Kybernetický terorizmus a počítačová kriminalita

Cyberterrorism and computer crime

Bc. Anna Bičianová

Diplomová práce
2008

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

ABSTRAKT

Táto práca pojednáva o počítačovej kriminalite, terorizme a ich prieniku do virtuálneho sveta - kyberpriestoru. V tejto tzv. „piatej dimenzii“ spolu s novou informačnou technológiou postupne vznikol nový fenomén kyberterorizmus, ktorý predstavuje jednu z najväčších pravdepodobných hrozieb celosvetovej bezpečnosti počas nadchádzajúceho desaťročia.

Kľúčové slová: kyberterorizmus, počítačová kriminalita, kybernetické útoky, informačná vojna

ABSTRACT

These thesis deals with the computer crime, terrorism and their penetration to virtual world – the cyber world. In so called „the fifth dimension“ also with a new information technology was born a new phenomenon cyber-terrorism and presents a significant threat to global security during the next decade.

Keywords: terrorism, cyber-terrorism, computer crime, cyber-attacks, infoware

Poďakovanie:

Ďakujem Ing. Radkovi Šilhavému za odborné, pedagogické vedenie a pripomienky, ktoré prispeli k dokončeniu tejto práce.

Prehlasujem, že som diplomovú prácu vypracovala samostatne a použitú literatúru som citovala. V prípade publikácie výsledkov, ak je to uvoľnené na základe licenčnej zmluvy, budem uvedená ako spoluautor.

V Zlíne 20. mája 2008 ……..….

Podpis diplomanta

OBSAH

ÚVOD

„Chcem, aby ľudia počuli moje potvrdenie, že počítač je nová mocná metafora, ktorá nám pomáha porozumieť mnohým aspektom sveta, ale že tiež zotročuje myseľ tých, ktorí iné metafory nemajú a nemajú ani iné zdroje, na ktoré by sa mohli odvolať“. Takto jasné stanovisko prednesené Josephom Weizenbaumom na jeho prednáške v Obecnom dome v máji 2002 úplne jasno odráža zmenu na jeho životné postoje. Premena spolutvorca prvých počítačov, autora učiacich sa počítačov, profesora informatiky na MIT a počítačového disidenta, ktorý sa hlboko zamýšľa nad úlohou technológií na tomto svete, odrážala i mimo iného i vojenského zneužívanie počítačových technológií.

Otázka vplyvu počítačových systémov a informatizácie spoločnosti spolu s fenoménom bezpečnosti systémov sa stáva veľmi populárnou témou. Konajú sa konferencie na téma bezpečnosti, publikujú sa najrôznejšie osvedčené postupy, ktoré zabezpečujú počítačovú a komunikačnú infraštruktúru pred napadnutím, doporučujú sa stále nové programy alebo zariadenia pre ochranu systémov. Existujú desiatky firiem, ktoré za presne špecifikovanú čiastku „dodajú bezpečnostné riešenie“ a na Internete kolujú stovky návodov ako obísť bezpečnostné opatrenia. Slovo bezpečnosť sa stalo módou a bezpečnostné riešenie produktom kalkulujúcim sa strachom z neznáma, podobne ako poisťovací agenti, presvedčujúci obyvateľov o nutnosti poistiť sa proti povodni.

S informačnými technológiami sa v dnešnej dobe stretávame na každom kroku. Ich prínos vo všetkých oblastiach výroby, obchodu, komunikácie či zábavy je neodmysliteľný. Bohužiaľ, prienik týchto technológií do všetkých oblastí bežného života so sebou prináša i svoje temné stránky. Jednou z nich je počítačová kriminalita, fenomén, ktorý sa s nástupom digitálneho veku jednoducho musel objaviť. Zvláštnosti tohto druhu kriminality vyplývajú už zo samej podstaty moderných informačných technológií. Zatiaľ čo v dobách minulých sa musel napríklad zločinec, ktorý si vytkol za cieľ vylúpiť banku, v banke skutočne objaviť a svoj čin tam fyzicky uskutočniť, väčšinou za použitia alebo aspoň pod vyhrážkou násilia, tento „fyzický“ substrát sa u počítačovej kriminalite často vytráca. Banky sú dnes vylúpené on-line, pričom páchateľ môže sedieť pred obrazovkou počítača tisícky kilometrov ďaleko a lup si previesť do banky, ktorá leží na opačnej strane zemegule a to všetko behom niekoľkých sekúnd. Z týchto odlišností vyplýva i potreba využitia úplne odlišných metód práce represívnych orgánov, ako tomu bolo doposiaľ u kriminality klasické. Prvým krokom je predovšetkým pochopenie podstaty moderných

informačných technológií a z nich vyplývajúcich odlišností počítačového zločinu. Porozumenie počítačovej kriminality tak kladie pomerne vysoké nároky na vyvážené znalosti z dvoch navzájom nepríbuzných oborov – práva a informatiky či výpočtovej techniky.

Kybernalita alebo kybernetická kriminalita má svoje miesto vo virtuálnom priestore dátových a komunikačných sieti. Štúdium kybernality zakladá nový interdisciplinárny obor zaoberajúci sa nelegálnymi a škodlivými aktivitami v počítačovom priestore, ktoré sú založené na použitie alebo zneužitie počítačovej technológie. Stala sa reálnou súčasťou každodenného života, kedy nás technológia posunula do novej dimenzie, do dimenzie kyberpriestoru. A či chceme alebo nechceme, budeme sa musieť v tejto „piatej dimenzii“ naučiť žiť.

I. TEORETICKÁ ČASŤ

1 VYMEDZENIE ZÁKLADNÝCH POJMOV

1.1 Kyberpriestor

Výpočtová technika a Internet so sebou preniesli významnú zmenu. Interaktivita, sa stala podstatou počítačovej komunikácie, úplná strata mimoverbálneho vnímania, možnosť vytvárania nesmrteľných virtuálnych jedincov, jednoduchosť prechodu medzi komunitami a potlačená potreba kompromisov viedli k vytvoreniu nového „kybernetického" sveta, ktorý sa pre mnohých stal znesiteľnejší a príjemnejší ako svet reálny. Tento kyberpriestor sa stal piatou dimenziou života spoločnosti so všetkými rysmi, ktoré dennodenné spoločenské aktivity prinášajú. A podobne ako náš reálny svet i kyberpriestor nadobudol všetkých spoločenských atribút – politických, obchodných, emocionálnych, kultových alebo náboženských.

Do kyberpriestoru sa prenášajú všetky rysy súčasnej spoločnosti, ale život v kyberpriestore si formuluje svoje vlastné pravidlá, ktoré sa často vymykajú prirodzenému poriadku, v ktorom ľudské spoločenstvo žilo po storočia. Ak chce táto spoločnosť v kyberpriestore prežiť, nezostáva jej nič iné, než staré pravidlá chovania prispôsobiť, nové vytvoriť a naučiť sa v tomto piatom rozmere života spoločnosti existovať. Tento spôsob existencie však prináša i určité nové alebo modifikované nebezpečne, nové alebo modifikované formy chovania, s ktorými sa musíme vysporiadať, naučiť sa ich akceptovať alebo nájsť spôsoby, ako im čeliť.

Štúdium kybernetickej kriminality – kybernality zahrňuje radu nových pohľadov na jedincov i spoločnosť, resp. na ich projekcie do kyberpriestoru. Je nutné si uvedomiť, že všetky doposiaľ známe nelegálne aktivity prebiehali vo fyzickom priestore, kde každý z aktérov boli ľahko opísateľní a postihnuteľní. Tak tomu nie je v kyberpriestore, kde sa stretávame iba s projekciami páchateľov, s ich virtuálnym obrazom, ktorý môže byť od skutočných rysov páchateľa na hony vzdialený. A s tým sa stávajú metódy vyšetrovania a chápania trestných činov iba ťažko vyrovnávajú. Súčasné chápanie „kybernetického" trestného činu, ktorému chýbajú klasické atribúty, sa zatiaľ veľmi opatrne formuje. Štandardizované metódy policajného vyšetrovania zlyhávajú pri „naháňaní duchov" v kyberpriestore, justícia tápa vo formuláciách trestného zákona.

Štúdium kybernality vychádza z chápania a popisov technológii a možností, ktoré tieto technológie dávajú človeku. I keď v prvom priblížení je to hlavne informatika a

telekomunikácie, ktoré sú základnými technológiami pri vytvorení kyberpriestoru, môžeme nájsť niektoré špecifické vedy, ktoré tento proces významne ovplyvňujú. Do štádia kybernality však zasahujú významne i spoločenské vedy, hlavne sociológia, psychológia a právna veda.

1.1 Terorizmus

Terorizmus je definovaný ako súhrn antihumánnych metód hrubého zastrašovania politických odporcov hrozbou sily a užitia rôznych foriem násilia. Vedľa individuálneho terorizmu existuje terorizmus skupín, niektoré koordinujú svoju činnosť na medzinárodnej úrovni (medzinárodný terorizmus). Kľúčovým faktorom je vyvolávanie strachu a paniky a upútanie pozornosti za pomoci násilia.

K teroristickým akciám dochádza z rady rôznych podnetov. Väčšinou chcú teroristické organizácie na seba upozorniť, pretože teroristickým útokom je zviditeľnená ich ideológia, a hrdo sa k svojim útokom hlásia. Inokedy, v snahe o minimalizáciu rizika, volia stratégiu anonymity. Faktorom ovplyvňujúci toto chovanie a celý proces výberu cieľu teroristických akcií, sú prvotné dôvody terorizmus, kam patrí:

1. podľa **ideologickej príslušnosti**
    - **nacionalistický**
    - **revolučný**
    - **extrémizmus krajnej pravice**
    - **náboženský extrémizmus**
    - **jednoúčelové teroristické skupiny**
2. podľa **povahy cieľov**, ktoré chcú teroristi dosiahnuť – do istej miery sa prekrývajú s ideológiou hnutia
    - **štátom podporovaný terorizmus**
    - **protištátny terorizmus**
3. podľa **výberu cieľov**

- **útoky na veľmi špecificky vybrané ciele**
- **útoky na náhodne zvolený cieľ**

4. podľa **oblasti pôsobenia**
   - **mestský**
   - **vidiecky**,
5. podľa **zamerania násilia** - termín zamerania predstavuje v tomto prípade výber cieľov a prostredia, v ktorom teroristi operujú
   - **vnútroštátny**
   - **medzinárodný**
6. podľa **historického pôvodu** teroristickej skupiny

Ukázalo sa, že ani jeden systém kategorizácie nie je komplexný, preto sa tvorcovia antiteroristickej politiky snažia vytvárať nové rozdelenia, ktoré by pokryli celú možnú významovú šírku konkrétneho hnutia. Autori sa vo vymedzení pojmu terorizmus veľmi rôznia. Zhodne sa však väčšina autorov vyhýba poňatiu, že terorizmus je osobná záležitosť jednotlivca. Skôr sa zaoberajú analýzou politických programov a podpory od štátnych alebo miestnych inštitúcií a spoločnosti ako takej. Veľa vecí naznačuje, že teroristi nechcú, aby po ich činoch bolo veľa obetí, pretože by tým mohli prísť o širšiu podporu verejnosti, a o tu im ide predovšetkým. Cieľom teroristov teda nie je vysoký počet obetí, ale vzbudiť vo verejnosti pocit strachu, alebo zažehnať vzburu. Posledné teroristické útoky však majú cieľ trocha odlišný - usmrtiť čo najviac obetí a v konečnom dôsledku vyvolať pocit strachu.

Významnú úlohu tu hrajú, predovšetkým v posledných rokoch, aj všetky druhy médií, pretože venujú týmto správam značnú pozornosť, často so snahou urobiť z vlastného aktu terorizmu senzáciu, čím vlastne istým spôsobom teroristické požiadavky alebo dokonca aj program zverejňujú.

1.2.1 Ciele terorizmu

K teroristickým akciám môže dochádzať z rôznych dôvodov. Všeobecne existuje niekoľko hlavných cieľov terorizmu:

- **Reklamný cieľ** – ide o upútanie pozornosti pomocou masmédií. Násilnou akciou je prejavená snaha o zverejnenie programu teroristickej organizácie. Tomu významnou mierou napomáhajú aj dnešné svetové mediálne prostriedky, ktoré vyhľadávajú takéto drastické exkluzívne správy.
- **Jednorazový násilný akt** – ide o dosiahnutie cieľov ako je likvidácia osoby alebo osôb, ničenie konkrétneho objektu alebo objektov. Pri snahe vynútiť si vyjednávanie, slúžia teroristické akcie na zastrašovanie politickej moci alebo ako nátlak na politickú moc. Pri tomto taktickom použití násilia sa obeťami útokov stávajú často nevinní ľudia, ktorí nemajú nič spoločné s prípravou alebo výkonom vládnej politiky.
- **Strategický cieľ** – terorizmus predstavuje destabilizačný nástroj daného režimu. Vychádza z predpokladu, že teroristické akcie vyprovokujú štátnu moc k takým represiám a násiliu, ktorého výsledkom má byť revolučná vzbura. Toto predpokladajú predovšetkým anarchistické doktrinálne koncepcie.

***Obr.1**: Príklad teroristického grafitu*

V množstve prejavov terorizmu sa pri ich analýze vymedzujú typy, druhy a formy terorizmu. Ide o záležitosť, ktorá sa vzhľadom na meniaci sa charakter terorizmu kontinuálne dopracováva najmä v spojitosti s jeho aktuálnymi príčinami, zdrojmi a prejavmi. Skupiny uskutočňujúce samovražedné atentáty sa odlišujú svojou formou, veľkosťou, ideovou orientáciou, cieľmi a podporou.

Terorizmus, ktorý sa stal novou hrozbou, zmenil charakter 20. marca 1995. Vtedy po prvý raz teroristi použili chemické bojové látky proti civilnému obyvateľstvu. V tokijskom metre bola vypustená nervová látka sarin. V dôsledku tohto činu muselo viac ako 550 ľudí vyhľadať lekársku pomoc. Momentálne je na svete mnoho skupín aktívnych v tomto spôsobe útokov, prakticky každá teroristická skupina však má možnosť spáchať samovražedný teroristický útok.

1.2 Kyberterorizmus

Kyberterorizmus je konvergencia terorizmu a kyberpriestoru. Je obecne chápaný ako nezákonný útok alebo nebezpečný útok proti počítačom, počítačovým sieťam a informáciám v nich skladovaným v prípade, že útok je uskutočňovaný za účelom zastrašiť alebo donútiť vládu, alebo obyvateľov k podporovaniu sociálnych alebo politických cieľov. V tomto zmysle sú za akty kyberterorizmu považované útoky proti kritickej infraštruktúre a útoky, ktoré nenarúšajú nekľúčové služby obvykle pokladané za akty kyberterorizmu nie sú. Dôležitým faktom, ktorý sprevádza teroristické aktivity v kyberpriestore je psychologický moment napadnutia protivníkovej siete akýmkoľvek spôsobom. Tento efekt dostatočne znásobený hrozbami a inými metódami psychologickej vojny, môže byť postačujúci k tomu, aby vo vnútri protistrany vyvolal takú mieru strachu, ktorý sekundárne povedie k významným fyzickým, ekonomickým alebo iným škodám značného rozsahu. A práve na tento sekundárny efekt mnohé teroristické skupiny vsádzajú.

Kyberterorizmus patrí medzi najväčšie nebezpečia 21. storočia. Princípom kyberterorizmu je zneužívanie výpočtovej a telekomunikačnej techniky vrátane Internetu ako prostriedku a prostredia pre uskutočnenie teroristického útoku. Jedná sa o podobne ako u klasického konvenčného teroristického útoku o plánovanú činnosť, spravidla motivovanú politicky či

náboženský a realizovanú skôr malými skupinami než vojensky organizovanými štruktúrami[1]. Cieľom týchto skupín je predovšetkým ovplyvnenie verejného mienenia či politických elít, čím sa odlišujú od hackerstva. Vzhľadom k rýchlemu šíreniu komunikačných a telekomunikačných systémov po celom svete, predstavuje kyberterorizmus významné nebezpečie a je teroristickými skupinami využívaný v stále rastúcej miere.

