funkce.

Jak je vidět, oblast malware zahrnuje různé uživatelsky nepříjemné aplikace, které mohou mít na náš systém jeden nebo více negativních dopadů. Těmi mohou být:

- krádež dat a informací – v dnešní době nejtypičtější varianta nasazení malware, resp. spyware/adware na koncovou stanici.
- zničení dat – dnes druhá nejtypičtější varianta útoku malware na koncové stanice v počítačové síti.
- destabilizace systému – nekompatibilita malware s daným operačním systémem může vést k zablokování služeb či zhroucení celého systému; v některých variantách může dojít pouze ke zpomalení systému tím, že daný maligní kód alokuje určité zdroje (např. operační paměť).
- blokování místa – malware může alokovat určité místo v rámci pevného disku, což při dnešních kapacitách není takovým problémem, jako v minulosti, ale v oblasti operačních pamětí se může i při dnešních kapacitách jednat o významnou položku; přesto již tento projev není tolik žádaný a častý.
- jiné projevy malware – mezi nejméně nebezpečné projevy malware patří různé zvukové či grafické projevy, které ovšem mohou být v kombinaci s dalšími výše uvedenými variantami napadení.

Motivace útočníků (kyberteroristů) je samozřejmě různorodá – od finančního zisku přes slávu a snahu o publicitu a veřejné uznání až po realizaci pomsty proti konkrétní společnosti či skupině lidí. Samozřejmě, nejde zcela detailně a striktně veškeré kyberteroristy „zaškatulkovat“ do nějaké skupiny, ale je možné typově a motivačně dané útočníky rozdělit do 9 různých skupin.

Prvním společným motivačním faktorem je tzv. **internetový exhibicionismus (výstřednost)**, kdy útočníci mají touhu být uznáváni v rámci své skupiny tzv. odborníků.

Hacker-začátečník

Jedná se o začátečníka v oblasti IT s minimálními znalostmi a dovednostmi, využívající volně dostupných programových nástrojů z internetu. Většinou se jedná o ideálního nadšence, který funguje jako mezistupeň mezi hackerem-profesionálem a běžným uživatelem. Je to právě tento nováček, který zcela nepokrytě „rozšiřuje" malware do počítačů uživatelů a podporuje tak přímo či nepřímo činnost hackera-profesionála.

Motivací k tomuto druhu jednání je snaha o nalezení vzrušení a především uznání a slávy v rámci „hackerské" komunity. Pro seberealizaci v tomto směru je ochoten udělat téměř cokoliv.

U tohoto druhu útočníka neexistují typizované cíle jeho útoků, protože se snaží útočit na cokoliv bez ohledu na smysluplnost daného napadení a to proto, aby získal pomyslnou trofej a uznání v rámci „hackerské" skupiny.

Hacker-profesionál

Hacker-profesionál je typicky znalec IT preferující typickou myšlenku hackerství mluvící o svobodném přístupu a sdílení všech informací. Většinou se jedná o člověka, který neuznává osobní vlastnictví, zákon a normy, autorská práva a autority.

Jeho motivací je tzv. internetový exhibicionismus, což je snaha o překonání intelektuálních výzev a psychologicky i dětinská radost z překonávání překážek. Druhotným cílem je snaha o zajištění přístupnosti informací pro všechny.

Typické provedení jeho útoků je založeno na specifickém spolupodílnictví, protože nechce nést přímou vinu za útok a proto zpracovává programové skripty, které pak nechává šířit pomocí ostatních uživatelů v počítačové síti, popř. skrze ambiciózní začátečníky v oboru (hacker-začátečník).

Druhou možnou motivací útočníků v kyberprostoru je realizace **pomsty**, vedené buď proti konkrétní firmě, organizaci nebo zájmové skupině lidí. Většinou je jedná o skupinu zkušených lidí nebo IT odborníků.

Virový tvůrce

Virový tvůrce je typický odborník IT, většinou programátor s hlubokými znalostmi z oblasti bezpečnosti IT a počítačových sítí. Jedná se o velmi specifický druh lidí, kteří jsou buďto „zrazenými idealisty" nebo „nedoceněnými odborníky", což vede k jejich uzavření se světu a případnému začleňování se do různých, podobně orientovaných skupin, kde mohou získat jak docenění, tak možnost realizace svých motivací, kterými je většinou pomsta vůči společnosti nebo konkrétní skupině či organizaci, popř. snaha dokázat sobě nebo světu svou sílu a „dokonalost". Druhotnou motivací může být překonávání intelektuálních výzev.

