VYSOKÁ ŠKOLA EVROPSKÝCH A REGIONÁLNÍCH STUDIÍ, O.P.S., ČESKÉ BUDĚJOVICE

BAKALÁŘSKÁ PRÁCE

KYBERNETICKÝ TERORISMUS

Autor práce: Tomáš Pulkrábek

Studijní obor: Bezpečnostně právní činnost ve veřejné správě

Forma studia: Kombinovaná

Vedoucí práce: Mgr. Štěpán Kavan, Ph.D.

Katedra: Katedra právních oborů a bezpečnostních studií

2015

Prohlašuji, že jsem bakalářskou práci vypracoval samostatně, na základě vlastních zjištění a s použitím odborné literatury a materiálů uvedených v této práci.

Souhlasím, aby práce byla uložena v knihovně Vysoké školy evropských a regionálních studií v Českých Budějovicích a zpřístupněna v souladu s § 47b zákona č. 111/1998 Sb. v platném znění.

……..

Tomáš Pulkrábek

Děkuji vedoucímu bakalářské práce Mgr. Štěpánu Kavanovi, Ph.D. za poskytnuté rady a vedení bakalářské práce. Dále děkuji také své rodině, všem známým a kolegům za jejich podporu.

ABSTRAKT

PULKRÁBEK T., *Kybernetický terorismus: bakalářská práce,* České Budějovice: Vysoká škola evropských a regionálních studií, o. p. s., 2015. Vedoucí bakalářské práce: Mgr. Štěpán Kavan, Ph.D.

Klíčová slova: aktéři, bezpečnost, kybernetické útoky, kybernetický terorismus, kybernetické zbraně, legislativa, opatření, protiteroristická politika.

Bakalářská práce se zabývá zejména celkovou charakteristikou kybernetického terorismu. První část je věnována aktérům kybernetických útoků. Zde jsou uvedeni jednotlivci a účast institucí. Další část se zabývá kybernetickými zbraněmi, jejich neutuchajícím vývojem vzhledem ke stále se zlepšujícímu způsobu ochrany před nimi samotnými. Bakalářská práce dále popisuje výběr cílů k provedení kybernetických útoků. Zde je zhodnocena motivace, zranitelnost a síla ochranných úkonů potřebných k zastavení kybernetického útoku. V neposlední řadě práce seznamuje čtenáře s případovými studiemi z blízké minulosti a popisuje jejich důležitost pro globální vývoj společnosti. V závěrečné části jsou pak charakterizovány jednotlivé způsoby ochrany před kybernetickým terorismem, mezi které patří zejména protiteroristická politika, legislativa a preventivní bezpečností opatření.

ABSTRACT

PULKRÁBEK T., *Cyber Terrorism: Bachelor thesis,* České Budějovice: College of European and Regional Studies, 2015th. Supervisor: Mgr. Štěpán Kavan, Ph.D.

Klíčová slova: actors, security, cyber terrorism, cyber attacks, cyber weapons, legislation, measures, anti-terrorist policy.

The Bachelor thesis mainly deals with the general characteristics of cyberterrorism. First part is devoted to the actors of cyber attacks. Here are listed the sub-state groups, secret agents, individuals and state participation. Next part deals with cyber weapons, theirs unceasing development due to increasingly better way of protection before themselves. Further the thesis focuses on choice of targets to carry out cyber attacks. Here is evaluated motivation, vulnerability and strength of protective actions to stop cyber attack. Last but not least it introduces the reader with case studies from the near past and their importance to the global development of the company. In the final section is mentioned protection against cyber terrorism. The main elements include anti-terrorism policy, legislation and preventive security measure.

OBSAH

ÚVOD

Téma, o kterém se píše v této bakalářské práci, je v dnešní době velmi aktuální. Kybernetický terorismus je v současné době jedním z nejmodernějších a největších nebezpečí, které hrozí samotným státům a jejich obyvatelům, pokud opomeneme zastaralý způsob vedení terorismu a přírodní katastrofy, které však lidstvo z větší části nedokáže ovlivnit. Kybernetický terorismus je promyšlený, motivovaný útok aktérů proti informačním a počítačovým systémům, jehož cíl je násilí na civilních osobách, které má mnoho podob a může útočit na různé části kritické informační infrastruktury i na různé vrstvy obyvatelstva, nejčastěji se tak děje z důvodů politických či náboženských.