1.3 Počítačová kriminalita

Snaha maximálneho využitia informačných technológií má i svoje negatívne stránky. Akonáhle sa objaví nový vynález, nájdu sa ľudia, ktorí ho využijú k páchaniu trestnej činnosti. Tak sa objavila i počítačová kriminalita, predstavujúca nový druh trestné činnosti. S ňou sa musí dnes počítať všade tam, kde narastá využívanie výpočtových technológií a rozvíja sa informačný priemysel.

Počítačová kriminalita je výrazným javom dnešnej doby, ale záujem o informácie, ktoré boli spracované, prenášané a uchovávané iným spôsobom, je oveľa staršieho dáta. Len sme boli zvyknutí, a stále tak to i chápeme, tieto javy nazývať inými pojmami (vyzvedanie, vyzradzovanie atd.), hlavne podľa spôsobu uplatnenia informácii. S postupne stále sa rozširujúcim zavadzaním výpočtovej techniky rastie a rástla miera ich zneužívania a do istej miery zatieňuje klasické formy práce s informáciami a ich zneužívanie.

Pokiaľ prevažovalo štátne alebo iné kolektívne vlastníctvo, o ochranou informácií sa zaoberal prevažne štátny aparát. Po zmene vlastníckych pomerov, kedy dnes prevažuje súkromné vlastníctvo a zároveň informácie sa stali skôr tovarom, teda predajným i kúpyschopným artiklom, je ich ochrana oveľa významnejšia. Teda i ich zneužitie má relatívne hlbší dopad, aspoň pokiaľ sa vlastníka týka.

Počítačová kriminalita má radu výrazných charakteristík, ktoré ju odlišujú od kriminality klasickej. Vo väčšine prípadov počítačové kriminality sa neobjavujú prvky, ako je násilie,

[1] Existuje viac ako štyridsať krajín disponujúcich arzenálom pre vedenia informatického boja, ktorý môže byť použitý. A je možné, že tieto prostriedky sú k dispozícií i štátom podporujúcich terorizmus, ktorými môžu byť použité vo „vojenskom rozmere“.

použitie zbrane, ujma na zdraví osôb apod. U klasickej kriminality sa meria doba spáchania trestného činu na minúty, hodiny, dni, trestný čin v oblasti počítačovej kriminality môže byť spáchaný v niekoľkých tisícinách sekundy a páchateľ ani nemusí byť priamo na mieste činu.

Ďalšou významnou charakteristikou pre počítačovú kriminalitu sú v dôsledku značnej straty, či už priamo v podobe finančných čiastok, alebo v podobe zneužitia získaných údajov. Počítačovú kriminalitu sprevádza určitá diskrétnosť trestnej činnosti. Z uvedeného vyplýva, prečo počítačová kriminalita býva, pre svoju povahu, označovaná ako kriminalita "bielych limčekov".

Počítačová kriminalita môže postihnúť značnú časť osobného i spoločenského života. Výpočtová technika je nasadená do riadenia a správy štátu, v armáde, polícii, ekonomike, priemysle i hospodárstve, v zdravotníctve a inde. V počítačových systémoch jednotlivých inštitúcií sa sústreďujú informácie zo všetkých oblastí života spoločnosti i jednotlivca. Preto poškodenie funkcie počítačových systémov, nielen celoštátne budovaných, ale i lokálnych, môže viesť k dezorganizácii v mnohých sférach ľudskej činnosti.

Aby bolo možno hovoriť o počítačovej kriminalite, musí páchateľ k svojmu jednaniu užiť nielen výpočtovú techniku, ale jeho jednanie musí tiež naplňovať znaky skutkovej podstaty niektorého trestného činu uvedeného v trestnom zákone a nebezpečnosť takého jednania musí dosahovať požadovaného stupňa nebezpečnosti pre spoločnosť.

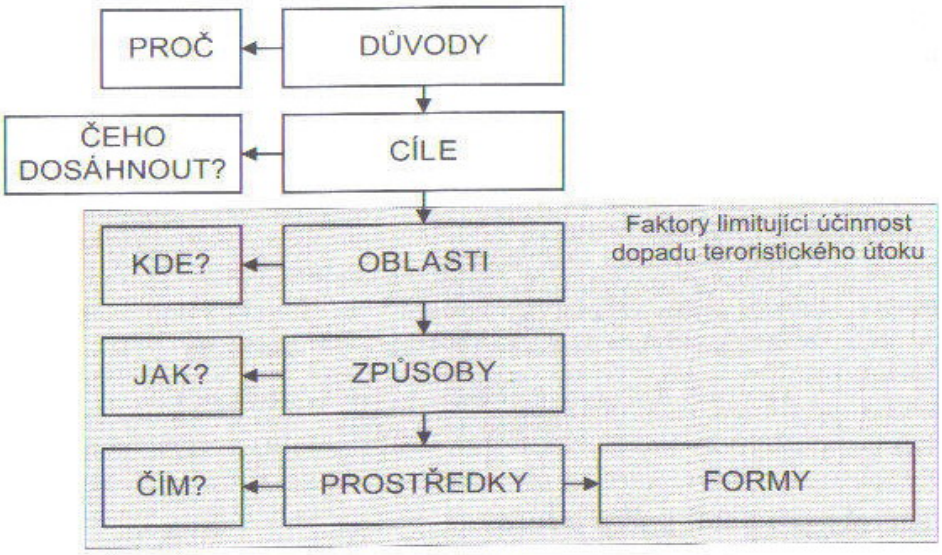
2 VZNIK A HISTÓRIA KYBERNETICKÉHO TERORIZMU

Pojem kyberterorizmus sa stal v poslednej dobe veľmi frekventovaným pojmom, no nebol doposiaľ presne definovaný. Po prvý krát bol použitý v deväťdesiatych rokoch minulého storočia Barrym Collinom, pracovníka Institute for Security and Inteligence v Kalifornii. Ten v roku 1996 popísal niekoľko scenárov, ktoré svojou povahou odpovedali kyberteroristickému útoku, a tak otvoril pole pre skúmanie možností kyberteroristov a dopadov ich aktivít.

Samotný terorizmus nie je nový. Avšak jeho dnešný charakter a globálne rozšírenie, vytvorenie zložitých sietí a vlastné aktivity, čo do sily, cieľov, koordinovanosti a napokon „úspechov“, sú nevídané. Terorizmus sa stal za posledných pätnásť rokov pod vplyvom nových trendov a udalostí frekventovanejším, ale i diferencovanejší. Je to i preto, že v časoch studenej vojny bola značná časť teroristických skupín, pokiaľ im bolo vôbec umožnené operovať, viac-menej pod kontrolou jedného alebo druhého z blokov a konali s jeho vedomím, sponzorstvom, zbraňami a niekedy i priamo z jeho podnetu a s asistenciou jeho tajných zložiek. S tým súvisela aj interpretácia takýchto akcií, ako národnooslobodzovacieho, či antiimperiálneho alebo antikomunistického boja. Po rozpade ZSSR, po skončení patronátu Moskvy, mnohé teroristické skupiny zanikli. Avšak mnohé nie, pričom niekoľko ich aj vzniklo. Teroristické skupiny síce stratili finančnú podporu, získali však voľnosť. Podobne aj mnohé diktátorské režimy, pred rozkladom sovietskeho moci ovládané či sponzorované z Moskvy, prestali po roku 1989 dostávať inštrukcie „stratili okovy“, a buď skolabovali a boli nahradené lepšími, resp. horšíme, alebo si našli novú legitimitu, smerovanie a ciele.

2.1 Terorizmus a jeho projekcia do kyberpriestoru

Terorizmus predstavuje jednu z foriem globálnych hrozieb. Je možné sledovať jeho nárast a rozširovanie do podstatnej časti sveta. Historické materiály dokladajú, že terorizmus bol vždy uskutočňovaný s konkrétnym cieľom a z počiatku boli teroristické akcie motivované skôr ideologicky. Postupom času táto motivácia prešla do náboženskej a nacionalistickej roviny, ktorá sa hlavne v poslednej dobe výrazne upevnila. Každý teroristický čin je sústredený na tri základné faktory: oblasť, spôsob a prostriedky realizácie (vid. Obr.2). Pri ich optimálnej kombinácii sú následky teroristického útoku ničivé.



Obr. 2.: *Schéma proces realizácie teroristických akcií*

Terorizmus môžeme rozdeliť podľa formy na letálne a neletálne formy terorizmu, kde prvá skupina sa vyznačuje použitím bežných prostriedkov pre realizáciu násilia. Letálny terorizmus môže byť ďalej členený na dve podskupiny, líšiace sa použitými prostriedkami, na konvenčný a nekonvenčný terorizmus. Do podskupiny konvenčných foriem letálneho terorizmu sa zaraďujú útoky páchané pomocou bežne dostupných bojových prostriedkov, napr. strelných zbraní. Medzi nekonvenčné formy letálneho terorizmu radíme zneužite zbraní hromadného ničenia.

Nekonvenčná forma neletálneho terorizmu zahrňuje, podobne ako u letálnych foriem, nekonvenčné zbrane, medzi ktoré možno zaradiť zbrane využívajúce princípy akustiky, optiky a elektromagnetického pulzu. Hlavným efektom pri ich použití je vyradenie protivníka alebo jeho elektronických systémov na určitú dobu z boja, a ta bez priameho ohrozenia života. Súčasťou použitia nekonvenčných zbraní je i vyvolanie psychického účinku a jeho využitie. Je zrejmé, že dopad na infraštruktúru protivníka, a tým i na životne dôležité funkcie štátu, napr. bankovníctvo, zásobovanie obyvateľstva a podobne.

Kybernetický terorizmus zlučuje prvky kybernetické vojny (či tzv. počítačovej vojny) a psychologickej vojny. Behom niekoľko posledných desiatok rokov prešla globálna spoločnosť výraznými technologickými zmenami v oblasti predávania a spracovávania informácií a veľká časť informačných aktivít prebieha elektronicky. V niektorých prípadoch tieto aktivity nie sú paralelne kryté iným spôsobom predávania a spracovávania informáciií. Úmerne tomu, ako veľký vplyv majú čisto elektronicky vyvíjané informačné

aktivity na činnosť rozhodujúcich/kontrolných centier v politickej, sociálnej, vojenskej, ekonomické oblasti, sú tieto centrá zraniteľné útoky smerujúcimi proti elektronickým cieľom.

Pre názornosť uvádzam Tabuľku 2, ktorá vyjadruje súvislosti hrozieb, prostriedkov a cieľov teroristického násilia[2].

Hrozby (threats)	**Prostriedky (means)**	**Ciele (targets)**	**Konečné ciele (ends)**
teroristické organizácie	vraždy	štátne organizácie	asymetrický konflikt
anonymní teroristické organizácie	kybernetický útok	bankovníctvo a financie, kritická infraštruktúra	bezpečnostná výhoda
pracovníci informačnej vojny	informační operácie	obchod	ekonomická výhoda
štátny terorizmus	infoware	obyvateľstvo, vlády	politická zmena
počítačoví hackeri	logické bomby	kritická infraštruktúra	politický vplyv a zisk
počítačoví hackeri	kybernetický útok	firmy, financie	finanční zisk
štátom sponzorovaný terorizmus	priama akcia	kritická infraštruktúra	politická zmena

Tab. 1: *Vzťahy hrozieb prostriedkov a ciele terorizmu*

[2] Skopal, P.: Kyberterorismus jako reálná hrozba současnosti?. Dostupné z WWW: <http://www.pauza.cz/r-art.asp/id=166>.

2.2 Taxonómia útočníkov podľa geopolitického hľadiska

Základné delenie, ktoré nám umožní istú klasifikáciu pôsobenia kyberteroristických skupín môže byť geopolitické hľadisko. V tomto zmysle možno potenciálnych útočníkov rozdeliť do niekoľkých skupín: teroristi, nepriateľské národné štáty, sympatizanti teroristov alebo iní odporcovia nejakej politiky a náhodní hackary bez politickej motivácie, ktorí iba vyhľadávajú vzrušenie a uznanie vo svojej komunite.

2.2.1 Teroristické skupiny

Nie je známe, či teroristická skupina Al-Kajdá alebo iné teroristické skupiny už vyvinuli kybernetické zbrane, ani ako sú ich schopnosti v tejto oblasti veľké. Naproti tomu je isté, že teroristické skupiny používajú informačné technológie a internet k plánovaniu svojich akcií, získavania peňažných prostriedkov, šírenia propagandy a svojich vyhrážok.

Odsúdený terorista, Ramzi Yousef, ktorý bol zodpovedný za plánovanie prvého útoku na World Trade Center v roku 1993, mal vo svojom laptopu v zašifrovaných súboroch uložené plány ďalších teroristických útokov na 12 dopravných lietadiel v Pacifiku. Neskorší útok na WTC a Pentagon 11. Septembra 2001, rovnako ako odhalenie britských bezpečnostných síl, že IRA mala v pláne zničiť elektrárne v okolí Londýna, dokazujú túžbu teroristov uderiť na kritické centrá infraštruktúry, na ktorých moderná informačná spoločnosť závisí. Útoky na WTC si nevyžiadali iba straty na životoch a majetku, ale tiež uzatvorili burzy a zničili dôležitú súčasť finančnej infraštruktúry New York City. Tento trend môže byť varovným signálom pred hrozbou zneužitia informačných technológií ako zbrane proti kľúčovým centrám infraštruktúry západnej spoločnosti.

2.2.2 Nepriateľské národné štáty

Niektoré krajiny, hlavne tie označované Spojenými štátmi za „osu zla“, by sa mohli v budúcnosti stať terčom amerických vojenských operácií. O mnohých týchto štátoch je známe, že vyvíjajú kybernetické prostriedky pre špionáž proti ostatným štátom, priemyslom, finančnej sfére. Tiež sa hovorí o možnom použití informatických zbraniach

proti USA a spojencom. Americký Defense Science Board[3] odhaduje, že v budúcnosti na Spojené štáty zaútočí pripravený protivník využívajúci široké spektrum kybernetických zbraní a techník. Medzi potenciálnych protivníkov patria hlavne Čína, Severná Kórea, Kuba a Rusko, o ktorých je známe, že takéto technológie vyvíjajú.

Informatický zbrojný potenciál je veľmi obľúbený, pretože asymetrické vojnové stratégie sú jednou z mála možností, ako súperiť s nepriateľom, ktorý má totálnu prevahu vojenskej i ekonomickej sily. Krajiny s rozvinutými kybernetickými zbraňami by určite infoware použili v prípade napadnutia zo strany koalície vedenej USA. Naviac existuje možnosť, že i štáty, ktoré by neboli priamo zapojené do odvetných akcií voči USA, by mohli spustiť útok kybernetickými zbraňami vydávajúc sa pri tom na nejakú teroristickú krajinu, pretože pôvodca teroristického útoku môže za sebou zametať stopy a zanechávať falošné vodítka.

2.2.3 Sympatizanti teroristov a protiamerickí hackeri

Z historických trendov vyplýva, že kybernetické útoky sympatizantov teroristických skupín a ľudí s protiamerickým poprípade iným „proti“ zaujatím budú častejšia ako útoky teroristov či nepriateľských štátov. Pokiaľ bude blízky východ chápať americkú kampaň boja proti terorizmu ako krížovú výpravu proti islamu, môže tu vzniknúť celá nová generácia kyberteroristom. V tomto prípade by mohli „premoslimské“ hackerové skupiny ako G-Force, The Pakistan Hackerz Club alebo Doctor Nuke využiť svojej schopnosti proti Spojeným štátom a ich spojencom a zároveň vychovať skúsených nasledovníkov.

Existujú tiež reálne hrozby, že by sa skupiny s akýmkoľvek zaujatím proti USA mohli spojiť a vytvoriť širokú nepriateľskú koalíciu zahrňujúcu náboženských fanatikov, extrémistické skupiny, odporcov americkej podpory Izreala, extrémistické skupiny a čínskych hackerov. Antikapitalistické a antiglobalizačné hnutie v minulých rokoch už využilo násilnú taktiku, aby ukázalo svoj odpor voči hodnotám definujúcim globálny status quo. Po teroristických útokoch 11. Septembra ich dokonca niektorí z nich prehlasovali za spravodlivú odvetu americkému imperializmu. Títo extrémisti a i umiernení odporcovia ich hnutia by sa mohli zapojiť do kybernetickej kampane proti USA a ich spojencom. Do

[3] DSB je komisia civilných expertov ustanovených pre radu Ministerstva obrany USA pre vedecké a technické záležitosti.

tejto informačnej vojny by mohli prispieť i čínski haceri, ktorí cítia, že majú s USA nevyrovnané účty. Naviac sú niektorí Číňania stále rozhorčení neúmyselným bombardovaním čínskej ambasády v Belehrade v roku 2000.

