Některé trendy informační války, počítačové kriminality a kyberterorismu

Josef Požár – Policejní akademie ČR v Praze

Úvod

Již po delší dobu jsme svědky bouřlivého rozvoje informačních a komunikačních technologií (ICT). Je zřejmé, že ještě bouřlivější období máme teprve před sebou. Snaha maximálního využití ICT má však i své negativní stránky a důsledky. Se vznikem nového technického fenoménu se najdou lidé, kteří jej využijí k páchání trestné činnosti. Nejinak je tomu s ICT. Tak se objevila i počítačová kriminalita, představující nový druh trestné činnosti. V souvislosti s teroristickými útoky využívají teroristé nových metod, forem a technik ICT a tak vznikl kybernetický terorismus čili kyberterorismus. Kyberterorismus (angl. cyberterrorism) pak volně chápeme jako aplikaci a využívání informačních a komunikačních technologií pro teroristické cíle různých skupin.

Tento kriminální fenomén má mezinárodní charakter. Dnes je možné během několika milisekund napadnout rozsáhlé komunikační sítě a narušit jejich funkci a tak ve své podstatě působit na vlády zemí a jejich obyvatelstvo panikou, hrozbami a jiným nebezpečím.

Cílem tohoto příspěvku poukázat na kybernetický terorismus jako jednu z forem terorismu a jeho souvislosti s počítačovou kriminalitou. Uvádí vztah informační války a kyberterorismu s možnými trendy kyberterorismu.

Informační válka

Z dostupné literatury je zjevné, že pojem **informační válka** (information war, infowar, information warfare) není dosud ustálen, neboť neexistuje jeho všeobecně přijatá definice. Práce [3], která velmi důkladně shrnuje terminologii vyskytující se v literatuře o informační válce, uvádí 2 definice pojmu information war a 29 definic pojmu information warfare. K předběžnému orientačnímu vymezení pojmu informační války lze použít skutečnosti, že další specifikací pojmu válka je nejčastěji 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, jaderné letecké, chemické, bakteriologické a také informační apod. Analogicky informační válka je válka, která je vedena v oblasti informací nebo válka, v níž se bojuje informacemi. Je třeba si však uvědomit, že „oblast informací“ neexistuje stejným způsobem jako země, moře, vzduch a vesmír. Podobně není informace zbraní ve stejném smyslu jako zbraň konvenční, jaderná, chemická, bakteriologická apod. Z analogie by se mohla informační válka také chápat jako válka o informace, tedy válka, kterou vedou lidé pracující s informacemi, případně jako válka, kterou charakterizují informace.

Význam informace zde budeme chápat v co nejširším smyslu jako synonymum pro poznání nebo vědění. Jen tak si totiž můžeme být jisti, že v našem zkoumání informační války nic důležitého nechybí. Informační válka by se v žádném případě neměla chápat jako něco nového výlučně spojeného s počítači, počítačovými sítěmi nebo dalšími moderními technologiemi. Informační válka je stará jako válka sama. Geniální stratég vedení informační války může být i počítačově negramotný člověk. Pokud by si to vyspělé země neuvědomovaly, mohly by být někdy navzdory své vyspělé technologii velmi nepříjemně překvapeny.

Protože každá válka, a tedy i informační, je zvláštním případem konfliktu, konfliktní situace, budeme při výkladu vycházet z obecné teorie produkce a řešení konfliktních situací. Tuto problematiku velmi podrobně popisuje Hník[1].

Optimální řešení informační války, nehledě na technická omezení, je nemožné bez optimálního jednání všech účastníků situace, pro něž hledáme řešení. To však možné není, neboť ve státech nebo velkých skupinách, které mohou vést informační válku, je vždy naprostá většina těch, kteří nežijí a tedy ani nejednají optimálně. V praxi bude důležité znát optimální řešení dané situace, avšak realizovat bude možno jen řešení relativně nejlepší, totiž to, které dovolí skutečné cíle, znalosti a dovednosti účastníků nehledě na jejich technické, ekonomické a organizační možnosti. Informační válka je nadto z principiálních důvodů chudá na informace, účastníci se většinou musí rozhodovat na základě neustálého nedostatku informací, přičemž o důležitých skutečnostech nemohou mít poznání jisté, nýbrž jen pravděpodobné. Snaha o přesnost v teorii by také neměla zakrýt skutečnost, že jednotlivé správné rozhodnutí se z teorie odvodit nedá. Každé rozhodnutí v dané situaci by se mělo uskutečnit jako syntéza všech dostupných obecných i konkrétních poznatků; v základu je to úkon svobodné vůle a jako takový podléhá kriteriím etickým. Touto problematikou je proto nutné se zabývat také, jinak řešení problematiky informační války nemůže být úplné. Zde je možné a vhodné na tuto skutečnost jenom upozornit.