Cílem virových tvůrců jsou počítačové systémy a veškeré počítačové sítě. Virový tvůrce prostě útočí na cokoliv.

Vnitřní nepřítel

Jednou z nejzákeřnějších forem útočníků je tzv. vnitřní nepřítel, což představuje nejčastěji „zrazeného" zaměstnance firmy či organizace, který cítí určitý stav (pozici) ve firmě jako osobní křivdu a hodlá zneužít svých pravomocí k odplatě vůči dané organizaci či společnosti. Většinou se jedná o IT odborníka či administrátora výpočetních systémů introvertního typu, často egocentrický člověk s nedostatkem empatie a schopnosti mezilidské ko-

munikace. A právě pocit nedoceněnosti, křivdy nebo méněcennosti je hybnou formou jeho aktivit.

Typicky využívá velmi dobře maskované útoku pomocí malware vedoucí často k likvidaci či vysokým finančním ztrátám pro cílovou společnost, bez většího faktického zisku pro útočníka.

Další velkou motivací kyberútočníků je snaha o **finanční zisk**, popř. **finanční ztrátu** pro cílový objekt. Přímé útoky na bankovní konta sice dnes již nejsou tak časté, ale pokusy o odposlechy přihlašovacích údajů do jednotlivých systémů bank (phishing) jsou dnes popsány v desítkách variant. Podívejme se tedy typizaci těchto druhů útočníků.

Informační válečník

Jedná se o profesionála zabývajícího se primárně ochranou IT systémů před narušiteli. Daný odborník většinou má hluboké technologické znalosti a speciální trénink, díky čemuž se stává velmi těžkým protivníkem a ideálním útočníkem.

Motivace tohoto typu útočníků je buď ve vlastenectví nebo sounáležitost s náboženskou, sociální či jinou entitou (typicky názorově blízký ideologii teroristické skupiny). Extrémní motivací může však být i finanční zisk či snaha o finanční likvidaci protivníka.

Typické útoky jsou vedeny za účelem destabilizace a poškození integrity dat či nabourání informačních systémů, především na úrovni kontroly rozhodovacích procesů. K dosažení cíle využívá tradiční i netradiční metody, postupy a technologie, vycházející z jeho hlubokého porozumění a zkušenostem z oblasti bezpečnosti informačních systémů.

Zloděj

Zloděj je útočník s průměrnými znalostmi IT technologií, jenž touží především po finančním prospěchu bez zbytečné slávy a publicity. Průběžně se zkušenostmi mění jeho znalosti IT a postupně se zdokonaluje až na úroveň profesního kriminálníka. Jeho motivací je nenasytnost po finančním zisku, pro který udělá cokoliv.

K typickým druhům útoků, které používá je právě odposlech přihlašovacích údajů (phishing) do informačních systémů bank či k účtům nebo útoky vedené na platební karty klientů těchto zařízení.

Profesní kriminálník

Je profesionál, který se dal na cestu zločinu a své znalosti z oblasti IT plně využívá k uskutečnění svých protizákonných aktivit. Může být i najímán různými zločinnými organizacemi a maximálně se vyhýbá střetům se státními institucemi. Psychicky se jedná o velmi odolného jedince, jehož jediným cílem jsou peníze nebo finanční prospěch. Popularita je pro jeho aktivity rizikem, protože vždy svým jednáním porušuje zákony.

Typické útoky jsou vedeny také na účty či platební karty klientů finančních domů, ale vždy se snahou o získání všech finančních prostředků, nikoliv pouze nějaké části.

Poslední možnou motivací k útokům v kyberprostoru je snaha o **publicitu** a **slávu**, která mnohdy souvisí k labilní psychikou daného jedince, popř. s traumaty, která v minulosti zažil.

Kybernetický chuligán

Většinou hrdý egoista s vyššími znalostmi v oblasti IT, často programující vlastní skripty fungující na úrovni webových technologií. Výběr cílů podniká tak, aby podpořil upoutání pozornosti médií, často proto útočí na státní instituce či polostátní organizace.