V současné době nikdo nedokáže se určit, kdy a kde může nastat kybernetický útok, nicméně pokud se tak již stane, jsme schopni rychle analyzovat, jaké jsou možnosti a cesty k minimalizaci daného útoku či jeho úplnému zastavení. Všechny moderní státy, které může takové nebezpečí reálně postihnout, by měly přijmout patřičná bezpečnostní opatření, aby těmto útokům mohly pokud možno úplně předejít, případně alespoň snížili pravděpodobnost jeho vzniku a minimalizovaly možné škody.

Všechny vyspělé státy musí neustále prohlubovat ochranu proti kybernetickému terorismu. Po událostech z nedávné minulosti si celý svět začal ještě více uvědomovat, že kybernetické útoky mohou nastat takřka kdykoliv a kdekoliv na světě a mohou zasáhnout hlavně vyspělé státy, které mají maximální bezpečnostní opatření, avšak vzhledem k neustálému vývoji nemohou nikdy zabránit všem útokům.

Vyspělé státy se svou politikou aktivně podílí na boji proti kybernetickému terorismu, a to zejména vytvářením odborných agentur pro větší bezpečnost v kybernetickém prostoru. Zde se shromažďují největší skupiny odborníků v boji s kybernetickým terorismem. Hlavním posláním těchto agentur by mělo být hledání nejslabších článků v kybernetickém prostoru, zejména v oblasti energetiky, bankovnictví, dopravy a telekomunikace.

Důležitou částí, která by mohla být přínosná pro prevenci potenciálních kybernetických útoků, je zejména důkladná analýza a zmapování kybernetických útočníků, jejich zbraní v kybernetickém prostoru, cíle a případné další hrozby pro

možné budoucí kybernetické útoky. Bakalářská práce analyzuje současný stav, kybernetické útoky proběhlé v minulosti, jejich význam a dopad na společnost, dále řeší prevenci a bezpečnostní opatření, která je nutné přijmout, aby bylo nebezpečí kybernetických útoků sníženo na minimum. V další části je zmíněna právní legislativa v této problematice, názor společnosti a odborníků na boj s kybernetickým terorismem. Práce tak odhaluje hlavní struktury kybernetického terorismu, dopady kybernetických útoků v lokálním i globálním měřítku a popisuje bezpečnostní opatření proti kybernetickým útokům.

1 CÍLE A METODIKA BAKALÁŘSKÉ PRÁCE

Hlavním cílem bakalářské práce je celkové zhodnocení a vysvětlení kybernetického terorismu. Především pokusit se říci, jak a čím se liší aktéři, kteří se připravují nebo vedou kybernetický útok. Důležité je zjistit, na jaké úrovni pracují jak instituce, tak i jednotlivci, kteří také velmi často využívají způsob moderního boje. Dalším cílem je zhodnotit, jak jsou jednotliví aktéři schopni pracovat a reagovat na nenadálé skutečnosti, které je mohou potkat v páchání protizákonné činnosti. Bakalářská práce dále popisuje zbraně a prostředky použité v kyberprostoru. Jedná se z velké části především o technologické možnosti a finanční prostředky, které samotné útočníky přesně vymezují. Podstatnou věcí je také výběr cílů pro vedení kybernetického útoku. Mezi hlavní motivační prvky patří zejména politika, náboženství a finanční zisk.

Dílčím cílem je pokusit se popsat již proběhlé kybernetické útoky pomocí případových studií. Jsou zde tedy popsány útoky na servery vlády, bank, zpravodajské servery a kritickou informační infrastrukturu, která je tvořena zejména telekomunikacemi, dopravou, zpravodajstvím či energetikou. Zejména jsou zde zmíněna tzv. „slepá místa“ při odrážení kybernetických útoků. S tím souvisí i aktuální popis preventivních opatření jednotlivých ohrožených subjektů. Hlavními způsoby prevence jsou zejména protiteroristická politika, legislativa a preventivní bezpečností opatření.

Bohužel každá vyspělá země již čelila a neustále čelí mnoha druhům kybernetických útoků. Hrozba přímého kybernetického útoku na suverenitu každého jednotlivého státu je minimální, ve většině případů se jedná spíše o ohrožení jednotlivých složek v daném státu nebo špionážní využití v kyberprostoru.