2.2.4 Vyhľadávači vzrušenia (thrill seekers)

Akýkoľvek konflikt odohrávajúci sa v kyberpriestore priťahuje obrovské množstvo hackerov. Táto kategória útočníkov nie je vedená ani politickým ani ideologickým zápalom, ale iba exhibicionalistickou túhou. I keď sa jedná o pomerne veľkú skupinu, ktorá využíva vzniknutý kyberkonflikt, jej aktivity sú relatívne malou hrozbou pre počítačové systémy západných krajín. Úroveň prepracovanosti ich útokov je v porovnaní s inými účastníkmi konfliktu väčšinou veľmi nízka, pretože používajú hlavne prefabrikovane hackerové nástroje. Taktiež ich motivácia nie je tak vysoká a v prípade, že sa konflikt predlžuje, strácajú záujem. Naproti tomu, pravdepodobnosť útoku zo strany týchto skupín je extrémne vysoká vďaka mediálnej sledovanosti situácie, čo zvyšuje možnosť „preslávit“ sa.

I keď tejto kategórií útočníkov nebola prisúdená vysoká nebezpečnosť, zostáva tu stále možnosť, že vďaka nim bude odstavený z prevádzky nejaký kritický systém.

3 FORMY KYBERTERORIZMU

Významným aspektom kybernetického útoku je jeho asymetria, kedy niekoľko málo špecialistov môže s relatívne malými nákladmi poškodiť hospodárstvo technicky vyspelého štátu natoľko, že si jeho obnova vyžiadať roky. Skutočnosť, že kybernetický útok môže zasiahnuť súčasne na rade miest sveta naraz, prírodné prekážky a vzdialenosť tu nehrajú úlohu, a zapríčiniť tak ďalekosiahle dopady na reálny svet, činí scenár kybernetického útoku príťažlivý nielen pre „zločinecké štáty“ či teroristické skupiny, ale i pre osamote jednajúcich vydieračov. Previazanosť modernej spoločnosti na informačné systém je tak vysoká, že bez ochrany kyberpriestoru strácajú efekt ostatné bezpečnostné stratégie. Je treba podotknúť, že stále rastúca prepojenosť sveta a vzájomná závislosť všetkých zložiek modernej civilizácie, významne obmedzuje možnosť kybernetických útokov, iniciovaných štátmi. I tzv. „zločinecké štáty“ sú do tej miery zapojené do globálnych počítačových sietí, že kolaps svetových finančných trhov, ktorý by masový kybernetický útok mohol spôsobiť, by negatívne dopadol i na nich. To však nemusí odradiť neštátnych aktérov, ako sú nadnárodné teroristické skupiny. Im môžu byť výkyvy svetovej ekonomiky ľahostajné, resp. s nimi môžu počítať vo svojich plánoch.

Medzi metódy používané kyberteroristami patrí:

- **Fyzické napadnutie**, teda neautorizovaný fyzický prístup do priestoru vyhradených pre prevádzkové zložky technológie alebo ich časti. Cieľom útoku môže byť napríklad umiestnenie odpočúvacieho alebo podobného zariadenia priamo v mieste koncentrácie technológie, kopírovanie dát priamo z nosičov alebo fotografovanie obsahu displeja. Nie je vylúčená ani fyzická deštrukcia zariadenia alebo jeho odcudzenia.
- **Spúšťanie útokov typu DoS alebo DoA** či rozšírením maligného kódu (víry, červy), kedy väčšinou nejde o preniknutie do cieľového systému, ale útok ma skôr slúžiť k degradácií jeho činnosti a znemožnenie jeho riadneho používania.
- **Defacement webových stránok alebo iný sémantický útok** – útoky tohto typu sú najnebezpečnejšie v prípade, kedy podvrhnutá stránka má rovnaký alebo skoro rovnaký vzhľad ako pôvodná stránka. Takýto útok je obvykle určený k získaniu dôverných údajov ako sú prihlasovacie údaje, čísla a piny kreditných kariet, zdravotných informácií a pod.

- **Útoky na kľúčové uzly internetu.** Hlavne sa jedná o útoky doménové servery DNS. Preklad mien na potvrdenej adresy a tým zmenené miesta určenie správ nielen, že spôsobia chaos v celej príslušnej doméne, ale môže slúžiť i k získaniu dátových tokov od sieťových uzlov, ktoré by boli inak nedosiahnuteľné.
- **Útoky na slabiny smerovacích protokolov**, ktoré môžu slúžiť k odkloneniu dátových tokov od cieľových uzlov alebo i ich duplikácií a odklonu. Typickým cieľom takéhoto útoku je odpočúvanie prenášaných správ alebo potvrdenie či zmena správy.

3.1 Nástroje kybernetických útokov

Nie každý jednotlivec alebo skupina, ktorá používajú informačné technológie k šíreniu svojho programu alebo k útoku na svojich protivníkov sú nevyhnutne kyberteroristi. Je zložité určiť, či vzniknutý útok je od teroristu alebo študenta s technickou znalosťou prístupu do systému. Často býva otázne, čo je skutočne kyberterorizmus a čo je iba hacking. Existuje množstvo nástrojov, ktoré kyberteroristi môžu používať k dosiahnutiu svojho cieľa. Niektoré z nich sú uvedené v nasledujúcej časti.

3.1.1 Backdoors

Backdoors alebo zadné vrátka sú veľmi výstižným názvom pre kódy, ktoré po inštalácii na cieľový počítač umožňujú jeho vzdialené riadenie. Jedná sa o obľúbený hackerský nastroj a akonáhle hacker objaví bezpečnostnú dieru, jeho prvým krokom je nainštalovanie backdoors. Typický hacker má vždy v zálohe niekoľko počítačov s tajne nainštalovaným nástrojom pre vzdialené riadenie a čím je lepší, tým viac strojov má k dispozícií. Tieto, tzv. kompromitované stroje sú potom používané k podnikaniu ďalších útokov na cieľový stroj. Často tento reťazec medzi útočníkom a cieľovým strojom môže mať i desať alebo viac skompromitovaných strojov, ktoré izolujú a chránia pôvodného útočníka pred odhalením.

Kvalitný backdoor možno ťažko zistiť, zvlášť ak nie je často používaný, a hackerovi poskytuje úplnú kontrolu nad kompromitovaným strojom. Komunikácia medzi nástrojom vo vnútri kompromitovaného počítača a hackerom sa uskutočňuje pomocou nástrojom spustenej služby na portu s vysokým číslom alebo je maskovaná ako štandardná služba ako napr. http (webový prístup, Port 80) alebo telnet (terminálový prístup, port 23). Tieto nainštalované služby väčšinou nie sú odfiltrované firewally, a tak sú prístupné i cez bezpečnostné prvky siete.

Moderný backdoors majú zdokonalenú komunikáciu a využívajú väčšinou protokolov niektorých interaktívnych nástrojov komunikácie ako je IRC, obľúbené ICQ alebo MSN messenger. To umožňuje lepšie ukrytie komunikácie a istý komunikačný komfort.

3.1.2 Skenery

Slúžia pre zistenie otvorených portov počítača, a teda i služieb, ktoré na ňom bežia. Skener tak útočníkovi veľmi rýchlo zistí základné informácie o cieľovom počítači a môže slúžiť i k získaniu informácií o operačnom systéme. Sken otvorených portov môže byť predzvesťou potencionálneho útoku, a preto systémy sa snažia tieto tzv. podskeny detekovať a spojenie s možným útočníkom na nejakú dobu prerušiť alebo učiniť iné bezpečnostné opatrenia.

Problém skenovania spočíva v rôznych implementáciách sieťového protokolu, resp. ich štandardov. Tieto odchýlky v implementácií na jednej strane môžu skenovanie značne komplikovať a dávať falošné výsledky, na druhej strane umožňujú nenápadnú detekciu systémov podľa odchyliek v detailoch implementácie štandardov. Okrem detekcie otvorených portov umožňujú skenery i identifikáciu služby, ktorá iba beží na príslušnom porte.

3.1.3 Sniffery

Slovo „sniff“ znamená v angličtine „čuchať“ a názov „sniffer“ je teda priliehavou voľbou pre program odpočúvajúci sieťový prevoz. Nejedná sa priamo o nástroj útoku, skôr o prostriedok k zhromaždeniu informácií potrebných pre prípravu útoku. Rozhodujúce pre získanie správnych informácií je umiestnenie snifferu v sieti. Hlavne v prepínaných sieťach, kde je spoločný segment minimalizovaný, je použitie snifferu problematické, pretože väčšina informácií je mimo sniffer.

Práca snifferu je jednoduchá, prepne sieťové rozhranie do tzv. promiskuitného módu, a tak prijíma všetky pakety, ktoré sa na sieti pohybujú bez akejkoľvek ďalšej filtrácie. Tieto pakety sú zaznamenané a ďalej analyzované – typ protokolu, IP adresy, MAC adresy, nastavenie príznaku a pod. Súčasťou analýzy je vydelenie dátovej časti s obsahom prenášanej správy. Tak je možné odpočúvať komunikáciu v sieti, zachytiť otvorene prenášané heslá alebo iné citlivé údaje.

3.1.4 Rootkity

Jedná sa o súbor techník pre skrývanie činností uskutočňovaných na operačnom systéme. Samotný názov „rootkit“ je zavádzajúci a vychádza z prostredia, v ktorom rootkity vznikli – z unixových operačných systémov a vychádza s pomenovania účtu superužívateľa alebo administrátora unixového systému. Ide o podmnožinu back doors a ich funkcia je veľmi podobná. Avšak na rozdiel od backdoors, ktoré na unix-like systéme budú pravdepodobne skoro odhalené, rootkit zostáva po kompromitácií účtu superužívateľa stále v utajení. V praxi ide o bežne používané programy ako ps, top, inetd, ktoré sú modifikované tak, aby administrátor nič nepoznal a hacker mal k stroju neobmedzený prístup.

3.1.5 Debuggery

Nástroje používané bežne pri ladení nového programu, sú neodmysliteľnou pomôckou každého hackera. V okamžiku, kedy sa podarí odhaliť nejakú bezpečnostnú dieru, nastupuje analýza kódu a overovanie funkcie exploitu, ktorý bude zistenú bezpečnostnú slabinu využívať. Postup je obvykle taký, že útočník sa snaží vložiť svoj kúsok do miesta využiť. Obvykle sa ukladá iba skok na adresu, kde bude uložený výkonný kód exploitu a zbytok sa doplňuje nevýkonnými inštrukciami, napr. NOP (no operation). Pri napadnutiu sa uskutoční skon na útočníkov kód, ten sa vykoná a opäť sa skočí späť do pôvodného kódu.

Debugger umožní overenie správnej funkcie kódu, ale i nájdenie najvhodnejšieho miesta pre uloženie odskoku a výkonného kódu útočníka. Toho je možné využiť pri odhaľovaní časti kódu pre kontrolu platnej licencie k programu. V tomto prípade útočník zisťuje, kde sa ukrýva podprogram, kontrolujúci či pridelené číslo licencie odpovedá správnemu číslu, a teda či program je prevádzkovaný jeho pôvodným vlastníkom. Crackeri používajú debugger k nájdeniu tohto podprogramu a jeho následné odstránenie, čím zbavia program jeho ochranných prvkov.

3.1.6 Nástroje DoS

Skratka DoS znamená „Dential of Service“ alebo potlačenie služby[4]. Myšlienka tohto útoku je jednoduchá – pokiaľ nemôžem zaútočiť priamo na cieľový stroj, zaútočím na jeho spojovacie cesty. Existuje niekoľko základných metód DoS:

- Zahltenie odosielaním jalového paketu z viacerých strojov (tzv. DDoS – Distributed Dential of Service).
- Zahltenie príkazom ping do siete cieľového stroja.
- Zahltenie voľných systémových prostriedkov.

3.1.7 Trojské kone

Trojské kone patria k najobľúbenejším hackerským nástrojom súčasnosti. Jedná sa o malé programy, ktoré sú zabalené do voľne stiahnuteľného kódu utility alebo do nevej bezplatne poskytovanej hry. Trojské kone sa používajú na najrôznejšie účely, od monitorovania činnosti cieľového počítača až po zneužitie pre útok DoS. Zaujímavá varianta trojských koní je dolovanie dát alebo „Data Mining“. Ide o programy, ktoré po nainštalovaní monitorujú činnosť užívateľa.

3.2 Aktivity teroristov voči informačným technológiám

Pri pokuse o kategorizáciu možných útokov proti informačným technológiám protistrany dôjdeme k nasledujúcim trom základným skupinám:

- **Priamy útok na lokálne technológie** – druh útoku je závislý na povahe lokality a na významu umiestnenej technológie v celkovom rozmere cieľovej infraštruktúry. Ak zanedbáme klasický fyzický útok, potom najjednoduchším prípadom môže byť sémantický útok, kedy defacement webových stránok sa obmedzí na zmenu ich obsahu. Útoky na infraštruktúru kritických systémov môžu vo svojom konečnom dopade viesť nielen k značným ekonomickým škodám, ale i k stratám na životoch.

[4] Dostupné z WWW:. <http:// www.infoware.sk/buxus_dev/generate_page.php?page_id=53320>.

- **Súbežný útok** – v rámci fyzického útoku nemierenom proti inému cieli je zasiahnutá i informatická alebo telekomunikačná infraštruktúra. Takýto prípad väčšinou vedie iba k degradácií prevádzkových parametrov zasiahnutej komunikačnej infraštruktúry a nemusí mať nutne fatálne následky. Ďaleko významnejšia je strata dát, ku ktorej dôjde pri fyzickom zničení nosičov informácie, alebo zničenie prevádzkovej technológie.
- **Zneužitie technológie k riadeniu teroristickej organizácie** – hlavne globálny charakter informatického a telekomunikačného prostredia umožňuje predávanie informácií a kooridináciu teroristických aktivít na celom svete. Uvádza sa, že útok na WTC v New Yorku bol organizovaný práve s využitím Internetu[5].

3.3 Komunikačné kanály teroristických skupín

I napriek tomu, že teroristické skupiny pracujú izolovanie na princípe „netvar", komunikácií s ostatnými skupinami a s centrom sa môžu vyhnúť. K tomu im slúži celá rada prostriedkov, počínajúc bežnou poštou a končiac šifrovanou mobilnou komunikáciou alebo satelitným systémom Irídium. Avšak najčastejším médiom je pravdepodobne Internet. Mimo to, že umožňuje takmer neobmedzenú rozličnosť komunikačných techník, dovoľuje i ľahké šifrovanie, utajovanie alebo skrývanie prenášaných správ a pri vhodnom postupe i obtiažne zistiteľnú identitu odosielateľa i adresáta. Všetky tieto vlastnosti nahrávajú teroristickým skupinám, a tak kyberpriestor – Internet, sa stáva doménou koordinácie teroristických akcií.

Kategorizovať techniky používané teroristickými skupinami pre komunikáciu jej obtiažne. Medzi jedny z najobtiažnejších sa javí steganografické techniky ukrývanie informácií. Je to hlavne preto, že klasické šifrovanie síce zamedzí zistenie obsahu správy, ale prezradí, že je správa šifrovaná, a teda jej obsah je „podozrivý". Steganografické techniky nie sú ľahko identifikovateľné a hľadanie steganografickej spracovanej správy je náročné.

---

[5] Nemusí sa jednať iba o Internet. Práve v súvislosti s citovanou teroristickou akciou sa uvádza, že nejakú dobu pred útokom na WTC bol aktivovaný družicový komunikačný systém Irídium, ktorý bol pre malú ekonomickú návratnosť už dlhšiu dobu mimo prevádzku. Pritom významný vlastnícky podiel na tomto systéme náleží osobám blízkym Al Kajde.

Príkladom môže byť komunikácia najznámejšej teroristickej skupiny Al-Kajdá. Pre prenosy informácií o chystaných teroristický útokoch boli používané obrázky na pornografických weboch so stenograficky ukrytou informáciou a chatové miestnosti zamerané na šport alebo pornografiu pre zdelovanie jednoduchých upozornení na nové správy. Vo voľných bitoch formátu .jpg boli ukrývané nielen texty, ale i plány cieľových objektov, fotografie cieľov alebo mapy. Steganografické metódy sa ukázali ako veľmi účinné pri minimálnych nákladoch na ich realizáciu – celá rada programov je voľné stiahnuteľná z internetu alebo sú k dispozícií za minimálne poplatky. Steganografické poplatky môžu ukrývať nielen textovú alebo grafickú informáciu, ale môžu slúžiť k prenosu i zvukového záznamu alebo videozáznamu. Rovnako ako sa nemusí orientovať iba na formát .jpg, ale môže používať voľné bity vo formátoch .gif, .mp3, .wav a podobne.