Jeho jedinou touhou je sláva a snaha o medializaci svých činů. Někdy dochází k paradoxu, kdy se díky výběru cílů se může stát „hrdina médií".

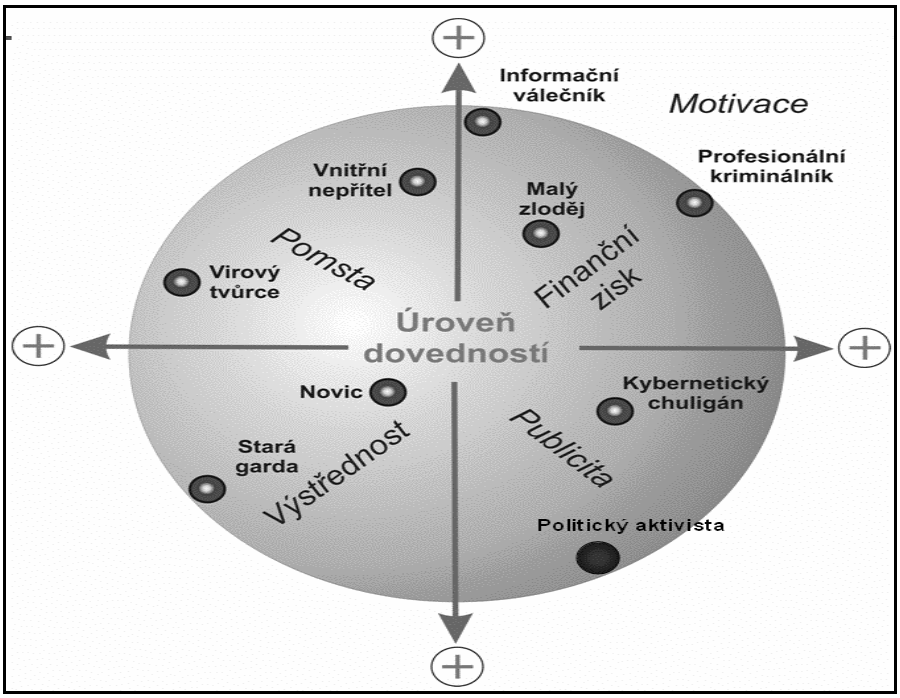
K jeho typickým útokům patří defacement webových stránek (záměna webu za svou verzi), krádeže a zneužití platebních karet, personálních údajů a telekomunikační podvody.

Politický aktivista

Po informačním válečníkovi druhý nejhorší druh útočníka. Většinou se jedná o znalce z oblasti IT, jehož snahou je skrze kyberprostor reagovat na aktuální politické dění. Často se jedná o fanatika nebo idealistu zastávající extrémní politické názory, za něž vášnivě bojuje. Motivací k útokům mu je aktuální politické dění na úrovni mezinárodní nebo národní politiky.

Ke svým útokům využívá plně svých znalostí z oblasti a tudíž pro dosažení politických cílů může využívat široké spektrum různorodých metod – od propagandistického defacementu po přímé napadení a likvidaci státních informačních systémů.

Toto je tedy obecná typizace útočníků. V běžném životě samozřejmě některé druhy útočníků splývají a některé se mohou dále detailněji členit, což ovšem není cílem tohoto článku. Následující obrázek ukazuje všechny skupiny v přehledném schématu (obr. 2.).



Zdroj: RAK, R. Homo sapiens versus security. ICTfórum/PERSONALIS 2006. [předneseno 27.9.2006]. Praha. (prezentace na konferenci – nepublikováno).

Obr. 2.: Graf klasifikace typů kyber-útočníků

Přesto podle analýz je možné říci, že nejčastější motivací pro kybernetické útoky je reakce na konkrétní politické situace mezinárodní nebo národní politiky.

Podle dopadů je ověřeno, že na stabilitu a funkčnost počítačové sítě má větší vliv právě kybernetický útok (např. šíření počítačového viru), než-li přímé destruktivní útoky (např. útok na ambasády či na WTC). Je to logické, protože kybernetický útok je z hlediska strategického použití spíše záležitostí vojenskou. Jeho ideální použití je jako souběžného útoku společně s přímou likvidací či jako přípravu pro přímou bojovou operaci (např. umlčení komunikační soustavy protivníka).