Mezi hlavní prostředky, které by měly k účelu vyšší bezpečnosti posloužit, patří lepší spolupráce spřátelených zemí. A to zejména součinnost ve výměně informací týkajících se jednotlivých organizací, které jsou určeny k zastavování protiprávního jednání, a střeží tak správnou funkci státu a jeho jednotlivých součástí.

Zmíněná problematika je řešena v bakalářské práci za pomocí analýzy již známých skutečností, aktérů, zbraní a cílů kybernetických útoků, prostřednictvím dotazníkových šetření či řízených rozhovorů s odborníky. Využitím komparativní

metody jsou pak porovnány různé typy ochrany před kybernetickým terorismem, přičemž důležité je zjištění, jak efektivně můžeme s kybernetickým terorismem bojovat.

2 Aktéři

Naší ústřední problematikou je terorismus v kyberprostoru, a proto je zásadní pojmenovat aktéry, kteří jej zneužívají. Kybernetický terorismus je dělen na dvě základní složky, které tvoří největší nebezpečí. Postup je tedy takový, že všechny dané kategorie jsou v první fázi podrobeny důkladné analýze a zařazení do jednotlivých skupin. V další fázi jsou pak u každé skupiny určeny její největší přednosti v souvislosti s účelem a možnostmi využití a ideálním časovým obdobím.

2.1 Jednotlivci

Hrozby v rámci kybernetického terorismu plynou i z aktivit na individuální úrovni. Za kybernetického teroristu je považován jedinec, který se na promyšleném útoku proti počítačovým a informačním systémům, počítačovým programům a datům podílí nebo ho sám organizuje, čímž na straně nebojových cílů dochází k vytvoření ztráty. Mezi nejčastěji se vyskytující formy kybernetického zločinu jedince patří hacking, cracking, cyberstalking, piráctví, kybernetická pornografie a phreaking. Toto je však pouze zúžený výčet všech technik kybernetických zločinů jednotlivce. Podoba, ve které se nachází současný kybernetický zločin, prochází neustálou evolucí. Za primárního činitele ovlivňujícího rychlost vývoje kybernetického zločinu lze označit samotnou rychlost vývoje informační a komunikační technologie (ICT).[1]

Velký význam jednotlivce je v oblasti kybernetického terorismu spatřován zejména v možnosti pronajmutí schopného jedince pro tyto účely.[2] Zvolený jedinec však ve většině případů neprovádí útok úplně sám, ale pouze se podílí na vedení v oblasti, kterou bude schopen dostatečně pokrýt.

Příkladem útoku jednotlivce je incident z dubna 2007 v Estonsku, kdy došlo ke zničení velkého objemu dat ze serverů Národního úřadu pro letectví

[1] ABERLE, P. *Budoucnost kybernetického terorismu*, Brno, 2010. s. 13.

[2] JIROVSKÝ, V. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních*, Praha, 2007, s. 5

a kosmonautiku (NASA). Dalším příkladem je průnik hackera britské národnosti Garyho McKinnona do databáze Pentagonu z roku 2002.

V kontextu evoluce zůstává skupina jednotlivců v rámci kybernetického terorismu dlouhodobě tou nejzajímavější. Vývoj lze sledovat především v jejich úloze při přípravě realizaci útoků.[3]

2.2 Instituce

Aktéři (ekonomičtí, političtí, vojenští atd.) jsou obvykle členěny na mezinárodní organizace (doslovně chápané jako organizace více států), národní organizace (aktivistické sítě, některé obchodní korporace), organizace, které vyvíjejí činnost v rámci národních států a státy samotné.[4]

Dle provedených výzkumů jsou za nejzajímavější útočníky považovány právě národní organizace. Národní organizace jsou považovány nejenom za nejvhodnější cíle kybernetického terorismu, ale současně také za pachatele. Existence a efektivita těchto organizací je z největší míry podmíněna změnami ve způsobech zpracování předávání informací, tedy i přenosem strukturálního těžiště do větší blízkosti k novým komunikačním a informačním technologiím. Na tomto místě je také nutné zmínit, že tyto organizace jsou vůči snahám státu o zablokování či omezení jejich aktivit do značné míry imunní.[5]

Maxmilián Strmiska definuje státní terorismus jako politicky motivovanou a zdůvodňovanou metodu.[6] Státní terorismus je složen ze tří způsobů, prostřednictvím kterých se stát teroristických aktivit účastní:

a) Státní (nebo-li vládní) terorismus – je označováním situace, kdy je teroru vystaveno civilní obyvatelstvo (popř. je ze strany státu potlačováno). Státním

[3] ABERLE, P. *Budoucnost kybernetického terorismu*, Brno, 2010, s. 15.