Situace, účastník situace, a cíl účastníka situace jsou základní a vzájemně provázané pojmy. K tomu, aby bylo možno o předmětu přesně uvažovat, jsou však naprosto nezbytné. Bez nich nelze zavést pojem konflikt, konfliktní situace, a bez pojmu konflikt je velmi obtížné přesně uvažovat i o informační válce.

V každém konfliktu tedy i k kriminalistice a kyberterorismu existují zjednodušeně řečeno dvě strany: útočník a obránce. Oba mají své cíle, které jsou protichůdné, konfliktní.

Cíl, který souvisí s informací, může představovat získání informace, znemožnění získání informace, udržení získané informace, ztracení či zničení získané informace, šíření informace nebo znemožnění šíření informace. Obránce se 1. může snažit získat informaci nebo 2. se může snažit získanou informaci udržet. V prvním případě se útočník snaží znemožnit obránci informací získat, ve druhém případě se útočník snaží, aby obránce získanou informaci ztratil. Další dvě možnosti jsou analogické předchozím dvěma, pouze jsou zaměněni obránce a útočník: 3. útočník chce získat informaci, obránce tomu chce zabránit, 4. útočník chce udržet získanou informaci, obránce chce, aby útočník získanou informaci ztratil. Pátá možnost vzniká, když se obránce snaží, aby útočník získal nějakou informaci, útočník se tomu snaží zabránit, čili se snaží sám sobě znemožnit získat informaci. Šestá možnost vzniká, když se obránce snaží, aby útočník získanou informaci udržel, útočník se tomu snaží zabránit. Další dvě logické možnosti jsou analogické případům č. 5 a 6 se záměnou obránce a útočníka: 7. útočník chce, aby obránce nějakou informaci získal, obránce se tomu snaží zabránit, 8. útočník chce, aby obránce získanou informaci udržel, obránce se ji snaží ztratit. Devátá možnost vzniká, když se obránce snaží šířit informaci a útočník se tomu snaží zabránit, desátá možnost je opačná: informaci se snaží šířit útočník, obránce se tomu snaží zabránit.

[1] HNÍK , V. Hrozby informační války. In *2. ročník konference Informační bezpečnost – teorie a praxe : Sborník materiálů z konference konané ve dnech 7. a 8.10.2002.* Brno : AFOI, AFCEA, 2002.

U obránce, podobně i u útočníka mohou nastat následující stavy, které vyjadřuje tabulka 1:

	Obránce	**Útočník**
1	Chce získat informaci	Chce znemožnit obránci získat informaci
2	Chce udržet získanou informaci	Chce, aby obránce získanou informaci ztratil
3	Chce znemožnit útočníkovi získat informaci	Chce získat informaci
4	Chce, aby útočník získanou informaci ztratil	Chce udržet získanou informaci
5	Chce, aby útočník získal informaci	Chce, aby nemohl získat informaci
6	Chce, aby útočník udržel získanou informaci	Chce ztratit získanou informaci
7	Chce, aby nemohl získat informaci	Chce, aby obránce získal informaci
8	Chce ztratit získanou informaci	Chce, aby obránce udržel získanou informaci
9	Chce šířit informaci	Chce zabránit šíření informace
10	Chce zabránit šíření informace	Chce šířit informaci

Tab. 1. Typy informačního boje

Uvedených deset možností představuje deset základních typů informačního boje a informační války. Účastníci boje nebo války vstupují do konfliktu právě kvůli sporu o informaci. Bez dotyčné informace a neslučitelného názoru na ni od obou stran by boj nebo válka nemohly vzniknout nebo se udržet. Nejde při tom prvotně o to, jak důležitá tato informace je, čeho se týká, a dokonce nejde ani o to, zda je pravdivá nebo nepravdivá. Podstatné je to, aby se cíle obou protivníků týkaly té informace, byly vzájemně v rozporu a aby byl obránce k prosazení svých cílů z důvodu dostatečně závažného oprávněn použít násilí.