Predmetom stenagografickej manipulácie nemusí byť dostupný súbor, ale môže byť použitý priamo text elektronickej správy. Napríklad program „Spam Mimic Encode“ vytvorí z regulérnej krátkej správy inú správu, nerozoznateľnú od spamu, a tak ju vlastne ukryje. Prijatá „spamová“ správa je potom dekódovaná späť programov „Spam Mimic Decode“ do čitateľnej podoby.

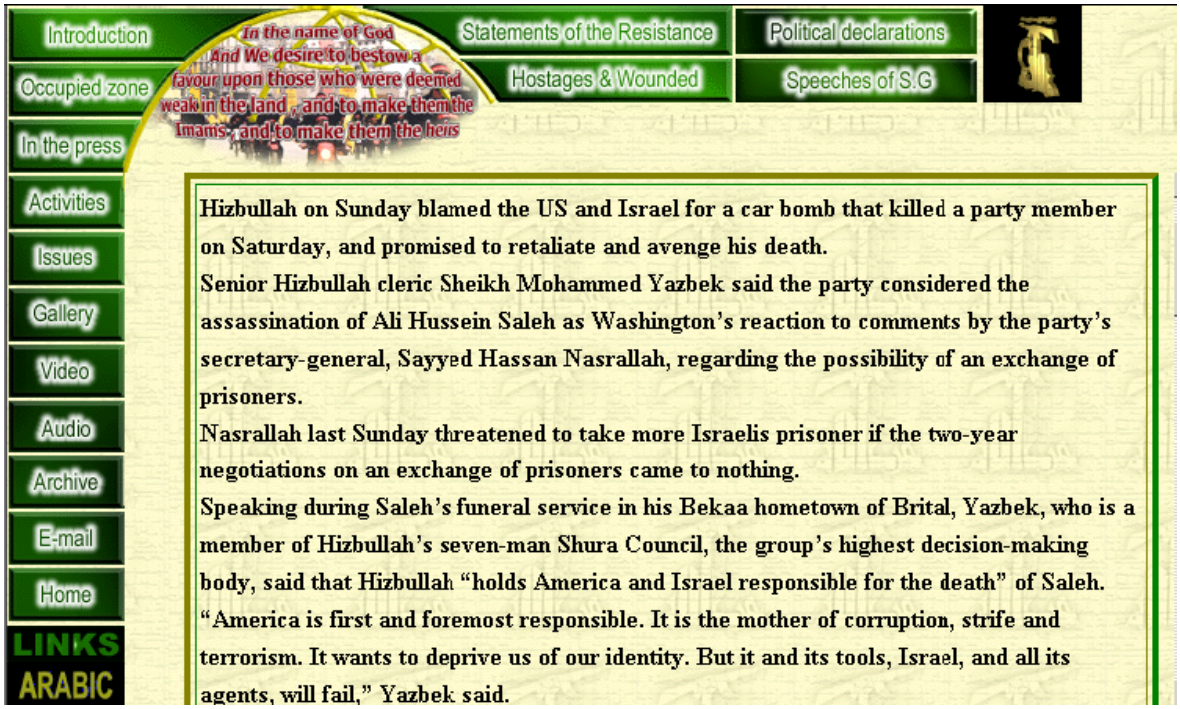
3.4 Ideologické zneužívanie kyberpriestoru

Internet poskytuje možnosť extrémistickým a teroristickým skupinám i jednotlivcom, a to hlavne v oblasti rýchlej a relatívne utajovanej komunikácie, kedy slúži k vzájomnej výmene informácií a pokynov, k plánovaniu a koordinácií akcií alebo prevodov finančných prostriedkov. Podstatnou mierou sa podieľa na šírenie propagandy, získavania a mobilizácií nových aktivistov, sympatizantov či sponzorov; obhajobe teroristických činov a podnecovanie jednotlivcov k ich páchaniu. Internetové servery teroristických skupín často obsahujú návody na výrobu improvizovaných zbraní alebo rafinovanou propagandou zacielenou na mladšiu generáciu.

Bezmála všetky teroristické skupiny a organizácie prevádzkujú svoje internetové stránky. Obvykle sú zverejňované v niekoľkých jazykových mutáciách a nechýbajú ani špeciálne stránky zamerané na deti a a ženy obsahujúce rozprávky či komiksy, do ktorých sú spracované príbehy sebevražebných atentátnikov. Interaktívny spôsob komunikácie s teroristickou sieťou, kedy obidve strany zostávajú v anonymite a nikdy sa nestretnú vedie k fenoménu, ktorý sa nazýva „samoradikalizácia“ a „samovýcvik“. Osoby prechádzajúce

týmto výcvikom pôsobia izolovane od ostatných teroristov, jednotlivcov či malých skupín, plánujú a pripravujú alebo prevádzajú teroristický útok, ani by sa priamo stretli s ideovými vodcami siete, ku ktorej sa hlásia.

Monitorovanie stránok týchto organizácií policajnými orgánmi a spravodajskými službami je nesmierne nákladné. Nie je dostatočný počet analytikov, schopných aspoň rámcovo monitorovať, nato hlboko študovať, všetky existujúce stránky a to hlavne v arabčine. I keď by to bolo technicky jednoduché likvidovať tieto internetové stránky, boli by to skôr kontraproduktívne, pretože zánik stánok na jednom servery by viedol k ich otvoreniu na servery inom. Monitorované stránky teroristických skupín sú na druhú stranu často zdrojom informácií, užitočných i pre bezpečnostné zložky a v prípade ich systematického odstraňovania by teroristi mohli začať používať iný, ťažšie monitorovateľný spôsob komunikácie.



Obr.3: *Príklad Hizballah website*

Ozývajú sa názory, že teroristi dávajú prednosť vizuálnym efektom, spôsobeným napríklad bombami a internet im slúži skôr k propagande a vzájomnej komunikácií, nemusí to platiť vecne. Kyberteroristický útok a likvidácia určitého segmentu infraštruktúry môže byť rovnako tak efektívne sprevádzaným javom „klasického" teroristického útoku. V súčasnej

dobe sa hlavne objavujú sprevádzané javy v kyberpriestore, ktoré reagujú na konkrétnu akciu strán zapojených do teroristického stretu.

4 FORMY POČÍTAČOVEJ KRIMINALITY

Pri členení počítačovej kriminality sa pridŕžam rozdeleniu podľa Rady Európy**.** Jej zmyslom je zjednotiť legislatívu európskych krajín, nielen preto, že sa jedná o problematiku počítačové kriminality, ale tiež z toho dôvodu, že táto trestná činnosť má medzinárodný charakter. Členenie podľa Rady Európy je nasledujúce:

Do Minimálneho zoznamu trestných činov sú zahrňované:

- počítačové podvody,
- počítačové falzifikácie,
- poškodzovanie počítačových dát a programov,
- počítačová sabotáž,
- neoprávnený prístup,
- neoprávnený prienik,
- neoprávnené kopírovanie autorsky chráneného programu,
- neoprávnené kopírovanie fotografie.

Do Voliteľného zoznamu trestných činov je zahrnutá:

- zmena v dátach alebo počítačových programoch,
- počítačová špionáž,
- neoprávnené užívanie počítača,
- neoprávnené užívanie autorsky chráneného programu.

Tím, že boli vymedzené jednania do týchto dvoch zoznamov, došlo v podstate k vymedzeniu trestných činov, ktoré je potrebné stíhať v európskych krajinách. Minimálny zoznam obsahuje také jednania, ktoré by mali byť ako skutkové podstaty trestných činov zapracované do právnych noriem jednotlivých zemí, aby bolo možné viesť účinný boj proti počítačovej kriminalite. Vo Voliteľnom zozname sú uvedené jednania, ktoré by bolo vhodné kvalifikovať ako trestné činy, avšak nie to nevyhnutné.

Týmto prehľadným spôsobom bola klasifikovaná počítačová kriminalita tak, aby bolo zreteľné, čo všetko možné je pod tento pojem zahrnúť. Podľa môjho názoru je významnejšie rozdeliť počítačovou kriminalitu podľa foriem jeho páchania.

- **Útok proti počítaču** - Táto kriminalita predstavuje vlastne útoky proti technickým prostriedkom informačného procesu, t.j. zberu, prenosu, uchovanie, spracovanie a distribúcií dát (informácií), ktoré je uskutočňované prostredníctvom výpočtovej techniky. Páchateľ sleduje predovšetkým obohatenie vlastnej alebo tretej osoby. Môže sa jednať o priamy útok alebo útok vo svojich dôsledkoch alebo útoky s rôznou motiváciou zamerané proti fungovaniu výpočtovej techniky a k neoprávnenému nakladaniu s ňou.

- **Útok proti programovému vybavení a dátam -** útok proti programovému vybavení počítača a uloženým dátam. Ten útok môže nadobudnúť niekoľko foriem. Od najjednoduchšieho zmazanie programového vybavení až po zavedení víru do programového vybavení a následné straty programov a dát.

- **Deštrukčná činnosť prostredníctvom víru -** v súvislosti s útokom na programové vybavenie a dáta počítača s možnosťou ich veľmi pravdepodobnej straty je potrebné sa zmieniť o deštrukčnej činnosti počítačových vírov. Počítačový vírus je nenápadný malý program, ktorý má pri spustení schopnosť sám seba rozmnožovať. Ďaleko razantnejší, a tím spoločensky nebezpečnejšie, sú logické útoky, kedy páchateľ využije vlastností počítačového systému, hlavne jeho slabín. Jedná sa o tzv. logické bomby, kedy sa programy aktivujú za určitých podmienok, napr. po určité dobe alebo po spustení určitého súboru a potom vykonávajú i svoji vlastní "vírovou" činnosťou.

- **Počítačové pirátstvo -** Pod pojem "počítačové pirátstvo" či "softwarové pirátstvo" je zahrňovaná trestná činnosť, kedy páchateľ úmyselne, bez zvolenia autora (bez riadneho oprávnenia) kopíruje programové vybavení a ďalej ich predáva za účelom zisku, alebo pracou na tomto nelegálne získanom programovom vybavení dosahuje zisku pre seba alebo inú osobu.

- **Zneužívanie výpočtovej techniky pre osobné účely -** Páchatelia tejto trestnej činnosti sú obvykle špecialisti na spracovanie dát, systémoví programátori apod. V každom prípade je treba zdôrazniť, že nedovolené dispozície s cudzími vecami sú nežiaduce. I používanie cudzieho počítače k iným než zadaným úlohám je nežiaduce bez ohľadu na to, či je realizované neziskovo, mimo pracovní dobu, a nie na úkor plnenie pracovných povinností.

- **Prenikanie do počítačových systémov** - Relatívne samostatnú oblasť v útokoch proti programovému vybaveniu a dátam uloženým v informačných systémoch tvorí tzv. skupina hackerov - prienikárov, ktorí sa snažia obísť zabezpečenie informačného systému a neoprávnene do neho vniknúť. Na začiatku prieniku je recesia a túha dokázať, že hacker je "lepší" než použitý bezpečnostní systém. Od skupiny hackerov sa odlišuje iná skupina, tzv. crackeri, ktorí sa zaoberajú narušením ochrany programov (napr. proti neoprávnenému kopírovaniu). Osoba môže byť hackerom, ktorý sa snaží vniknúť do cudzej databázy, ale tiež i crackerom, ktorý vymyslí a zrealizuje odblokovanie určitého programového vybavenia.

- **Zmeny v programoch, dátach a technickom zariadení -** Páchatelia týchto trestných činov predovšetkým menia programy a dáta za pomocou iných programov, vírom alebo priamymi zásahmi programátora. Jedná sa o tzv. počítačovou defraudáciu, kvalifikovanú ako trestný čin poškodzovania cudzích vecí

- **Neoprávnený prístup k dátam, získavanie utajovaných informácií - počítačová špionáž -** Špionáž uprednostňuje systémy verejnej infraštruktúry ako sú elektrárenské siete, bezpečnosť letísk, finančné trhy či distribučné siete. Hackeri sa čoraz častejšie podieľajú na profesionálne plánovaných, dobre zaplatených operáciách

- **Zneužívanie počítačových prostriedkov k páchaniu inej trestnej činnosti -** Najjednoduchší, ale i najúčinnejší spôsob získaní finančných prostriedkov prostredníctvom počítačov je manipulácia s dátami. Môže byť zameraná na rôzne oblasti ľudskej činnosti, napr. na úpravu evidenčných údajov o skladovanom

tovare. Páchatelia tejto trestnej činnosti menia dáta úpravou dokladov, z nich sú dáta zriaďované alebo ich úpravou na médiu, na ktorom sú uložené. Najčastejšou formou je zmena vstupných dokladov a získavanie iných dát do počítača.

- **Použitie počítača k páchaniu ďalšej trestnej činnosti -** kriminálne javy, kde je počítač nástrojom páchateľa k páchaniu ďalšej trestnej činnosti, ktorá už nie je viazaná na výpočtovú techniku, programy alebo dáta. Typickým predstaviteľom tejto oblasti je využitie výpočtovej techniky k modelovaniu situácií, ktoré môžu nastať pri páchaniu trestného činu. Jedná sa o činnosť veľmi náročnú, ktorú v dobrej kvalite zvláda iba odborník zaoberajúci sa problematikou modelovaniu situácií.

4.1 Hackerské nástroje

Prvé hackerské nástroje z počiatku osemdesiatych rokov minulého storočia boli založené na schopnosti hackera pochopiť psychológiu obsluhy počítača a uhádnuť používané heslo. Vzhľadom k malému zabezpečeniu vtedajších systémov a nepatrnej vedomosti obsluhy týchto systémov o zaistení bezpečnosti uložených informácií nebolo uhádnutia hesla pre dobrého psychológa väčšinou zložité. V polovici osemdesiatych rokov sa objavili prvé autoreplikujúce kódy a prelamovače hesiel, založené na postupnom skúšaní možných kombinácií povolených znakov. Zároveň sa objavili prvé skutočné hackerské pokusy o odhalenie chýb alebo slabín systému i ich využitie.

Technológia, s ktorou hackeri súťažia a ktorú používajú, nutne potrebuje programové heslo alebo i hardwarové nástroje, aby ju bolo možné analyzovať a ovládať. Nasledujúci zoznam hackerských nástrojov nie je úplný a zahrňuje prevažne nástroje známejšie a používanejšie. Podľa typu použitia je možno hackerské nástroje rozdeliť na:

- Hardwarové nástroje, kam patria techniky hľadania bezpečnostných dier v čipových kartách. Bolo by mylným predpokladom do hackerské komunity zahrňovať iba programátorov, pretože prvé techniky phreackerov boli v podstate blue-boxy a týmto označením sa veľa technických zariadení pre neoprávnený prístup označuje dodnes.

- Softwarové alebo programové nástroje, ktoré v hackerskej komunite prevažujú a ich prehľad je uvedený v nasledujúcej podkapitole

- Sociálne inžinierstvo alebo techniky zneužitia ľudského elementu

4.1.1 Definícia hackera

I keď sa hackerské nástroje neustále zdokonaľujú a automatizujú, najdôležitejšia súčasť hackerského útoku je a zostáva sama osoba hackera. Sú to jeho nabité vedomosti, znalosti a dovednosti, ktoré určujú úspešnosť útoku. Hacker je osoba, ktorú baví skúmať detaily programových systémov a hľadať metódy, ako ich vylepšiť. Vyniká v programovaní a veľakrát sa jedná expertov alebo nadšencov v danom vednom obore.