[4] BARBER, R. *Hacking Techniques*,2003, č. 3, p. 9-10.

[5] BASTL, M. *Kybernetický terorismus: studie nekonvenčních forem boje v kontextu soudobého válečnictví,* Brno, 2007, s. 111.

[6] STRMISKA, M. *Terorismus a demokracie*. Brno: Masarykova univerzita, 2001, s. 14.

terorismem je tedy rozuměna aktivita vykonávaná státem ve státě. V oblasti terorismu kybernetického se jedná o cílené používání kybernetických nástrojů za účelem vyvolání zamýšleného efektu psychologického charakteru doprovázeného hrozbou fyzického násilí s využitím ICT. Tento způsob se nabízí především v případě států, jež se potýkají se separatistickými tendencemi, v případě autoritářských států a rozvrácených států. Souběžně se zvyšujícím se využíváním ICT se ve společnosti přímou úměrou zvyšuje také možnost zneužívání těchto nástrojů a technologií právě pro účely kybernetického terorismu. Vyšší výskyt státního terorismu se logicky předpokládá v zemích, kde je dostatečně vyvinutý ICT systém.

b) Státní účast – není na rozdíl od státního terorismu omezena pouze na vnitrostátní úroveň. Zvolené cíle jsou pro stát nebezpečné a mají široké spektrum (soukromí sektor, samotné státy i jednotlivci). Mnohdy bývá pojem státní účast spojován s pojmem kybernetická válka. To, že byl útok veden státní službou je velmi těžko prokazatelné. Je tomu tak díky rychlosti a anonymitě. Toto jsou také důvody toho, že doposud nebyl prokázán jediný útok, ve kterém by stát hrál hlavní roli. I přesto existují indicie, které pomáhají pochopit, jaký význam má při kybernetických útocích státní účast.

Státní sponzoring – tvoří třetí skupina, která je založena aktivitách teroristů, kterým připadne státní podpora (zejména v podobě jejich financování). Seznam zemí (např. Sýrie, Kuba, Írán, Súdán) sponzorujících terorismus byl zveřejněn roku 2009 americkým Ministerstvem vnitra. Možnost odhalení je i v tomto případě obtížná, protože v naprosté většině takových případů neexistuje přímý důkaz.[7]

Řada autorů se domnívá, že příprava na vedení kybernetické války realizovaná valnou částí technologicky vyspělých států povede k vývoji efektivních kybernetických zbraní.[8] Mnohdy je zmiňováno zejména riziko úniku technologie technologií výroby produktů samotných, jež by se mohly dostat na černý trh nebo do rukou potencionálních teroristů. Bez ohledu na to, zda by k takovému úniku nesmyslně či úmyslně (poskytnutí technologie např. státem ideologicky blízké teroristické skupině) došlo, je zřejmé, že

[7] ABERLE, P. *Budoucnost kybernetického terorismu*, Brno, 2010, s. 16 – 18.

[8] BASTL, M. *Kybernetický terorismus: studie nekonvenčních forem boje v kontextu soudobého válečnictví*, Brno, 2007, s. 93.

praktická demonstrace efektivity takových zbraňových systémů by mohla motivovat teroristy ke snaze o jejich získání či paralelní vývoj.