Podstata počítačové kriminality

Počítačová kriminalita je jistě výrazným jevem dnešní doby. Zájem o informace, byť byly zpracovávány, přenášeny a uchovávány jiným způsobem, je mnohem staršího data. Jen jsme byli zvyklí a stále tak to i chápeme, tyto jevy nazývat jinými pojmy jako vyzvídání, vyzrazování atd., zejména podle způsobu uplatnění informací. Z toho vyplývá, že bychom spíše měli hovořit o informační kriminalitě, která je chápána jako širší pojem než kriminalita počítačová.

Termínem počítačová kriminalita se obvykle označují trestné činy zaměřené proti počítačům stejně tak i trestné činy páchané pomocí počítače. Počítačovou kriminalitu definujeme velmi obecně jako trestný čin namířený proti integritě, dostupnosti nebo utajení počítačových systémů nebo trestný čin, při kterém je použito informačních či telekomunikačních technologií. Jiní autoři chápou počítačovou kriminalitu jako veškeré aktivity, které vedou k neautorizovanému čtení, manipulaci, vymazání nebo zneužití dat. Je to tzv. počítačová defraudace jako jedna z metod počítačové kriminality založená na změně nebo jiné interpretaci dat s cílem získat výhodu, peníze pro vlastní neoprávněnou potřebu.[2]

Státy Evropské Unie a Evropského parlamentu se dohodly na následující definici počítačové kriminality: je to nemorální a neoprávněné jednání, které zahrnují zneužití údajů získaných prostřednictvím ICT nebo jejich znění. Počítače v podstatě neumožňují páchat

[2] ZELENKA, J., ČECH, P., NAIMAN,K. *Ochrana dat. Informační bezpečnost – výkladový slovník.* Hradec Králové : Gaudeamus. 2002, s.106.

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 anebo špionáž.

Počítačová kriminalita má řadu výrazných charakteristik, které ji odlišují od kriminality klasické. Ve většině případů počítačové kriminality se neobjevují takové prvky, jako je násilí, použití zbraně, újma na zdraví osob apod. Zatímco však u klasické kriminality se měří doba spáchání trestného činu na minuty, hodiny, dny, trestný čin v oblasti počítačové kriminality může být spáchán v několika tisícinách sekundy a pachatel ani nemusí být přímo přítomný na místě činu.

Další významnou charakteristikou pro počítačovou kriminalitu jsou v důsledku značné ztráty, ať již přímo v podobě finančních částek, nebo v podobě zneužití získaných údajů. Počítačovou kriminalitu také provází určitá diskrétnost trestné činnosti. Z uvedeného vyplývá, proč počítačová kriminalita bývá, pro svou povahu, označována jako kriminalita "bílých límečků".

S počítačovou kriminalitou souvisí jistě i ochrana informací a dat v informačních systémech. Aby bylo možno hovořit o počítačové kriminalitě, musí pachatel ke svému jednání užít nejen výpočetní techniku, ale jeho jednání musí také naplňovat znaky skutkové podstaty některého trestného činu uvedeného v trestním zákoně a nebezpečnost takového jednání musí dosahovat požadovaného stupně nebezpečnosti činu pro společnost.

Za počítačovou kriminalitu budeme považovat trestné činy, jejichž objektem, eventuálně objektivní stránkou bude informační technologie v plném slova smyslu. Jedno z možných členění počítačové kriminality přijala Rada Evropy. Jejím smyslem je mimo jiné 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:

- 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:

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

Tím, že byla vymezena jednání do těchto dvou seznamů, došlo v podstatě k vymezení trestných činů, které je žádoucí stíhat v evropských zemích. 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. Tímto způsobem byla klasifikována počítačová kriminalita tak, že by mělo být jasné, co vše lze pod tento pojem zahrnout. S počítačovou

kriminalitou vyššího stadia je kyberterorismus, který je druhem počítačové kriminality na rozsáhlém prostoru vyvoláním strachu širokých vrstev obyvatel.