Ďalšiu skupinu tvoria prelamovači hesiel „password crackers“. Ide o jeden z najstarších nástrojov používaných hackermi. Slúžia k prelomeniu ochrany alebo autorizácií, ktorá je uskutočňovaná statickým heslom (moderné bezpečnostné techniky používajú dynamické heslá, ktoré sú závislé na čase prístupu a užívateľ musí vždy použiť zvláštny kalkulátor k vygenerovaniu aktuálneho hesla). Princíp ich práce spočíva v najrôznejšej kombinácií znakov, ktoré podľa uváženia autora prelamovača alebo jeho užívateľa pripadajú v úvahu a pokiaľ autorizácia prejde je nájdené správne heslo odoslané hackerovi. Existujú dva základné druhy útokov realizovaných prelamovačmi hesiel:

- Slovníkové útoky, ktoré skúšajú použiť známe slová z vlastnej databáze slov.

- Útoky hrubou silou, ktoré postupne generujú všetky možné kombinácie potrebnej dĺžky z vybraných znakov a skúša, či nevyhovujú zadanému heslu.

Počítačoví zločinci sa pri vývoji, distribúcií a použití nebezpečného kódu a služieb stále viac profesionalizujú a dokonca komercionalizujú. Profesionálni crackeri môžu využívať napríklad rôzne nástroje pre phishing, ktoré umožňujú automaticky vytvárať phishingové weby (falošné kópie pôvodných webov). Útočníci zneužívajú bezpečnostných slabín dôveryhodných webov. Napadnutý web môžu crackeri zneužiť ako zdroj pre distribúciu nebezpečných programov, ktoré napadajú ostatné počítače. Zvlášť cenné sú komunitné servery, pretože poskytujú prístup k veľkému množstvu ľudí, z nich veľký počet danému

webu dôveruje. Tieto služby na viac obsahujú mnoho dôverných informácii o užívateľoch, čo následne slúži ku krádežiam identity.

5 SPÔSOBY KYBERNTICKÉHO BOJA

Pre súčasnú dobu je príznačné zvyšovanie rôznych aktivít pri boji proti hacerom a počítačovej kriminalite vôbec. Toto platí pre prostredie Internetu a k nemu pripojené systémy dvojnásobne. Bezpečnosť v oblasti informačných technológií je kľúčovým problémom v každom modernom národnom hospodárstve. Z hľadiska využívania výpočtovej techniky boli vojenské konflikty až do súčasnosti len na úrovni podpory pomocou počítača (Computer Aided War). Informačná vojna v pravom slova zmysle začína až v tom momente, keď sa hlavnou zbraňou a súčasne terčom útokov stane práve počítač.

Dokonalé počítačové systémy sú dnes veľkou konkurenčnou výhodou vyspelých krajín, bez ktorých nemôžu fungovať. Súčasne však tým predstavujú aj ich najzraniteľnejšie miesto. V takejto vojne ide o to, ako zneužiť, poškodiť alebo zničiť informácie, prípade informačné systémy protivníka a súčasne uchrániť pred napadnutím svoje. Veľmi účinné môže byť zmazanie dôležitých údajov alebo celých databázových systémov pred pripravovanou vojenskou akciou metódou tzv. *hrubej softvérovej sily*.

Hackeri sú dnes, na rozdiel od v minulosti častých príležitostných nelegálnych sieťových aktivít, často využívaný na organizovanými kriminálnymi organizáciami, veľkými firmami aj vládami na cieľavedomú prípravu veľkých informačných bitiek proti obranným mechanizmom počítačových systémov.

Hlbokým paradoxom súčasnosti je skutočnosť, že najvyspelejšie štáty sveta intenzívne rozvíjajúce možnosti informačnej vojny (hlavne krajiny NATO), sú aj metódami tejto vojny najviac zraniteľné. Naopak, ich potenciálni protivníci sú na nižšej informačno-technologickej úrovni. To potom znamená, že sa síce nemôžu v takom rozsahu tejto vojne venovať, ale súčasne sú týmito prostriedkami oveľa menej zraniteľní. Kto takéto výpočtové systémy nemá, tomu ich ani nie je možné napadnúť alebo dokonca zničiť.

Kybernetické vojny sprevádzajú takmer každý politický, náboženský alebo vojenský konflikt. Dnešný Internet, spojujúci milióny serverov a užívateľských staníc sa stáva virtuálnym bojiskom, či to chceme alebo nie. Medzi najpopulárnejšie a najznámejšie metódy patrí *defacement*, kedy sú pôvodné stránky serveru nahradené novými, ktoré obsahujú špecifické politické alebo sociálne postavenie.

Kybernetické vojny sú vedené elektronickými prostriedkami s cieľom poškodiť alebo ochromiť informačné systémy a s nimi infraštruktúru nepriateľa počas vojnového konfliktu vedeného klasickými zbraňami. To je podstatný rozdiel oproti terorizmu. Kybernetické vojny majú niekoľko dôležitých atribútov:

1. *Sprevádzajú vždy reálny vojnový konflikt, vzplanú veľmi skoro po eskalácii klasického konfliktu.*
2. *Ich intenzita sa z roka na rok stupňuje.*
3. *Útoky sú čoraz komplikovanejšie a organizovanejšie.*

5.1 Spôsoby útokov

Informačná vojna patrí medzi najnovšie koncepcie predovšetkým Ministerstva obrany USA. Hlavnými zbraňami v informačnej vojne sú informačné prostriedky a informačné technológie. Používané sú k rýchlemu a hlavne skrytému pôsobeniu na vojenské, ale aj civilné informačné systémy protivníka s cieľom narušovať alebo znemožňovať prevádzku týchto systémov, manipulovať s obsahom a formou prenášaných informácií.

V modernej počítačovej dobe už nemajú až taký význam zbrane hromadného ničenia. Nové rozmery začali nadobúdať tzv. humanitné, nesmrtiace zbrane. Preto boli zavedené nové pojmy ako HERF[6], alebo EMPW[7].

V prípade HERF ide o neviditeľný zväzok lúčov pre človek neškodný, ale deštruktívny pre všetky elektronické zariadenia. Silu výboja je možné regulovať, takže výpočtové prostriedky sa len buď reštartujú alebo dokonca úplne zničia. Fungovanie HERF možno prirovnať k "rádiovej" puške, ktorou je možné zničiť konkrétny počítač alebo súčasne celý informačný systém. Ďalšie nebezpečenstvo použitia možno dokumentovať na reálnej možnosti zostrelenia napríklad lietadla doslova preplneného elektronikou.

---

[6] High Energy Radio Frequency - vysoko energetický rádiový signál.

[7] Electromagnetic Pulse Weapon - elektromagnetická pulzná zbraň.

EMPV má rovnaké účinky ako HERF s tým rozdielom, že na rozdiel od "protipočítačovej pušky" pôsobí ako "proti počítačová bomba". Po aktivovaní EMPV vyvolá veľmi silné pulzujúce magnetické pole úplne a nezvratne zničiace všetku elektroniku v jej dosahu.

Ďalšími možnými spôsobmi útokov je infiltrácia počítačových programov zdravotne postihujúcich obsluhu pred obrazovkou (prípadne ju len dočasne vyradí). K tomuto účelu úplne postačí nastaviť vhodný rytmus a frekvenciu blikania[8].

Nepriateľské výpočtové systémy môžu po príslušnom zásahu robiť malé chyby, pretože veľkými by na seba upozornili a narúšať bojové akcie. Možné je "bombardovať" výpočtové centrá protivníka. V prípade zapojenia hackerov sa môže ich útok prejaviť napríklad ako obyčajná porucha.

Konzultanti známej americkej poradenskej firmy KPMG uviedli na konferencii New Hack Tour, ktorá bola v roku 1998 venovaná problematike hackerov, niekoľko najčastejších hackerských úskokov:

- **Útok na server pracujúci pod operačným systémom Unix alebo Windows NT cez protokol TCP/IP.** Implementácia tohto protokolu do väčšiny operačných systémov údajne nie je bezchybná.
- **Odchytávanie dát** z rôznych (nešifrovaných) webových formulárov a webových mailových serverov.
- **Útoky typu *Smurfing* a *Spoofing,* kedy hackeri svoju aktivitu a tvária sa, akoby sa nachádzali na inej adrese.** Typicky v prípade spoofingu je možné oklamať firewall modifikáciou hlavičky paketov tak, že sa tieto pakety tvária ako IP adresa patriaca do vnútornej siete.

Jeden z možných spôsobov útoku môže dokonca vyvolať aj vznik medzinárodného konfliktu. Princípom je využitie úspešného útoku (v skutočnosti fingovaného) na nejaký menej zabezpečený server ako odrazový mostík pre skutočný útok na iný server. Už sa

[8] V prípade japonského kresleného televízneho seriálu pre deti s akousi "postavičkou" vysielajúcou svetelné lúče museli byť hospitalizované desiatky detí.

vyskytli prípady použitia ako destabilizačného prvku medzinárodných vzťahov, zatiaľ len s následkom diplomatických protestov.

Útok je možné zjednodušene popísať na modelovej situácii dvoch štátov A a B, medzi ktorými panuje veľké napätie. Útočník (napr. tretí štát, ktorý má záujem na prepuknutí a následnej eskalácii konfliktu) sa cez server ministerstva obrany štátu A dostane na server armády štátu B (svoju prítomnosť sa prirodzene nesnaží veľmi zamaskovať). Po odhalení útoku povedú stopy na ministerstvo obrany štátu A, ktorý bude prirodzene následne obvinený z vážneho porušenia bezpečnosti štátu B. Pri tomto útoku útočník totiž pri odchode z cieľového servera späť na odrazový mostík "nedokonalo" zamaskuje stopy a tie potom povedú práve k zneužitému serveru.

V minulosti bolo pravidlom slušnosti hackerov nič nepoškodiť v prelomenom systéme. Dnes to už nie je pravidlom a "hackovanie" sa využíva aj na vojenské účely (na oslabenie obranyschopnosti protivníka), priemyselnú špionáž, finančné podvody alebo kriminálne účely.

Zatiaľ sú chytenými kriminálnikmi iba mladíci, ktorí prenikajú do systémov skôr zo zábavy. Čiže nejde o nič príliš spoločensky závažného a nebezpečného, žiadni priemysloví špióni alebo dokonca vojenské kontrarozviedky. Podľa predpokladov organizácie CERT[9] pri Carnegie Mellon University v Pittsburghu, veľká väčšina prienikov zostane neodhalená a narušiteľom sa pritom podarí požadované informácie získať. Kto tieto informácie požaduje, čo za ne platí a komu, to dnes skutočne nikto nie je schopný odhadnúť a nieto ešte zverejniť. To ale môže tiež znamenať, že odhalenými sú len "prienikári - amatéri" a skutoční "profesionáli" môžu pôsobiť beztrestne ďalej.

Túto skutočnosť nepriamo potvrdilo vyjadrenie Josepha Markowitza, riaditeľa kancelárie Community Open Source Program Office, ktorá vznikla pri CIA (Central Intelligence Agency) dňa 1.marca 1994. Podľa tohto vyjadrenia sa koncom leta 1994 na Internet mala pripojiť spravodajská služba CIA a päť ďalších výzvedných služieb, aby tu zbierali

[9] Computer Emergency Response Team, je podporovaný Pentagonom v rámci projektov ARPA - Advanced Research Projects Agency.

neklasifikované a verejne prístupné informácie. Malo by ísť o "prístup k systému vo veľkom" pomocou šiestich uzlov**.** Spravodajské údaje budú využívať aj ďalšie sesterské agentúry typu NSA (National Security Agency) a DIA (Defence Intelligence Agency). O skutočných možnostiach uvedených špionážnych služieb svedčí aj tá skutočnosť, že spoločný ročný rozpočet týchto služieb sa neudáva v jednotkách miliárd dolárov, ale v desiatkach miliárd.

Paradoxne vyznieva skutočnosť, že uvedené špionážne agentúry sa okamžite sami a veľmi živo začali zaujímať i o možné hrozby pôsobiace z Internetu**,** predovšetkým zo strany hackerov. Markowitz uviedol, že prebieha inštalácia bezpečnostného systému, čo je v podstate prístupový server, ktorý chráni internú (vlastnú) sieť proti akýmkoľvek rušivým snahám zvonku. Špeciálne hardvérové zariadenie, ktorého schéma nebola zverejnená, okrem toho umožní, aby analytici prenášali súbory Internetu na svoje vysoko tajné pracovné stanice bez toho, aby bolo možné vykonať prenos opačným smerom.

A čo bolo hlavnými dôvodmi pre takýto krok? Jedným z dôvodov orientácie na Internet je nízke riziko a v porovnaní s nákladnými špionážnymi družicami aj nesmierne lacná prevádzka. Ďalším dôvodom bola možnosť využitia dobrodenia siete ako Internet aj tam, kde sú spravodajské služby prakticky bezmocné.

S ohľadom na už skôr uvedenú skutočnosť, že je jednoduchšie a lacnejšie nabúravať a ničiť, než budovať a chrániť, sa dostávame do nepríjemnej situácie, kedy môže vojnu vyhrať ten, kto ponúkne viac jednému šikovnému a bezcharakternému nadšencovi - hackerovi. Za týchto okolností by malo dôjsť k vážnemu zamysleniu nad úlohou a mierou nasadenia týchto technológií predovšetkým v armáde a ďalších bezpečnostných zložkách, pretože strategická výhodnosť použitia informačných technológií sa môže náhle zmeniť v achillovu pätu celého systému bezpečnosti krajiny.

Je tu však ešte širší pohľad na vzťah medzi bezpečnosťou a informačnými technológiami. V tomto pohľade nejde len o ohrozenie napríklad akcieschopnosti armády, ale aj o možné ohrozenie celého demokratického systému akousi "piatou kolóniou". Touto piatou kolóniou by sa mohol stať práve Internet v jeho dnešnej, celkom neregulovanej podobe. V tejto súvislosti je treba ešte podotknúť, že veľkú časť užívateľov siete Internet tvoria mladí či neplnoletí ľudia, ktorí sú ešte neskúsení a nevyzretí a teda rôznymi spôsobmi ľahšie ovplyvniteľní a manipulovateľný.

Celý problém má zložité legislatívne pozadie vzhľadom k tomu, že Internet nemá žiadneho vlastníka, ktorého by bolo možné postihovať. Internet nadnárodný a nadštátny a teda nespadá do jurisdikcie žiadneho konkrétneho štátu**.** Jedinou možnosťou by sa tak mohla stať koordinovaná globálna regulácia. I tu je možnosť stretu s problémami zneužitia regulačných nástrojov pre mocenské ciele predovšetkým zo strany diktátorských a autoritárskych režimov.

5.2 Príklady informačných stretov

Jedny z prvých známych prípadov informačných vojen, ktoré ovplyvnili výsledky vojenských operácií a možno mali ešte ďalekosiahlejšie dôsledky na priebeh 2.svetovej vojny, boli súboje na poli kryptografie. Známy je napríklad prípad nemeckého šifrovacieho prostriedku Enigma. Nemci do konca vojny neodhalili dešifrovacie možnosti spojencov a Winston Churchil dokonca obetoval mesto Coventry, aby Nemci nenadobudli nejaké podozrenie o schopnosti čítať ich utajenú komunikáciu[10]. Vzájomné čítanie šifrovaných správ oboch bojujúcich strán v priebehu celej vojny menilo priebehy mnohých inak dobre pripravených operácií.

Ďalšie prvky informačnej vojny sa stali súčasťou prakticky všetkých posledných ozbrojených konfliktov, ktorých sa Spojené štáty zúčastnili (napr. vojna v Perzskom zálive, Líbyi alebo v bývalej Juhoslávii).

Napríklad vnášaním dezinformačných správ a falošných povelov do systémov irackej armády v rozhodujúcich fázach bojových operácií dochádzalo k zmätku a následnému narušeniu procesov velenia rozhodujúcich zbraňových systémov letectva a protivzdušnej obrany takým spôsobom, že velitelia neboli schopní rozlišovať skutočné informácie od dezinformácií a výsledkom bol úplný chaos.

Do éteru boli takisto vysielané zo záznamu sekvencie zvukovej korešpondencie napr. pilotov s pozemnými strediskami velenia a navádzania a aj samotných pilotov navzájom, či

[10] Vrcholní anglickí predstavitelia vedeli o pripravovanom bombardovaní mesta z komunikácie Nemcov práve prostriedkami Enigma, ale obyvateľov mesta vôbec nevarovali a ani neposilnili protilietadlovú ochranu mesta.

posádok tankov s miestami velenia pozemných vojsk. Dôsledky boli pre irackú armádu doslova katastrofálne a oveľa závažnejšie, než sa pôvodne všeobecne očakávalo.