Ovšem i v době míru je kybernetický útok velmi nebezpečnou zbraní použitelnou k vydírání či likvidaci konkurence nebo oponenta bez přímé konfrontace. Uplatnění těchto metod a postupů je možné jak v rámci průmyslové špionáže (vytěžení informací), tak v konkurenčním boji či v rámci propagace teroristické ideologie.

Problém internetu a moderní informační společnosti bude do budoucna v tom, jak odolávat jednotlivým bojovníkům či celým armádám kyber-válečníků, kteří se ve své slepé snaze za slávou, penězi či likvidací protivníka budou postupně „nahlodávat" stabilitu a funkčnost globální počítačové sítě. A právě v této skutečnosti je největší zranitelnost, jak moderní informační společnosti, která bez informací nemůže plnohodnotně fungovat, tak i počítačové sítě (internetu) jako nosného média. Pro bezpečnostní složky státu, počínaje policií, armádou a zpravodajskými službami konče, zde vyvstává nová hrozba, které je nutné čelit a dostatečně dobře se na ní připravit – jak technologicky a personálně, tak především znalostně.

Vyvstává zde nebezpečí, že budoucí konflikty zcela ztratí svůj konvenční rozměr a stanou se nekonvenčními válkami, v nichž ani nebude nutné, aby jedna či druhá strana použila klasického vojenské taktiky či letálních zbraní. Naopak k likvidaci státu protivníka bude stačit vysoce specializovaná skupina, která provede několik útoků na kritickou informační strukturu daného státu (banky, pojišťovny, komunikační sítě, informační systémy národní působnosti, informační systémy státní správy, databáze (např. obyvatelstva), systémy řízení podniků, systémy dodávky rozvodných sítí, apod.). Výsledkem pak může být destabilizace a případná likvidace státu zevnitř.

Cílem výcviku nejen ozbrojených sil, ale i ostatních bezpečnostních složek státu by měla být schopnost zachytit, analyzovat a eliminovat tyto pokusy o destabilizaci státu, stejně jako příprava a nácvik krizového plánu v případě masivního kyberútoku, který samozřejmě může být pouze podpůrnou součástí dalších paralelních akcí (např. přímého útoku, hospodářských sankcí, blokády státu, leteckého bombardování a dalších). Ideální by v tomto směru byla úzká spolupráce policie a armády, které by tak byly připraveny v době míru i v době krize na společnou ochranu v oblasti informačních technologií.

Literatura:

JÍROVSKÝ, V. Kyberterorismus. ICTfórum/PERSONALIS 2006. [předneseno 27.9.2006]. Praha. (prezentace na konferenci – nepublikováno).

RAK, R. Homo sapiens versus security. ICTfórum/PERSONALIS 2006. [předneseno 27.9.2006]. Praha (prezentace na konferenci – nepublikováno).

Kyberterorismus roste závratným tempem. Novinky.cz [online]. 2006 [cit. 25.10.2006]. Dostupné na WWW: [http://www.novinky.cz/internet/kyberterorismus-roste-zavratnym-tempem_62464_hthrs.html].

Cyber-terorismus do dvou let realitou. Zive.cz [online]. 2006 [cit. 25.10.2006]. Dostupné na WWW: [http://www.zive.cz/h/Uzivatel/Ar.asp?ARI=119425].

Poznámky:

[1] DYTRT, Z., MIKULECKÝ, P., NEJEZCHLEBA, M., PRILLWITZ, G., ROUDNÝ, R. (editoři): Etika podnikání a veřejné správy: Informační společnost – etická výzva pro 21. století. Sborník z 2. mezinárodní konference, Hradec Králové, 18. – 20. 5. 1999, Vyd. VUSTE ENVIS Praha, 1999, ISBN 80-902356-5-4

[2] Kyberprostor [cit. 19.10.2006]. Wikipedia – the Free Encyclopedia. [online]. Dostupné na WWW: [http://en.wikipedia.org/wiki/Cyberspace].

[3] DENNING, D. E. [cit. 15.10.2006]. Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy. [online]. Dostupné na WWW: [http://www.nautilus.org/info-policy/workshop/papers/denning.html].