Trendy počítačové kriminality

Kromě běžných uživatelů ICT se bohužel řadí také mnoho zločinců. Počítačovou kriminalitu v současné době rozvíjejí ti, kteří v ní hledají zdroj obživy, což vede k narůstajícími zapojení organizovaného zločinu. Metody profesionálních zločinců jsou stále rafinovanější, a proto aktivní ochrana se stává absolutní nezbytností.

Dnešní firmy, organizace a státní instituce jsou na počítačích, počítačových sítích a obzvláště na internetu silné závislé. Vzniká nové odvětví hospodářské kriminality[3]. Počet evropských uživatelů internetu v prosinci 2004 prolomil hranici 100 milionů. Bohužel základní předností internetu jsou zároveň klíčovými složkami internetu, které potřebuje ke svému úspěšnému fundování také pachatelé počítačové kriminality. Dnes lze počítačovou kriminalitu charakterizovat následujícími trendy:

1) Nové delikty lze spáchat pouze on-line. Jedná se o trestné činy či pouze přestupky proti integritě, důvěrnosti a dostupnosti počítačových dat a informací. Nejlépe dokumentovanou formou tohoto typu deliktu je hacking.
2) Tradiční útoky na okolní počítače, sítě a informační systémy jsou provádění prostředky ICT také on-line. Pachatelé používají k útoku na systémy chránění trestním právem i prostřednictvím vydírání, podvodů a sociálního inženýrství. Před dvěma roky bylo zaznamenáno každý měsíc přibližně 300 škodlivých kódů a dnes je evidováno až 1500 ohrožení. Je to proto, že vzrostl počet síťových robotů (netvorů). Počítačová kriminalita zároveň odráží vývoj tradičních off-line kriminálních aktivit. Odhaduje se, že přibližně 70% veškerých škodlivých kódů vzniká za účelem zisku. Počítačová kriminalita je v Evropě trestně právní kategorií s nejvyšším nárůstem trestných činů.
3) Vzrůstající ohrožení mobilních komunikačních systémů. Loňský virus Cabir a jeho následné varianty ukázaly, že ani mobilní zařízení nejsou před útoky zvenčí bezpečná. Podle odhadů vzroste počet útoků na mobilní zařízení v průběhu roku pěti až desetinásobně.
4) Zneužívání sítí Wi-Fi. Síťoví červi představují nebezpečí pro mobilní telefony a další přenosná zařízení. Bezpečnost sítí Wi-Fi však byla v roce 2004 rovněž předmětem velkých obav. Viry napadající sítě Wi-Fi přecházet mezi jednotlivými sítěmi a spouštět lokalizované útoky typu Denial-of-Service.
5) Masové rozšíření spammingu pomocí trojských koní a botů. Velký nárůst počtu e-mailových červů (mass mailers) upozornil na jejich existenci. Masový spamming, který následně umožňuje stažení trojských virů, nakazí nechráněné počítače, aniž by to jeho uživatel zpozoroval. Takový způsob tajného infikování počítačů umožňuje útočníkům ovládat pomocí „botů“ – automatických programů, které z jiného počítače ovládají napadený počítač na dálku. Odborníci odhadují, že počet botů narůstá až o 30 každý den. Jedná se o nesmírně populární způsob napadení, protože infikování se neustále vyvíjí a je velice obtížné je vystopovat. V důsledku toho lze předpokládat, že poroste počet závažných „nárazových“ útoků. Jak se tisíce nakažených počítačů začnou spojovat do jedné obrovské sítě (bot network – botnet), umožní provádět rozsáhlé útoky typu Distributed Denial of Service, kde bude kritické úrovně dosaženo během několika minut a dokonce sekund a tak nastane zhroucení napadených serverů a stane se tak nedostupný , bude odmítat poskytovat služby.

[3] CHMELÍK, J., HÁJEK, S.,NEČAS, S. *Úvod do hospodářské kriminality*. Plzeň : Vydavatelství a nakladatelství Aleš Čeněk, 2005. s. 9.