Pritom význam prvého skutočného overenia prostriedkov informačnej vojny v reálnom boji bol neprávom odsúvaný do úzadia. Možno úmyselne, s cieľom odviesť pozornosť od konkrétnych príznakov informačnej vojny.

Ani špecialisti irackej armády nie sú schopní dodnes vyhodnotiť, kde, ako a za akých okolností boli ich informačné, komunikačné a elektronické systémy napadnuté. Z toho dôvodu mohli byť rovnaké spôsoby vedenia informačnej vojny zopakované ešte raz v roku 1998, kedy sa opäť rozhorel ozbrojený konflikt v Iraku. Situácia sa potom opakovala len s malým rozdielom, že metódy boja boli ďalej inovované a táto informačné vojna bola tak ešte rafinovanejšia a účinnejšia.

Podobne juhoslovanská protivzdušná obrana bola rušením rádiových sietí natoľko ochromená, že nebola schopná bežnej streľby na bojové lietadlá NATO. Systémy velenia a riadenia, spojovacie siete boli paralyzované, bojaschopnosť sa blížila k nule.

Niekoľko príkladov vojnových ohnísk ilustruje existenciu vedenia kybernetických vojen v nasledujúcich častiach.

5.2.1 Kosovo verzus NATO

Kosovská vojna bola prvou vojnou NATO a zároveň vojnou, pre ktorú média implicitne i explicitne vytvárali dôvody. Z právnych a politických dôvodov vojnou nikdy nazývaná nebola. Obecne sa vojna v Kosove označuje ako dielo donucovacej diplomacie.

Pozoruhodným sprievodným javom vojny bolo zlyhanie spravodajských agentúr. Napríklad Defence Intelligence Agency ani nezaradila vo februári 1999 Kosovo do svojho prehľadu svetových ohnísk napokojov. CIA zase vybrala čínske veľvyslanectvo za cieľ raketového útoku v domnienke, že ide o juhoslovanské federálne riaditeľstvo zásobovania. Tiež kombinácia počasia, roľnícke vychytralosti a technicky primitívna diverzia zmiatla multimiliardové moderné zbrane NATO, ktoré sa snažili nájsť a zničiť srbské obrnené jednotky v Kosove. Ukázalo sa, že laserom riadené bomby sa dajú veľmi zle používať v mrakoch a v Kosove ja na jar vždy počasie zamračené. Výkvet technologickej dokonalosti – strely s plochou dráhou len zamierané na radary systému protivzdušnej

obrany boli zmätené jednoduchou taktikou: Srbovia na niekoľko sekúnd radar zapli, potom ho znovu vypli. Dezorientované rakety sa zatúlali do Bulharska. Srbovia stavali „lákajúce“ mosty z umelej hmoty a NATO ich zničilo, postavili pece na drevo, s komínmi natočenými tak, aby vypadali ako hlavne a NATO ich zničilo s dokonalou presnosťou.

Opakom tejto primitívnej stratégie zameranej na dokonalú technológiu protivníka boli kybernetické útoky zamerané proti infraštruktúre NATO. Po dobu bombardovania boli webové stránky NATO vystavené neustálym útokom, ktoré boli podľa zdrojov NATO iniciované hackermi priamo podporovanými juhoslovanskou armádou. Na všetkých serveroch NATO, ktoré hosťujú medzinárodnú webovú stránku NATO a e-mailové služby, bol spozorovaný DDoS útok typu „ping saturation“ a mailové servery boli neustále bombardované záplavou e-mailov obsahujúcie víry. Tieto útoky opakovane vyraďovali z prevádzky servery NATO. Po zásahu čínskej ambasády posilnili čínsky hackery správy typu: „Neprestaneme útočiť, pokiaľ neskončí vojna!“ na americké vládne stránky.

Obr. 4: *Počas vojny v Kosove boli stránky NATO zaplavené neustálymi útokmi*

V rovnakej dobe ako útoky na servery NATO sa objavovalo veľa defacementov stránok americkej armády, vlády i komerčných firiem, ktoré mali na svedomí srbskí, ruskí a čínski sympatizanti juhoslovanskej vlády. I keď služby priamo spojené s bombardovacou kampaňou NATO neboli týmito útokmi dotknuté, útoky proti komunikačnej infraštruktúre spôsobili vážne poruchy vnútorných i vonkajších komunikačných služieb.

5.2.2 India verzus Pakistan

Preindickí a prepakistanskí hackeri trávia už roky v kybernetických stretoch, ktorých základným motívom sú národné a etnické rozdiely. Od ukončenia vojny v Kašmíre v roku 2000 hackeri obidvoch strán neustávajú vo svojich virtuálnych súbojoch. Medzi najznámejších aktérov patrila skupina G-Foce Pakistan, pôvodne teritoriálne zaradená do oblasti Pakistanu, neskôr bola identifikovaná ako skupina pakistanských hackerov žijúcich v USA. Prepakistánski hackeri sú oveľa aktívnejší v tejto oblasti, do konca roku 2005 napadli viac ako 500 indických serverov zatiaľ čo preindickí hackeri iba niekoľko pakistanských.

5.2.3 Čína verzus Taiwan

Behom prezidentských volieb napadli čínsky heckeri v auguste 1999 taiwanské servery. Používali hlavne metódu defacementu, a to nielen proti politickým a ekonomickým inštitúciam, ale zasiahnuté boli i servery elektrárenských spoločností, telekomunikačných firiem a servery riadené letovým prevozom. Podľa niektorých zdrojov boli cieľom napadnutia 195 serverov snaha negatívne ovplyvniť alebo narušiť taiwanskú infraštruktúru.

6 VPLYV VÝVOJA KYBERNETIKY A VÝPOČTOVEJ TECHNIKY NA POČÍTAČOVÚ KRIMINALITU

Rozsah problematiky počítačovej kriminality veľmi dobre dokumentuje preambula Manuálu pre prevenciu a kontrolu počítačového zločinu OSN: „Rozvoj sveta informačných technológií so sebou prináša i temné stránky. Počítačové systémy ponúkajú nové a vysoko sofistikované možnosti porušovania práva a predovšetkým potenciálu pre páchanie tradičných typov zločinov netradičnou cestou. K ekonomickým škodám, ktoré počítačová kriminalita prináša, je treba pripočítať závislosť celého ľudstva na počítačových systémoch doslova vo všetkých oblastiach denného života, od riadenia leteckej, železničnej i autobusovej dopravy po zdravotníctvo i obranu. I malá chyba v počítačovom systéme môže znamenať ohrozenie ľudských životov.“

Kybernetickou kriminalitou alebo kybernalitou**,** rozumieme takú činnosť, ktorou je porušovaný zákon alebo je v rozpore s morálnymi pravidlami spoločnosti. Táto kriminalita môže byť namierená priamo proti počítačom, ich hardwaru, software, dátam, sieťam alebo v nej vystupuje počítač iba ako nástroj pre páchanie trestného činu, prípadne počítačová sieť a k nej pripojené zariadenia sú prostredím, v ktorom sa takáto činnosť odohráva. Obtiažnosť sledovania prejavov kybernality spočíva v tom, že sa odohrávajú v prostredí, ktoré je objektívne iba veľmi ťažko vnímateľné. Diania v tomto prostredí môžeme pozorovať len pomocou strojov a prístrojov, ktoré nám prístup do kyberpriestoru umožňujú. Útočník, alebo páchateľ pracuje v globálnom prostredí, môže sa v kyberpriestore veľmi rýchlo a nepozorovateľne pohybovať, meniť identity alebo i miznúť. Môže vytvárať, predstierať alebo realizovať rôzne hrozby a vždy bude o krok vpred.

Štúdium kybernality je veľmi široká medzioborová disciplína a nevzťahuje sa iba na úzky okruh trestných alebo nemorálnych činov. Podobne, ako treba organizovaná kriminalita alebo násilná trestná činnosť, zahrňuje i kybernalita veľa rôznorodých oblastí, ktoré sa môžu vzájomne prelínať. Preto nie je ju ľahké jednoducho a jednoznačne kategorizovať a možných kritérií pre jej klasifikáciu nájdeme celú radu. Môžeme napr. vychádzať z delenia podľa role, akú zohráva výpočtová technika pri páchaní trestnej činnosti alebo spôsobom, ktorým sa prejaví vzniknutá škoda, podľa motívu páchateľa alebo podľa jeho vzťahu k poškodenému a podobne.

Všetky skupiny kriminálnych činov, či už v bežnom živote alebo v kyberpriestore, sú spoločensky nebezpečné a predstavujú pre spoločnosť hrozby. Latentné nebezpečie kybernetických hrozieb spočíva hlavne v tom, že ich aktivity nie sú viditeľné a konečné dôsledky nie sú s priebehom páchaného trestného činu viditeľne späté.

6.1 Počítačová kriminalita sa stáva výnosnou činnosťou

Už nie sme v pionierskych dobách osamelých hackerov, ktorí napádali systémy pre zábavu a uznanie. Ti stále existujú, ale v súčasnosti predstavujú významnú hrozbu organizované kriminálne skupiny. Sústredia sa na krádeže dôverných obchodných informácií a ich predaj, vydieranie firiem, ktorých dáta boli odcudzené, vykrádanie bankových účtov a v neposlední rade nelegálny predaj softwaru, filmov a hudby. Organizovaná skupina samozrejme predstavuje podstatne väčšie riziko než jednotlivec a bezpečnostné opatrenia musia byť adekvátne zosilnené. V dôsledku to znamená podmienku na implementáciu komplexnejších a efektívnejších riešení bezpečnosti. Hlavnou motiváciou páchateľov počítačovej kriminality je naďalej finančný zisk a počítačoví zločinci pri uskutočňovaní nebezpečných činností využívajú profesionálnejšie metódy útoku, nástroje a stratégie. Globálne počítačové hrozby sa neustále rozrastajú. Bdelosť a informovanosť o vyvíjajúcom sa svete hrozieb preto nikdy nebola tak dôležitá.

6.1.1 Vývoj útokov na výpočtovú techniku

Hacking, ako nástroj páchania počítačovej kriminality sa dostal do povedomia na prelome šesťdesiatych a sedemdesiatych rokov, kedy skupina technologických nadšencov využívala nedokonalosť telefónnej sieti na uskutočňovanie nespoplatnených diaľkových telefónnych hovorov. Skutočný rozvoj hackingu sa začal prejavovať až v osemdesiatych rokoch, kedy sa širšieho uplatnenia dostáva technológii BBS – Bulletin Board System. BBS boli počítače umožňujúce vzdialené pripojenie a umožňujúce užívateľovi čerpať informácie z databáze uloženej na počítači pomocou štandardizovaných dotazov.

S nástupom webových technológií a prvým vydaním Netscape Navigatoure sa začínajú objavovať prvé špecializované hackerské nástroje, označované ako „easy-to-use“. Od polovice deväťdesiatych rokov minulého storočia začali hackeri používať sofistikované nástroje pre predbežnú diagnostiku sietí a automatizáciu útokov.

Rok	Udalosť
1983	Počítač s kódovým označením WOPR (súčasť vojenského systému BURGR) interpretoval hackerské vniknutie ako odpálenie nepriateľskej nukleárnej rakety. Následkom toho bola uvedená časť armády do stavu vysokej pohotovosti.
1988	Morrisov „Worm“ sa vymkol kontrole a napadol 6 000 počítačov. Dostal tak radu univerzitných a vládnych počítačov mimo prevádzku.
1988	Národná banka v Chicagu sa stala obeťou počítačového podvodu za 70 miliónov dolárov.
1995	Ruskí hackeri previedli 10 miliónov dolárov z Citybank na svoje kontá.
1996	Hackeri napadli webové stránky významných amerických inštitúcií – CIA, Air Force a Ministerstva vnútra.
1996	U.S. General Acounting Office zverejnil správu, že došlo k 250 000 útokom na počítače ministerstva obrany, z toho 65 % bolo úspešných.
1999	Prezident Clinton podpísal nárast výdajov o 1,65 miliardy dolárov na zvýšenie bezpečnosti vládnych počítačov.
1999	Skupina hackerov vydiera anglickú vládu – ovládli britský vojenský satelit a za predanie kontroly požadovali nemalú čiastku.
2000	Jeden z najväčších DDoS útokov postihol servery eBay, Yahoo, Amazon a ďalšie.
2000	Boli ukradnuté zdrojové kódy Windows a Microsoft Office.
2001	Uskutočnený útok na DNS servery. I keď sa podarili zistiť útok skoro okamžite, odstránené následkov trvalo dva dni. Po celú dobu boli neprístupné stránky firmy Microsoft.
2002	Microsoft prerušil vývoj systému Windows, 8 000 programátorov bolo vyškolených pre oblasť bezpečnosti.

Tab. 2: *Prehľad významných útokov na prelomu storočia*

Počítačoví útočníci zneužívajú veľkej výhody, ktorou je anonymita pri ich činnosti v on-line svete. Aj keď je meranie kyberkriminality veľmi zložité, je jasné, že v mnohých prípadoch predbehla svojim rozsahom tradičné kriminálne činy. Kyberzločinnosť je relatívne novým spôsobom páchania kriminality a stále naberá na význame. Americký Federálny vyšetrovací úrad (FBI) zaradil kyber-útoky na tretie miesto v prioritách objasňovania zločinov, hneď za terorizmus a priemyslovú špionáž. Charakteristické pre dnešnú dobu je trvalé stúpanie objemu a dôležitosti spracovávaných, prenášaných a

uchovávaných dát. Súčasne stále masovo stúpa počet užívateľov Internetu. Je teda logické, že zločinnosť v kyberpriestore sa stane rysom dnešnej doby.

6.2 Trendy budúceho vývoja počítačovej kriminality

Jeden z výrazných trendov v súčasnej IT kriminalite je neodvrátiteľná *profesionalizácia*. Ďalším nebezpečným javom, ktorý súvisí jednak s profesionalizáciou, ale tiež so vzrastajúcou *úrovňou zabezpečenia IT* a vzrastajúcou obtiažnosťou prieniku, je skutočnosť, že sa vypláca ísť na systém z úplne inej strany a najzraniteľnejším miestom sa stávajú osoby s prístupovými právami ti systému, teda zamestnanci, administrátori a podobne. Tí môžu byť podplatení alebo zastrašení, aby prezradili prístupové informácie, prípadne aby informácie vyniesli sami. V prípade, kedy dôjde k takémuto vnútornému prieniku do systému, sú všetky bezpečnostné opatrenia na úrovni systému samotného úplne zbytočné.

Druhým markantným trendom v dnešnej počítačovej kriminalite je tendencia, ktorá býva označovaná výstižne ako posun do copyrightu k copyleftu. Jedná sa o stav, kedy je spochybňované samé autorské právo a jeho inštitúty, umelo vytvárané nezdravé vzťahy na trhu a nevyvážané – straniacim vydavateľským spoločnostiam. Prostredníctvom moderných IT technológií a predovšetkým Internetu dochádza k masovému porušovaniu autorských noriem všade vo svete.

Hlavnou motiváciou páchateľov počítačovej kriminality je naďalej finančný zisk a počítačoví zločinci pri uskutočňovaní nebezpečných činností využívajú profesionálnejšie metódy útoku, nástroje a stratégie. Globálne počítačové hrozby sa neustále rozrastajú. Bdelosť a informovanosť o vyvíjajúcom sa svete hrozieb preto nikdy nebola tak dôležitá,"

„*Tí, ktorí sú ochotní predať slobodu za krátkodobý pocit bezpečia, si nezaslúžia ani slobodu, ani bezpečie*“.

Benjamin Franklin

II. PRAKTICKÁ ČASŤ

7 ROZBOR ZNÁMYCH ÚTOKOV

V nasledujúcej časti sa venujem dvom útokom na dôležité infraštruktúry. Prvý z nich popisuje prienik počítačového víru do americkej jadrovej elektrárne, ďalší útok sa venuje napadnutiu estónskych serverov a komunikačnej siete. Tento útok býva označovaný i ako prvá vlastenecká kybervojna.

Kybernetický útok sa od klasického vojenského útoku líši tým, že pri ňom nevznikajú materiálne škody a nenarastá výška ľudských obetí. Hlavným cieľom kyberútoku je ochromiť hlavné obchodné tepny, získať či zničiť dôležité vládne dáta, narušiť bezpečnosť štátu, poškodiť sieťovú infraštruktúru krajiny.