Z výše uvedených vyplívá, že v současnosti není možno do výčtu aktérů kybernetického terorismu zařadit kategorii stát, protože o přímém ani nepřímém zapojení státu do teroristických aktivit neexistují přesvědčivé důkazy, které by vedly ke ztrátám civilistů. Do budoucna je však sledování aktivit státu v této oblasti považováno za nezbytné.[9]

2.3 Dílčí závěr

Za kybernetického teroristu je považován jedinec, který se na promyšleném útoku proti počítačovým a informačním systémům, počítačovým programům a datům podílí nebo ho sám organizuje, čímž na straně nebojových cílů dochází k vytvoření ztráty. Mezi nejčastěji se vyskytující formy kybernetického zločinu jedince patří hacking, cracking, cyberstalking, piráctví, kybernetická pornografie a phreaking. Aktéři (ekonomičtí, političtí, vojenští atd.) jsou obvykle členěni na mezinárodní organizace, národní organizace, organizace, které vyvíjejí činnost v rámci národních států a státy samotné. Z toho vyplívá, že v současnosti není možno do útoku možné do výčtu aktéru kybernetického terorismu zařadit přímo kategorii stát, protože o přímém ani nepřímém zapojení státu do teroristických aktivit neexistují přesvědčivé důkazy.

[9] ABERLE, P. *Budoucnost kybernetického terorismu*, Brno, 2010, s. 18.

3 Kybernetické zbraně

V následné kapitole se seznámíme s nejpoužívanějšími nástroji – programy, které v minulosti byly využity nebo se stále využívají pro účely kybernetického terorismu. Největší důraz je obecně kladen na stále důkladnější sledování evoluce internetových služeb a nástrojů, díky nimž lze sledovat vzájemné propojení teroristických aktivit a informačně komunikačních technologií, které mají schopnosti vytvořit ztráty či riziko na straně nebojových cílů. K největším rozšíření těchto nástrojů došlo v průběhu 90. let 20. století, přesto o největším vrcholu můžeme hovořit kolem roku 2000, toto můžeme nazývat jako období Y2K. Bohužel s tímto obdobím byl spojen strach z neočekávaných událostí. Problém byl soustředěn na přechod s číslovkou větší než 1999. Mohla nastat vážná situace, kdy by informační systémy nemusely tento průběh zvládnout. Dokonce hrozilo selhání nadnárodních podniků, bank i letových provozů. Právě pro tyto důvody došlo k radikálním bezpečnostním krokům v oblasti ICT. Hosův katalog nabízí šest možných nástrojů nebo metod využívaných v rámci kybernetického terorismu: logické bomby, trojské koně, červy, back boory, viry, sniffery.[10]

3.1 Vymezení nástrojů zneužívaných pro kybernetický terorismus

Nejznámější jsou **viry**, jež se současně uplatňují v kybernetickém terorismu dlouhodobě. Lze je definovat jako kódy, jež explicitně a rekurzivně kopírují potencionálně se vyvíjející verze sebe sama. Ale také kódy, které šíří sami sebe. Viry jsou obvykle šířeny proti vůli uživatele, což nepopírá jeho případná spolupráce.

Viry v podobě kódů šíří své kopie nebo sami sebe, a to tak že infikují systémové prvky nebo soubory nebo mění odkazy na tyto objekty. Poté co převezmou kontrolu, se začnou v dílčích generacích opět množit.[11].[12]

[10] HOS, M. *Terorismus a počítače. In. Terorismus a my*. Praha, 2001, s. 79.

[11] BIČIANOVÁ, A. *Kybernetický terorizmus a počítačová kriminalita*, Zlín, 2008, s. 89.

[12] SZOR, P. *Počítačové viry: analýza útoku a obrana*, Budapešť, 2006, s. 45.

Viry, jež jsou šířeny sítěmi, se primárně nazývají počítačoví červi (síťový vir). Některé z nich však používají metodu infikování souborů jako vedlejší způsob svého rozmnožování. Červy tedy na základě výše uvedeného lze označit jako poddruh počítačových virů. Na vzdáleném počítači se tyto červy obvykle spouštějí bez zásahu uživatele (opakem jsou červi, kteří se šíří pomocí e-mailů, kde je pomoc uživatele nutnosti). Samotné červy lze rozdělit do tří stěžejních skupin:

a) červy rozesílají e-maily (hromadně i jednotlivě),

b) králíci, jež jsou zvláštním druhem počítačového červa, jde o programy existující pouze v jedné kopii a to v každém okamžiku. Tato kopie se pak kopíruje sítěmi spojených počítačových hostitelů.

c) chobotnice je druh počítačového červa, kterého tvoří sada více programů rozmístěných ve větším množství počítačů v síti (více než v jednom). Příklad je, že na jednom počítači je nainstalovaná „hlava“ a na druhém „ocas“, ty pak spolu vzájemně komunikují a provádějí nějakou funkci. Chobotnice není příliš častá, ale její rozkvět se dá do budoucna předvídat.