6) Nárůst phishingu. Podle Anti.Phishing Working Group bylo v listopadu 2004 zaznamenáno 1518 nových jedinečných phishingových útoků proti 176 útoky v lednu téhož roku. Phishing znamená rozesílání falešných e-mailových zpráv ze zdánlivě oficiálních zdrojů. Tyto zprávy obsahují zpětné adresy nebo odkazy a požadují, aby adresát aktualizoval určité osobní informace, např. hesla, čísla bankovních účtů nebo dokonce PIN. To je však oblast sociálního inženýrství, které se v posledním období velice rozšiřuje. Vzhledem k tomu, že internetoví zločinci jsou stále motivováni finančním ziskem, se předpokládá, že počet případů phishingu se každý měsíc zdvojnásobí.
7) Rozšiřování spywaru. Internetoví zločinci se stále častěji zaměřují na finanční zisk. Spyware se tak bude stále častěji využívat např. k ukradení identity (identity theft), či monitorování klávesnice za účelem zachycení osobních údajů apod.

Pojem a podstata kyberterorismu

Novým rysem kyberterorismu v budoucnu bude plošnost a brutalita. 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 nejvíc lidí, způsobit rozsáhlé materiální škody a hospodářské ztráty. Imperativem je vyvolat celospolečenskou paniku, hrůzu a strach, otřást psychikou společnosti, zviklat víru lidí ve schopnost vlády chránit své občany.

Možnost využití počítačů i k páchání kriminální činnosti si odborníci uvědomili velmi rychle. Proto vznikl pojem cybercrime, který se u nás ujal pod názvem kyberterorismus.[4] 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.[5]

Obecně jsou známy dvě metody teroristických útoků

1) Cílem útoku je zničení protivníkova informačního systému a systémů závislých na ICT.
2) Informační technologie jsou využívány jako nástroj útoku pro manipulaci a zneužití cizích informačních systémů, ke krádeži nebo změně dat, případně k přetížení a zahlcení informačních systémů.

Značné možnosti k uplatnění kyberterorismu poskytuje prostředí internetu. Umožňuje teroristickým skupinám i jednotlivcům rychlou a utajenou výměnu informací, poskytuje prostor pro šíření jejich ideologií a názorů, umožňuje získávání nových aktivistů i sympatizantů. V jiných případech se internet stává bránou k průniku do počítačových sítí a poskytuje tak příležitosti k vedení kyberteroristických operací. Je však faktem, že teroristické skupiny využívají zatím internet více k propagandě a ke vzájemné komunikaci než ke kybernetickým útokům.

Uvádíme některé formy kyberterorismu, které shrneme do několika charakteristických bodů. Může se jednat o

- Kriminální akce s cílem získání peněz z cizích bankovních kont. Všechny banky nepoužívají dokonalé bezpečnostní systémy a toho v mnoha případech využívají právě kyberteroristé, nezřídka i přímí zaměstnanci finančního ústavu.

[4] SKOPAL, P. *Kyberterorismus jako reálná hrozba současnosti?.* Dostupné na Internetu: <http://www.pauza.cz/r-art.asp/id=166>.
[5] BRZYBOHATÝ, M. *Současný terorismus*. Dostupné na Internetu: <http://www.army.cz/avis/vojenské_rozhledy/2002_2/46.htm>.

- Snahy o získání výhody v oblasti konkurenčního zpravodajství (competitive inteligence). V praxi lze přece zveřejnit negativní informace o představitelích společností, 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. Kyberterorista pak provede útok na slabá místa informačního systému nebo zaměstnanci zaútočí na organizaci zevnitř. Z výzkumů 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 napadnou 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 určitými opatřeními již nyní. Tyto státy organizují operace, které mají v praxi potvrdit úspěšnost jejich boje proti kyberterorismu, ale přitom svou skutečnou utajují a maskují.
- Další závažný problém při využití Internetu k šíření extremistických názorů, pornografie, návodů na výrobu jaderných zbraní, omamných prostředků, výbušnin apod.

Kyberterorismus se stává vážnou hrozbou pro demokratické státy. V době, kdy vývoj výpočetní techniky má dynamiku v jiném odvětví nevídanou, lze předpokládat, že v blízké budoucnosti bude tento nebezpečný jev stále více aktuální.