7.1 Prienik počítačového červa do jadrovej elektrárne

Koncom januára 2003 sa podarilo preniknúť do privátnej počítačovej siete jadrovej elektrárne v U.S.A. červovi Win32/SQL.Slammer[11] do časti podnikovej siete spoločnosti FirstEnergy Corp[12]. Červ infikoval existujúci Microsoft SQL Server a následne vyradil z činnosti bezpečnostný monitorovací systém na približne päť hodín.

Spomínaná udalosť sa odohrala začiatkom roka, ale verejnosť sa o nej dozvedela až sedem mesiacov neskôr. Podľa dostupných informácií sa z dôvodu nedostatočného zabezpečenia počítačovej siete a v nej inštalovaných systémov podarilo preniknúť červovi Win32/SQL.Slammer do časti podnikovej siete spoločnosti. Z podnikovej siete sa červ ďalej rozšíril cez "zabezpečený kanál" chránený firewallom priamo do privátnej siete

[11] Počítačový červ naprogramovaný v assembleri. Šíri sa výlučne prostredníctvom počítačovej siete, v ktorej vyhľadáva systémy disponujúce aplikáciami MS SQL Server 2000 a MS Desktop Engine 2000. Takýmto sytémom červ zasiela UPD paket, ktorý po prijatí spôsobí na vzdialenom systéme vznik chyby nazývanej pretečenie zásobníka. Tá má za následok aktiváciu vykonateľného kódu samotného červa, ktorý sa však neukladá na pevný disk infikovaného systému, ale zotrváva výlučne v jeho operačnej pamäti. Následne potom, červ náhodne generuje IP adresy počítačov dostupných v sieti Internet a neustále posiela vo forme UDP paketu svoje vlastné telo. Touto operáciou si zabezpečuje permanentný proces rozširovania, čím môže vzhľadom na zvýšenie záťaže infikovaného systému spôsobiť jeho kolaps.

[12] Spoločnosť FirstEnergy Corp. riadi jadrovú elektráreň Davis-Besse v Ohiu, U.S.A.

spomínanej jadrovej elektrárne. V nej sa mu podarilo úplnou náhodou nájsť jediný Microsoft SQL Server, ktorý nedisponoval potrebnou dôležitou bezpečnostnou záplatou. Následne červ svojou aktivitou v privátnej počítačovej sieti jadrovej elektrárne spôsobil zvýšené zaťaženie jednotlivých počítačových systémov a tiež vyradenie bezpečnostného monitorovacieho systému z prevádzky. Zodpovedným pracovníkom elektrárne sa tento monitorovací systém, ako aj celú ich "zabezpečenú" počítačovú sieť podarilo uviesť do pôvodného stavu a plného výkonu po takmer piatich hodinách. Hovoriť sa dá v tomto prípade o skutočne veľkom šťastí, nakoľko v čase útoku bol bezpečnostný monitorovací systém zálohovaný jeho analógovým ekvivalentom a celá elektráreň sa nachádzala od februára 2002 v štádiu dlhodobej rekonštrukcie. Nečakané objavenie sa nevítaného hosťa – červa v počítačovej sieti jadrovej elektrárne nespôsobilo žiadne väčšie škody ani prevádzkové problémy, i keď dokázalo vyvolať päťhodinové vyradenie jedného z dôležitých bezpečnostných monitorovacích systémov z prevádzky[13].

Tento príklad je opäť jasným dôkazom toho, že cielené i čisto náhodné kyberteroristické útoky sú pre celú našu spoločnosť veľkou, no hlavne reálnou hrozbou. Otázkou zostáva, čo sa môže stať, ak na niektorý z dôležitých, či dokonca strategických objektov zaútočí v budúcnosti šikovnejší hacker alebo masovo sa šíriaci a navyše deštruktívny červ. Je na zamyslenie, aké rôzne podoby mali, majú a môžu mať moderné kyberteroristické útoky a čo môžeme urobiť preto, aby sa ich počet v praxi eliminoval na minimum.

7.2 Napadnutie dôležitých estónskych portálov

Prvý masový kybernetický útok sa odohral v máji minulého roka. Do „husto zasieťovaného“ Estónska sa podľa vyšetrovania nabúrali „vládni hackeri“ z Ruska. Išlo o vyústenie napätých vzťahov medzi Tallinnom a Moskvou. Útoky sa odohrali krátko potom, ako z Tallinnu, bol odstránený kontroverzný pamätník venovaný Červenej armáde.

Na internetové stránky estónskeho prezidentského úradu, parlamentu, ministerstiev, politických strán, médií, najväčších bánk a firiem, ktoré sa špecializujú na komunikáciu, sa

[13] Dostupné z WWW: <http://www.securityfocus.com/news/6767>.

nebezpečne rozmnožili hackerské útoky. Internetové stránky boli zaplavené desiatkami tisícov návštevníkov. Takýto nápor nezvládli a v podstate ich to paralyzovalo. Útok prebiehal na dôležité webstránky prostredníctvom obrovského množstva distribuovaných odmietnutí služby[14]. Estónci sú presvedčení, že útoky boli nariadené a koordinované z Ruska – s jasným politickým pozadím. Rusko obvinenie odmietlo a prehlasovalo, že útoky zdanlivo pochádzali z IP adries ruských vládnych úradov, išlo o niekoho snahu poškodiť Rusko. Do vyšetrovania prípadu sa vložilo i NATO, ktoré vyslalo do Tallinnu niekoľko svojich najlepších odborníkov na kybernetický terorizmus.

Estónsko po minuloročnej kríze nalieha, aby Európska únia zosúladila zákony proti elektronickým útokom a tak zjednodušila trestné stíhanie útočníkov. Kybernetické útoky nie sú definované ako priamy vojenský útok. To znamená, že sa na ne nevzťahuje Článok 5 Severoatlantickej zmluvy[15]. V tomto smere NATO prisľúbilo zmeny a kybernetické útoky by mali byť v legislatívnom aparáte jasne zahrnuté. Útoky boli závratne rýchle, majú tendenciu rýchle sa rozrastať, a tak treba reagovať veľmi pohotovo. Žiaľ, možnosti na proti reakciu končili na hraniciach štátu. Účinná obrana je medzinárodná.

7.3 Spoločná obrana

Žiadna krajina nemá úplnú kontrolu nad Internetom. Je to univerzálny zdroj. Ochranná politika v minulosti podnietila vznik nových medzinárodných noriem správania, ako napríklad nepísaných zvykových zákonov, ktoré chránia prístup k moru. Je však zatiaľ otázne, či sa vyvinie podobný právny rámec na ochranu Internetu z dlhodobého hľadiska.

Komplexná politická smernica, ktorú schválili najvyšší predstavitelia členských krajín NATO v novembri 2006, zahŕňa medzi požiadavkami na spôsobilosť o 15 rokov schopnosť chrániť informačné systémy kritického významu pre Alianciu proti kybernetickým útokom.

---

[14] Jednalo sa o útoky nástrojom DoS, vid. kapitola 7.2.1 Nástroje DoS.

[15] Ak bude napadnutý jeden alebo viacero členských štátov, tento útok bude považovaný za napadnutie všetkých.

Spôsobené škody sú nekonvenčné a útočiaca strana ich môže rýchlo spôsobiť kdekoľvek, odkiaľkoľvek a prakticky zadarmo. Zdieľanie informácií na úrovni NATO umožní včasné varovanie pred podozrivými aktivitami a tiež profilovanie možných útokov. Niektoré členské krajiny NATO sa pred hrozbami internetovej éry snažia chrániť vytvorením národného reakčného tímu pre prípad počítačového núdzového stavu CERT[16].

Koordinácia CERT na úrovni NATO v spolupráci s Európskou úniou by bola z krátkodobého hľadiska dôležitým krokom na obmedzenie významu kybernetických útokov. Napríklad, ak by bol odhalený útok na českú webovú stránku užívateľom, ktorý je pripojený vo francúzskej sieti, český CERT môže požiadať svojho francúzskeho partnera o prerušenie spojenia, ktoré sa pri útoku používa. Príklad z Estónska ilustruje potrebu okamžitej akcie. Estónsky CERT vznikol len v roku 2006 a v mnohých krajinách CERT zatiaľ nebol ustanovený.

7.4 Bezpečnosť v sieťach

Sieťovú bezpečnosť môžeme chápať ako infraštruktúru pozostávajúcu zo sieťových zariadení (servery, smerovače, prepínače, klientske počítače a pod.) a bezpečnostných politík definovaných sieťovými správcami, ktoré slúžia na ochranu pred prístupom do siete, respektíve prístupom k jednotlivým sieťovým zdrojom.

Ako sa brániť proti prienikom:

- **Zálohy** – možnosť návratu dát.
- **Single point of failure** – zabezpečenie takým spôsobom, aby sa na jednom systéme nenachádzali všetky služby (napr. firewall, IPS, mail server, file server). Keď útočník prelomí firewall, stále nemá prístup k mailom alebo file serveru.
- **Aktualizácia** – pravidelnou aktualizáciou zabezpečiť, aby sa na systéme nachádzali všeobecné diery a bugy. Útočník bude mať v prípade útoku sťaženú situáciu.
- **Správne heslá** – nastavovať zásadne zložité heslá.

[16] Computer Emergency Response Team

- **Firewall** – zabezpečuje prístup k jednotlivým službám, ktoré bežia na systéme, možno ním jednoducho určiť, kto má a kto nemá prístup, na základe viacerých kritérií, ako je napr. zdrojová adresa IP alebo adresa MAC.
- **VPN (Virtual Private Network)** – vystavujte na Internete len tie systémy, ktoré tam vyslovene musia byť. Zvyšné systémy potrebné pre komunikáciu len v rámci firemnej infraštruktúry, umiestniť do VPN, kde je komunikácia šifrovaná a systémy nie sú priamo viditeľné z Internetu. Vďaka šifrovaniu je zaistená relatívna bezpečnosť prenášaných dát, no vždy je tu riziko útokov, ktoré smerujú zvnútra siete.

Sieťová bezpečnosť je zložitá problematika a netreba ju brať na ľahkú váhu, pretože v konečnom dôsledku môže mať na podnikanie fatálny dosah, či už v podobe odcudzených, alebo stratených dát, ale aj nefunkčných systémov. Takisto treba mať na zreteli, že úroveň zabezpečenia nesmie byť prekážkou v reálnej práci, a preto treba hľadať vhodný kompromis medzi zabezpečením a obťažovaním používateľov systémov, lebo v prípade, že tí začnú predpísanú bezpečnostnú politiku obchádzať, môže prísť k neželaným dôsledkom.

ZÁVER

Informačná technológia umožňuje teroristom vytvárať globálne organizačné siete nového typu. Ich štruktúry sú, na rozdiel od tradičných skupín, voľnejšie a menej hierarchické. Oslabuje sa ich závislosť na štátoch, jednotlivé skupiny sú funkčne autonómne, no pripravené k spoločnej akcii. Teroristi sa organizujú do globálne prepojených sieti a semiautonomných buniek, ktoré sa združujú a preskupujú podľa potrieb konkrétnej úlohy.

Boj proti kyberterorizmu bude naďalej s rastúcou zložitosťou informačných a komunikačných technológií veľmi zložitý. Kyberteroristi budú vždy o krok vpred teóriou i praxou manažérov a špecialistov informačnej bezpečnosti. Domnievame sa, že kyberteroristi budú stále viac útočiť na dôležité informačné systémy štátnej infraštruktúry. Regulácia rozvodov elektrickej energie, úžitkovej a pitnej vody, dopravné systémy, zdravotníctvo, telekomunikácie sú ciele, ktoré môžu byť zasiahnuté. Ciele nie sú obmedzené iba na fyzické zariadenia. Kvalitatívna obsahová analýza odhaduje, že medzi tieto zbrane sú zaraďované tzv. "génové zbrane", ktoré môžu pôsobiť za živé organizmy, obilie, dobytok i ľudskú populáciu. Preto je nevyhnutné sa neustále vzdelávať oblastiach ako je ochrana dát, informačná bezpečnosť, kryptografie a ďalšie obory. Toto vzdelávanie by malo byť smerované nie len na informačných špecialistov, ale hlavne na politikov, manažérov všetkých stupňov, zamestnancov firiem a štátnych organizácií.

Táto práca pojednávala o možnostiach kybernetických schopnostiach teroristov, popisuje ako zraniteľnosti počítačovej bezpečnosti môžu byť využívané kyberteroristickým útokom. Trvalé počítačové bezpečnostné zraniteľnosti môžu vystavovať kritickú infraštruktúru, vládne počítačové systémy možným kyberteroristickým útokom a ovplyvniť ekonomiku alebo iné oblasti národnej bezpečnosti.

Práca sa zaoberala definíciou kybernetického terorizmu a počítačovej kriminality. Popisuje súčasné technológie podložené počítačovými vírmi, červami a spywarmami, ako tieto zákerné programy umožňujú kybernetické útoky a kriminalitu. Posledná časť pojednávala o známych útokov a ich následných efektov.
V prílohe mojej práce uvádzam príklad súčasných taktík využívaných počítačovými hackermi a taktiež môžu byt použité teroristami pri plánovaní možného kyberteroristického útoku.

V súčasnosti neexistuje žiadny dôkaz, že teroristické organizácie aktívne používajú počítače k plánovaniu útokov a medzi niektorými pozorovateľmi je nezhoda, či kritická infraštruktúra počítačov poskytuje efektívny cieľ podporujúci teroristické ciele. Napriek tomu teroristické organizácie v súčasnosti využívajú Internet ku komunikácií a dostupné informácie uvádzajú, že Al Qaeda[17] a iné skupiny môžu použitím počítačovej technológie pomôcť naplánovať teroristický útok.

Prostredie studenej vojny bolo typické tým, že existovali jasné zámery, ale neznámy potenciál. Súčasné prostredie sa zmenilo v tom, že poznáme dostupný potenciál, ale nepoznáme zámery potenciálnych protivníkov.

[17] Alternatívne názvy al-Qaida, al-Qa'ida alebo al-Qa'idah, je medzinárodné spojenectvo sunnitských islamistov, teroristická organizácia založená v roku 1988 Abdullah Yusuf Azzam (neskôr nahradený Osama Bin Laden).

ZÁVER V ANGLIČTINE

The information technology enables terrorists to create new form of organizational global networks. In contrast, their structures are different from conventional groups, looser and less hierarchal. Dependence on states is weakened; individual groups are functional autonomous ready to joint action. Terrorists are organising to interconnected global networks and semiautonomous cells that are gathered and reordered according to necessity particular task.

The war against cyber terrorism with rising informative and communication technology complexity stays very complicated in the future. Cyber terrorists will always be a step ahead by theory, manager's practise and information security experts. In my opinion, cyber terrorists will still increasingly attack to important information systems of government infrastructure. Distributions of electricity, supply and fresh water, transport systems, health service, telecommunication are aims that can be stricken. Targets are not limited just for physical facilities. Among those weapons belongs so called "gene weapons", which may have effect on living organisms, corn, livestock and population according to quality content analysis estimate. Therefore is necessary educated all the time in the field like data security, information security, cryptography and other fields. The education should be directed not only to information experts but mainly to politicians, managers of all degrees, company employees and government organizations.

This thesis discusses possible cyber capabilities of terrorists, describes how computer security vulnerabilities might be exploited through a cyber terror attack. Persistent computer security vulnerabilities may expose critical infrastructure and government computer systems to possible cyber attack by terrorists, possibly affecting the economy or other areas of national security.

The work presents a working definition cyber terrorism and computer crime, plus explains current technologies underlying computer viruses, worms and spyware, how these malicious programs enable cyber crime and attacks. The final section describes known cyber attacks and their possible effects.

Appendices to this work explain technologies underlying computer viruses, worms, and spyware, how these malicious programs enable cyber crime and cyber espionage, and how

tactics currently used by computer hackers might also be employed by terrorists while planning a possible cyber terror attack.

Currently no evidence exists that terrorist organizations are actively planning to use computers as a means of attack, and there is disagreement among some observers about whether critical infrastructure computers offer an effective target for furthering terrorists' goals. However, terrorist organizations now use the Internet to communicate, and news reports have indicated that Al Qaeda and other groups may be using computer technology to help plan future terrorist attacks.

The existence of clear intensions but unknown potential was typical of surroundings the cold war. Currently surroundings was turned, we know approachable potential while do not know intentensions of potentional enemies.

ZOZNAM POUŽITEJ LITERATÚRY

[1] JIROVSKÝ, V.: *Kybernetická kriminalita.* Praha: Grada Publishing, 2007.

[2] MATEJKA, M.: *Počítačová kriminalita.* Praha: Computerpress, 2002.

[3] POŽÁR, J.: *Některé trendy informační války, počítačové kriminality a kyberterorizmu.* Kriminalistika: c 2005, [cit. 2008-03-20]. Dostupné z WWW: <http://www.mvcr.cz/casopisy/kriminalistika/2005/04/pozar.html>.

[4] LÁTAL, I.: *Počítačová (informační) kriminalita a úloha policisti při jejím řešení* [online]. Policista: c 1998, [cit. 2008-03-20]. Dostupné z WWW: <http://www.mvcr.cz/casopisy/policista/prilohy/pc_krimi.html>.

[5] VOKURKOVÁ, L.: *Počítačová kriminalita se stáva výnosnou činností* [online]. IDG Czech, a. s.: c 2006-05-24, [cit. 2008-05-08]. Dostupné z WWW: <http://www.computerworld.cz/cw.nsf/ID/D7094AEA1534DB33C12571770040F9E6>.

[6] BBC NEWS: *Kosovo info warefar spreads* [online]. *UK:* c 1999-04-01, [cit. 2008-05-08]. Dostupné z WWW: <http://news.bbc.co.uk/2/hi/science/nature/308788.stm>.

[7] MAHMUD, S.: *Modern militant, counter-terror group use of the Internet* [online]. AFP Washington: c 2007-01-25, [cit. 2008-05-08]. Dostupné z WWW: <http://wanabehuman.blogspot.com/2007/01/politicstechnology-modern-militant.html>.

[8] SMIRIAK, M.: *Informačné vojny* [online]. PC denník: c 2001-09-24, [cit. 2008-05-08]. Dostupné z WWW: <http://programovanie.pc.sk/bezpecnost/infvojny/clanok.php?ID=259>.

[9] Jirovský, *V.: Známe prípady informačných vojen [online]*. PC denník: c 2001-09-27, [cit. 2008-05-08]. Dostupné z WWW: <http://programovanie.pc.sk/bezpecnost/infvojny/clanok.php?ID=260>.

[10] GÁLISOVÁ, M.: *Prvá vlastenecká kybervojna* [online]. Týždeň: *c* 2007, [cit. 2008-05-08]. Dostupné z WWW: <http://tyzden.sk/sk/svet/article5.php?searchstring=obvinenie>.

[11] RYAN, J.: Novovznikajúce a rozvíjajúce sa bezpečnostné hrozby: „iVojna“ [online]. NATO Revue: c 2007, [cit. 2008-05-02]. Dostupné z WWW: <http://www.nato.int/docu/review/2007/issue4/slovak/analysis2.html>.

[12] LEPIŠ, M.: *Kyberterorizus v praxi* [online]. Novinky: c 2003-08-21, [cit. 2008-04-25]. Dostupné z WWW: <http://www.virusy.sk/clanok.ltc?ID=420>.

[13] KLIMÁNEK, O.: *Hrozí světu kybernetická válka?* [online]. Telekomunikace, infrastruktura: *c* 2007-02-11, [cit. 2008-05-05] . Dostupné z WWW: <http://www.dsl.cz/clanky-dsl/clanek-892/Hrozi-svetu-kyberneticka-valka%3F>.

[14] ŽILA, M.: *Bezpečnosť v sieťach TCP/IP* [online]. Infoware: c 2008-04-03*,* [cit. 2008-05-08]. Dostupné z WWW: <http://www.infoware.sk/buxus_dev/generate_page.php?page_id=53320>.

[15] TRADOC DCSINT Handbook No. 1.02.: *Cyber operations and cyber terrorism* [online]. Handbook: c 2005, [cit. 2008-05-08]. Dostupné z WWW: <http://www.terrorisminfo.mipt.org/GetDoc.asp?id=2666&type=d> .

[16] Encyklopédia: *Terorizmus* [online]. [cit. 2008-04-10]. Dostupné z WWW: <http://sk.wikipedia.org/wiki/Terorizmus>.

[17] WILSON, C.: *Computer attack and cyber terrorism* [online]. CRS Report for Congress: c 2003-10-17, [cit. 2008-05-29]. Dostupné z WWW: <http://www.fas.org/irp/crs/RL32114.pdf>.

ZOZNAM POUŽITÝCH SYMBOLOV A SKRATIEK

ARPA	Advanced Research Projects Agency
BBS	Bulletin Board System
CERT	Computer Emergency Response Team
CIA	Central Intelligence Agency
DDoS	Distributed Dentiol of Servis
DoS	Dentiol of Servis
DIA	Defense Intelligence Agency
DNS	Domain Name System
DSB	Defense Science Board
EMPW	Electromagnetic Pulse Radio Weapon
FBI	Federal Bureau of Investigation
HERF	Hight Energy Radio Frequency
ICQ	komunikačný program
IRA	Irish Republican Army
IRC	Interner Relay Chat
IT	Information Technology
IPS	Internet Protocol address
KPMG	Jedna z najväčších amerických poradenských firiem na svete
MAC	Massachusetts Institute of Technolog
MIT	Massachusetts Institute of Technology
MSN	Messanger, komunikačný program
NATO	North Atlantic Treaty Organization
NSA	National Security Agency
OSN	Organizácia Spojených Národov

TCP/IP	Transport Control Protocol/Internet Protocol
VPN	Virtulal Private Work
WTC	World Trade Centre

ZOZNAM OBRÁZKOV

ZOZNAM TABULIEK

ZOZNAM PRÍLOH

PRÍLOHA P I: PLÁNOVANIE POČÍTAČOVÉHO ÚTOKU

Existuje päť základných tradičných krokov používaných počítačovými hackermi k získaniu neautorizovaného prístupu a následného prevzatia počítačového systému. Tieto kroky môžu byť využívané k plánovaniu počítačového útoku pre ciele kybernetickej kriminality, špionáže, taktiež môžu byť použité pre účely kybernetického terorizmu. Kroky sú často automatizované cez použitie špeciálnych hackerských nástrojov, ktoré sú voľne dostupné cez Internet. Profesionálny hackeri používajú vysoko sofistikované automatické nástroje a ich efekty sú spočiatku veľmi ťažké zistiteľné pre techniku a personál počítačovej bezpečnosti. Sofistikované hackerské nástroje sú zvyčajne zdieľané iba medzi vyhradenými skupinami profesionálnych hackerov.

- *Krok 1. Prieskum*

  V prvom kroku hackeri používajú rozsiahle predoperačné sledovanie, aby zistili detailné informácie o organizácií, ktorá im neskôr pomôže získať neautorizovaný prístup do počítačového systému. Najbežnejšia metóda je sociálne inžinierstvo alebo falošný zamestnanec odhaľujúci citlivé informácie (ako telefónne čísla alebo heslá). Iná možná metóda je inštalácia vírusu do počítača v kancelárii, worm alebo spyware program umožňujúci sledovanie a prenášanie užitočných informácií späť k útočníkovi. Spyware je druh škodlivého kódu, ktorý je v tichosti nainštalovaný do počítača bez vedomia užívateľa, pri prehliadaní škodlivej webovej stránky. Firewall a aktuálne antivírusové bezpečnostné produkty ho vôbec nemusia odhaliť[18]. Zatiaľ čo je monitorovaný stisk kláves k záznamu webovej aktivity alebo zber snímkov zobrazených na displeji a iné vyhradené informácie pre spätný prenos neznámej tretej osobe.

- *Krok 2. Skenovanie*

  Útočník uskutočňuje dodatočné sledovanie počítačového softvéru a konfiguráciu siete, aby vyhľadal možné vstupné body. Tento proces prebieha pomaly, niekedy trvá mesiace ako útočník hľadá niekoľko napadnuteľných otvorov do systému.

---

[18] Vid. <http:///www.spywareinfo.com/>.

- *Krok 3. Získanie prístupu*

  Akonáhle útočník získal zoznam softvéru a konfiguráciu zraniteľností na cieľovú sieť, môže potichu prevziať systém a sieť použitím ukradnutého hesla k vytvoreniu telefónneho účtu alebo využiť zraniteľnosť tak, aby dovoľovala inštalovať napr. škodlivého trojského koňa, ktorý bude ďalej očakávať príkazy zaslané cez Internet.

- *Krok 4. Udržovanie prístupu*

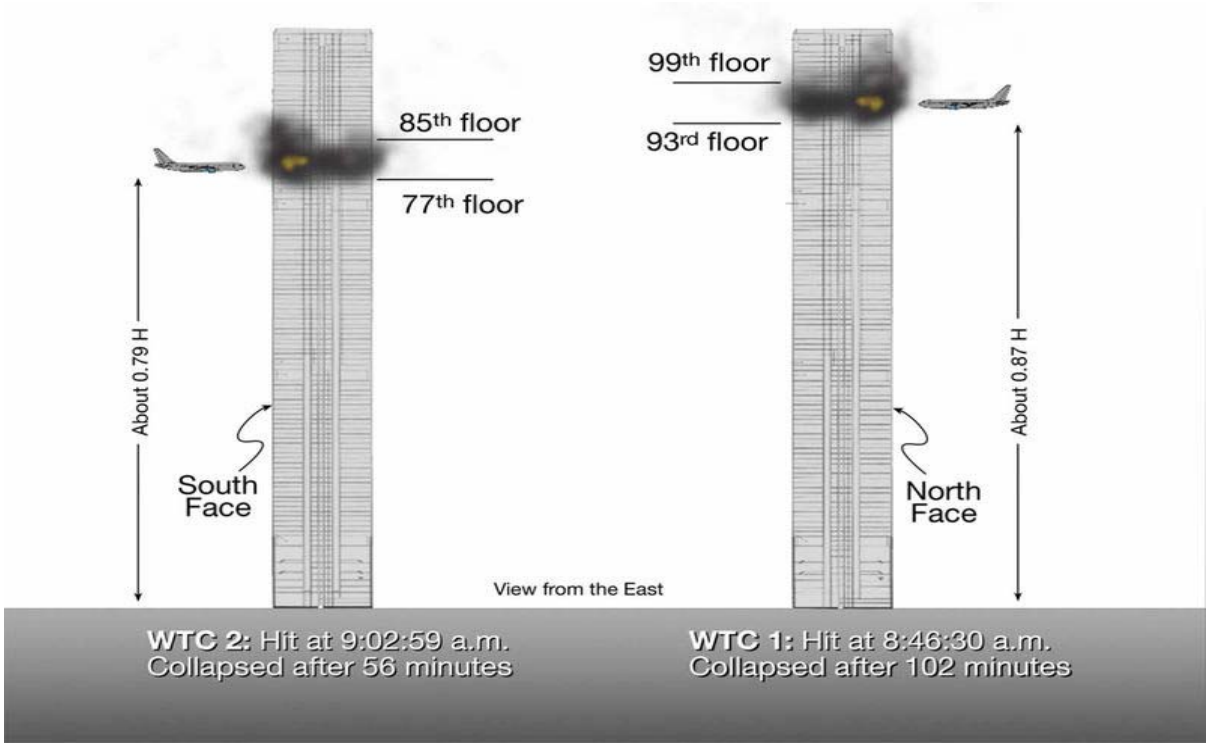
  Ak útočník získal neautorizovaný prístup, môže tajne inštalovať extra škodlivé programy umožňujúce návrat kedykoľvek je potrebné. Tieto program, známe ako Root Kits alebo Back Doors neupozornene bežia a poskytujú útočníkovi ľubovoľný tajný prístup. Ak získa všetky špeciálne privilégia systémového administrátora, potom môže byť počítač alebo sieť úplne prevziata a "vlastnená" útočníkom.

- *Krok 5. Prekrytie stôp*

  Rafinovaný útočníci uprednostňujú neprerušený prístup do počítačového systému a následné prevzatie dát. Musia zostať utajený, aby udržovali kontrolu a ďalej zhromažďovali pre ne potrebné informácie alebo vylepšovať prípravy na úplné zničenie. Programy Root Ket a Trojaský kôň útočníkovi často dovoľujú modifikovať log súbor počítačového systému a vytvárať skryté súbory pomáhajúce vyhnúť sa detekcii legitimácie systému administrátora. Bezpečnostné systémy nemôžu detekovať neautorizované aktivity dôkladného votrelca dlhú dobu.

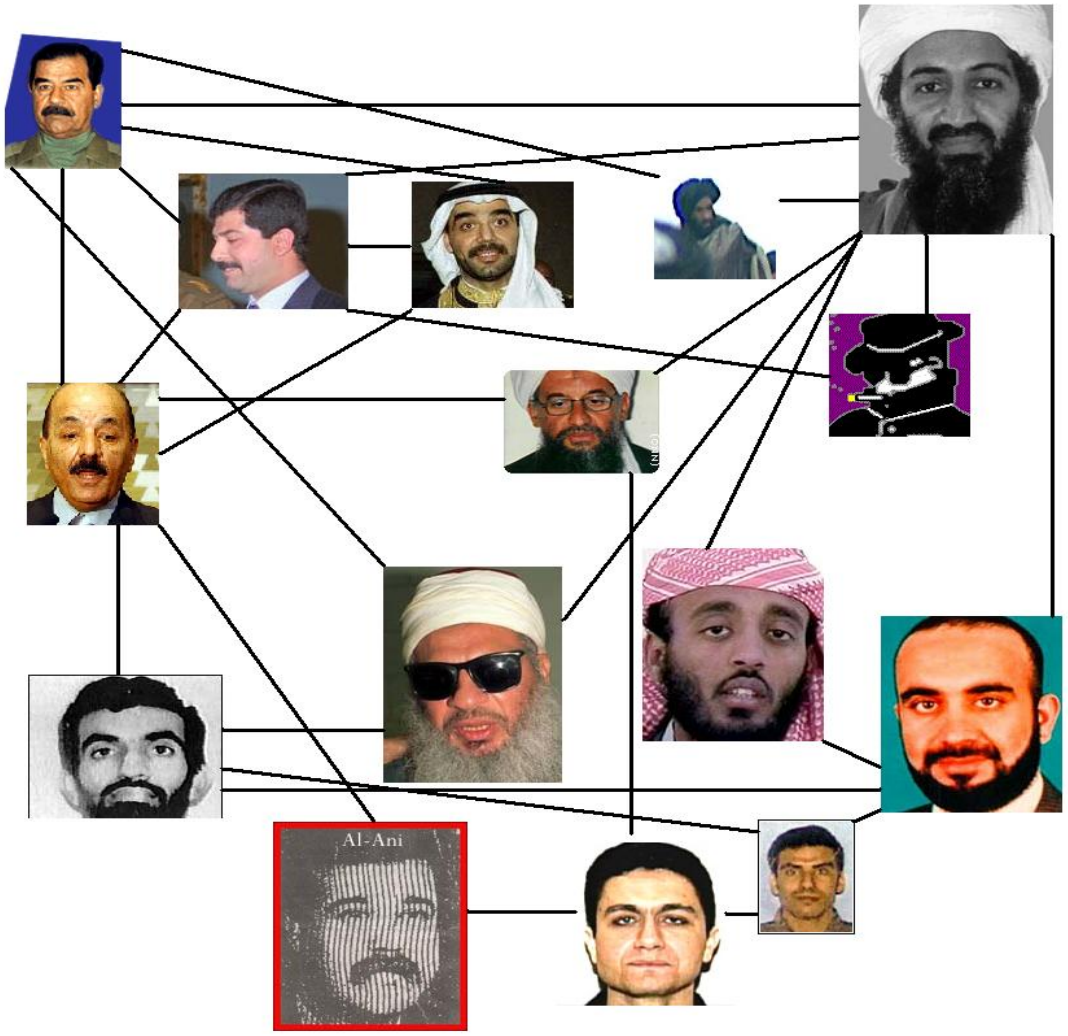
PRÍLOHA P II: OBRAZOVÁ PRÍLOHA

Obr. 5: *WTC, New York, 11.septembra 2001, jeden z najhorších teroristických útokov v histórií*



Obr. 6: *Ilustrácia miest, kde lietadlá narazili do mrakodrapov*

Obr. 7: *Bezpečnostná bariéra, stavaná izraelskou vládou na palestínskom území z obavy pred prenikaním teroristov na územie Izraela*



Obr. 8: *Irackés spojenie s Al-Qaeda, Bagdád má dlhú históriu v podpore terorizmu*