Aktivní obrana je záležitostí mezinárodní spolupráce. Zpravodajská činnost v oblasti kybeterorismu je první linií aktivní obrany. Její součástí by mělo být posilování mezinárodních režimu kontroly a omezování šíření terorismu a prevenci kyberterorismu. Měla by též obsahovat prvek věrohodného zastrašení vůči státům prokazatelně podporujícím terorismus jako negativní sankci včetně vojenského úderu, stejně jako pobídky pro státy, které se rozhodnou s touto praxí skoncovat jako pozitivní sankce včetně hospodářské pomoci a bezpečnostních garancí. Neměla by opomíjet rozvojovou pomoc jako jeden z nástrojů dlouhodobé prevence a oslabování základny podpory a motivace terorismu v rozvojových zemích.

Boj proti kyberterorismu se v poslední době stává prioritou demokratických států i mezinárodního společenství. Vzhledem k tomu, že teroristické organizace působí stále častěji na mezinárodní nebo dokonce globální úrovni. Tomu odpovídají typy používaných prostředků, účinnost útoku i volené cíle, a proto je nutné hledat adekvátní řešení tamtéž, tj. přistoupit na internacionalizaci, popřípadě globalizaci protiteroristických akcí. Důležitou složkou mezinárodního systému zaměřeného na boj proti kyberterorismu, jehož dotvoření by měly státy ve vlastním zájmu podporovat, musí nadále zůstat mezinárodní právo. Pokud by jej státy opomíjely, snadno by se mohly dostat do stejné pozice jako ti, proti nimž vystupují. Tím by ohrozily nejen vlastní prestiž, ale zdiskreditovaly by v očích světové veřejnosti celou protiteroristickou kampaň. V období, kdy jsou kyberteroristé schopni během jediné akce usmrtit tisíce osob, by takový stav rozhodne nebyl žádoucí.

Pro názornost uvádíme tabulku 2 v literatuře [7], která vyjadřuje souvislosti hrozeb a prostředků teroristického násilí.

Hrozby (threats)	Prostředky (means)	Cíle (targets)	konečné cíle (ends)
Teroristické organizace	Vraždy	Státní organizace	Asymetrický konflikt
anonymní teroristické organizace	kybernetický útok	bankovnictví a finance kritická infrastruktura	bezpečnostní výhoda
pracovníci informační války	informační operace	obchod	ekonomická výhoda
Státní terorismus	infowar	Obyvatelstvo, vlády	politická změna
počítačoví hackeři	Logické bomby	kritická infrastruktura	politický vliv a zisk
počítačoví hackeři	Kybernetický útok	firmy, finance	finanční zisk
státem sponzorovaný terorismus	přímá akce	kritická infrastruktura	politická změna

Tab. 2. Vztahy hrozeb prostředků a cílů terorismu

Trendy kyberterorismu

Výzkum a vývoj technologií přináší stále nové elektronické prostředky, výpočetní techniku, komunikační prostředky a možnosti kódování a šifrování přenosu dat, ale i nové zbraňové systémy. To vše je předmětem zájmu teroristických skupin. Nelze opomenout vzrůstající vliv organizovaného zločinu na evropské úrovni. Sofistikovanost jeho činností, rozdělení sfér působnosti, ale i jeho vzrůstající brutalita Organizovaný zločin umožňuje teroristickým organizacím zisk peněz z obchodu s drogami, jejich legalizaci, ale i provádění přímých podpůrných akcí.

Výzkum a vývoj technologií přináší stále nové elektronické prostředky, výpočetní techniku, komunikační prostředky a možnosti kódování a šifrování **přenosu** dat, ale i nové zbraňové systémy. To vše je předmětem zájmu teroristických skupin.

Pokusíme se stručně nastínit předpovědi, predikce vývoje a trendy kyberterorismu.

Předpověď 1: Počet trestných činů hlášených policií, které se týkají ICT a ukládání dat v elektronických mediích podstatně zvýší požadavky na změnu priorit pro přidělování zdrojů. Proto bude nutné organizovat kvalitativně nový obsah školení a vzdělávání policistů a vyšetřovatelů. Bude nutný vznik a použití nových policejních specializací. Stejně tak státní zástupci a soudci musí získat a osvojit si nové znalosti v této kategorii trestných činů.

Předpověď 2: Rozsáhlá problematika počítačové kriminality bude ovlivňovat zákonnost, kdy se bude zvyšovat počet obětí trestných činů a finančních ztrát v souvislosti s internetovými podvody, včetně krádeží pomocí změněné identity pachatele. To znamená, že problematika počítačové kriminality bude ovlivňovat státní zaměstnance, kteří se stanou předmětem této trestné činnosti s finančními ztrátami. Současně budou narůstat podvody na Internetu, včetně podvodů související se změnou identity.

Předpověď 3: K virtuálním útokům a kriminalitě kyberteroristů bude docházet se zvýšenou frekvencí. Tyto závažné trestné činy mají charakter hrozby psychologické informační války. Příkladem může být počítačové chatování a přenos zpráv, hrozby, etnické zastrašování. Bude proto nutné přijmout nové zákony v oblasti informační bezpečnosti. Současně také všechny orgány budou aplikovat nové metody a prostředky pro vyšetřování, prevence a vzdělávání a výcviku.

Předpověď 5: Charakter špionáže se bude rozšiřovat do oblasti informační války, ekonomické špionáže a krádeží duševního vlastnictví. Vzniknou tak nové vzorce, procesy, komponenty, struktury a aplikace nových technologií spojené s marketingem, výrobou a prodejem zboží nebo služeb.

Předpověď 6: Skupiny organizovaného zločinu a teroristé budou stále více používat počítač jako nástroj kriminální činnosti k zajišťování komunikace.

Předpověď 7: Teroristické skupiny budou stále více používat globální sítě jako nástroj pro dosažení svých cílů. Zahrnuje to používání Internetu pro utajenou komunikaci a koordinaci cílů včetně jak šifrování tak i steganografii[6], stejně jako snahu využít přístup do sítě systému kritických infrastruktur v zájmu vytvoření chaosu, desinformací a zničení souborů.

Předpověď 8. Zločinci, teroristé a anarchisté budou ve zvýšené míře využívat informační a komunikační technologie jako základní nástroje a metody kdy mohou získat nebo narušit data/informace nebo zničit komunikační prostředky, informační procesy a nebo datové sklady. Příkladem mohou být elektromagnetickými pulsy, vysoké radiové frekvence, maligní software jako viry, červi, trojští koně a spyware[7].

Tyto předpovědi se mohou v některých nuancích poněkud lišit. Domníváme se však, že v globálu tato prognóza je zaměřena hlavně na stát a jeho organizace. Kyberteroristické útoky budou charakterizovány svou utajeností IP adres, maskováním identity a použitím kryptografických nástrojů, včetně steganografie aj.

Závěr

Informační technologie umožňují teroristům vytváření globální organizační sítě nového typu. Jejich struktury jsou, na rozdíl od tradičních skupin, volnější a méně hierarchické. Oslabuje se jejich závislost na státech, jednotlivé skupiny jsou funkčně autonomní, nicméně připravené ke společné akci. Teroristé se organizují do globálně propojených sítí a semiautonomních buněk, které se sdružují a přeskupují podle potřeb konkrétního úkolu.

Boj proti kyberterorismu bude nadále s rostoucí složitostí informačních a komunikačních technologií velmi složitý. Kyberteroristé budou vždy o krůček před teorií i praxí manažerů a specialistů informační bezpečnosti. Domníváme se, že kyberteroristé budou stále více útočit na důležité informační systémy státní infrastruktury. Tak regulace rozvodů elektrické energie, užitkové a pitné vody, dopravní systémy, zdravotnictví, telekomunikace jsou cíle, které mohou být zasaženy. Ovšem cíle nejsou omezeny jen na fyzická zařízení. Kvalitativní obsahová analýza odhaduje, že mezi tyto zbraně jsou řazeny také tzv. „genové zbraně“ (gene weapons). Tak genetické zbraně mohou působit za živé organizmy, obilí, dobytek i lidskou populaci.

Proto je nezbytné se neustále vzdělávat v takových oblastech jako je ochrana dat, informační bezpečnost, kryptografie a další obory. Toto vzdělávání by mělo být směrováno nejen na informační specialisty, ale zejména na politiky, manažery všech stupňů a zaměstnance firem a státních organizací.

Literatura

[1] Brzybohatý, M.: *Současný terorismus*. Dostupné na Internetu: <http://www.army.cz/avis/vojenské_rozhledy/2002_2/46.htm>.

[2] Doseděl, T.: *Počítačová bezpečnost a ochrana dat.* Praha : Computer Press, 2004.

[6] též tajnopis, jedná se o ukrytí tajné zprávy do běžné zprávy, skrytí přenášené zprávy. Používají se tajné inkousty, mikrotečky apod.

[7] Program, který odesílá z počítače po síti určitý typ informací. Je to speciální typ trojského koně, který umožňuje vzdálenou správu napadeného počítače. Musí být uživatelem nainstalován spolu s nějakým programem a pak v podstatě prohlíží počítač uživatele a odesílá informace o akcích, aniž o tom uživatel ví.

[3] Hník, V.: *Hrozby informační války*. Brno: Sborník z konference Inf. bezpečnost, 2002.
[4] Chmelík, J., Hájek, S., Nečas, S.: *Úvod do hospodářské kriminality*. Plzeň : vydavatelství a nakladatelství Aleš Čeněk, 2005. s. 9.
[5] Matějka, M.: *Počítačová bezpečnost a ochrana dat*. Praha : Computer Press, 2004.
[6] Whitaker, R.: *The Convoluted Terminology of Information Warfare*. Dostupné na Internetu: <http:/www.informatik.umu.se/~rwhit/IWGlossary.html>.
[7] Skopal, P. *Kyberterorismus jako reálná hrozba současnosti?*. Dostupné na Internetu: <http://www.pauza.cz/r-art.asp/id=166>.
[8] Kol. *Hrozby a ohrožení*. Dostupné na Internetu: <http:://www.army.cz/avis/vojenske_rozhledy/2001_1/161.htm>.
[9] Zelenka, J., Čech, P., Naiman, K.: *Ochrana dat. Informační bezpečnost – výkladový slovník.* Hradec Králové : Gaudeamus. 2002, s.106.

Anotace

Článek se zabývá některými aspekty počítačové kriminality a kyberterorismu poukazuje na různý pojetí tohoto fenoménu. Poukazuje na úzké souvislosti informační války a kyberterorismu. Uvádí možné hrozby a trendy vývoje kyberterorismu, které by mohly mít vliv na mezinárodní společenství a jednotlivé státy. Boj s kyberterorismem bude s rozvojem informačních a komunikačních technologií velmi složitý, a proto bude nezbytné se neustále vzdělávat v takových oblastech jako je ochrana dat, informační bezpečnost, kryptografie a další obory informačních a komunikačních technologií.

V informační válce jsou pojmy situace, účastník situace, a cíl účastníka situace základní a vzájemně provázané. Teoreticky existuje 10 různých stavů a typů informační války. Bez nich nelze zavést pojem konflikt, konfliktní situace a bez pojmu konflikt je velmi obtížné přesně uvažovat i o informační válce.

Výzkum a vývoj technologií přináší stále nové elektronické prostředky, informační a komunikační techniku, prostředky kódování a šifrování přenosu dat, ale i nové zbraňové systémy. To vše je předmětem zájmu teroristických skupin.

Boj proti kyberterorismu bude nadále s rostoucí složitostí informačních a komunikačních technologií velmi složitý. Kyberteroristé budou vždy o krůček před teorií i praxí manažerů a specialistů informační bezpečnosti. Kyberteroristé proto budou stále více útočit na důležité informační systémy státní infrastruktury. Regulace rozvodů elektrické energie, užitkové a pitné vody, dopravní systémy, zdravotnictví, telekomunikace jsou cíle, které mohou být zasaženy. Ovšem cíle nejsou omezeny jen na fyzická zařízení. Kvalitativní obsahová analýza odhaduje, že mezi tyto zbraně jsou řazeny také tzv. „genové zbraně" (gene weapons). Tak genetické zbraně mohou působit za živé organizmy, obilí, dobytek i lidskou populaci.

Je proto nezbytné se neustále vzdělávat v takových oblastech jako je ochrana dat, informační bezpečnost, kryptografie a další obory. Toto vzdělávání by mělo být směrováno nejen na informační specialisty, ale zejména na politiky, manažery všech stupňů a zaměstnance firem a státních organizací.

Klíčová slova

Kyberterorismus, počítačová kriminalita, informační válka, informační a komunikační technologie, rizika a hrozby, predikce kyberterorismu.

RNDr. Josef Požár, CSc., Policejní akademie ČR Praha, Lhotecká 559/7,
E-mail: pozar@polac.cz