Počítačový červ obvykle vystupuje jako samostatný program, který nepotřebuje hostitele. Zde je nutné dodat, že tento typ programů svojí charakteristikou neodpovídá virům. Lze jej tedy spíše považovat za variantu svébytné třídy útočných nástrojů.[13].[14] **Logickou bombou** je označována úmyslná chyba programátora v rámci softwaru. Jde o naprogramovanou chybu běžného programu. Tato chyba při splnění podmínek, které jsou předem definované, provede akci, která je nejen nežádoucí ale také nedokumentovatelná. Aplikace se kupříkladu sama smaže po určitém počtu spuštění z disku a to jako součást schématu ochrany před kopírováním nebo může dojít k naprogramování dalších druhů škodlivých kódů, které budou provedeny pro případ kopírování. Kód logické bomby bývá v mnoha případech ukrytý mezi zdrojovými kódy daného programu.

[13] BIČIANOVÁ, A. *Kybernetický terorizmus a počítačová kriminalita*, Zlín, 2008, s. 90.

[14] SZOR, P. *Počítačové viry: analýza útoku a obrana*, Budapešť, 2006, s. 45.

Častým příkladem logických bomb jsou tzv. velikonoční vajíčka, kdy jde o skryté kódy, které si najdou cestu i do největších softwarových projektů. Typickým příkladem výskytu logické bomby v praxi byla hra známá z mobilních telefonů Nokia série 60 (hra Mosquitos). Obsahem hry bylo mimo jiné zabudovaná funkce, která byla původcem odesílání SMS zpráv do zpoplatněných linek. V rámci prvních verzí programu byla tato funkce součástí ochrany proti kopírování, došlo však bohužel k jejímu selhání, protože se nechovala dle záměru jejich autorů. Následkem toto došlo k odstranění tohoto kódu z následujících verzí tohoto programu (došlo také k deaktivaci zpoplatněných linek).[15].[16]

Program, který vytváří dojem užitečnosti (snaží se uživatele něčím zaujmout, aby neodolal a spustil jej na svém počítači) nebo předstírající jiné funkce (jako kamufláž svých aktivit), než kterými ve skutečnosti disponuje, nese název **trojský kůň.** Tento nástroj kybernetického terorismu není schopen sebereprodukce a šíří se samostatně. Není schopen ani modifikace běžného programu, tak aby byl schopen dodatečné nežádoucí a nedokumentované funkce. Trojský kůň je nejjednodušším druhem škodlivého programu. Primárním účelem trojských koňů bývá usnadnit či umožnit neautorizovaný průnik. Mezi jeho základní funkčnosti patří kradení hesel a tzv. backdoor. Kradení hesel spočívá v prohledávání systému a odesílání nalezených hesel útočníkovi. Od 90. let minulého století bývají mnohdy kombinovány s keyloggery (programy, které na napadeném počítači zaznamenávají stisknuté klávesy).[17] Tento nástroj je nejoblíbenějším hackerským do volně stáhnutelného kódu utility. Tento nástroj slouží k nejrůznějším účelům (např. monitorování činnosti cílového počítače, zneužití pro útok DoS, atd.). Zajímavou variantou trojského koně je *„Data Mining"* (jde o programy, které monitorují po nainstalování činnost uživatele). Ve své podstatě existují dva druhy trojského koně. Prvním je situace, kdy je 100 % kódu trojského koně snadno analyzovatelné. Ve druhém případě vzniká trojský kůň pečlivou modifikací originálního programu s dostatečně přidanou funkčností, která se řadí do podskupiny tzv. zadních vrátek nebo do sady pro administrátorský přístup. S největší

[15] BASTL, M. *Kybernetický terorismus: studie nekonvenčních forem boje v kontextu soudobého válečnictví*, Brno, 2007, s. 90.

[16] SZOR, P. *Počítačové viry: analýza útoku a obrana*, Budapešť, 2006, s. 46 – 47.

[17] BASTL, M. *Kybernetický terorismus: studie nekonvenčních forem boje v kontextu soudobého válečnictví*, Brno, 2007, s. 90.

pravděpodobností je neznámějším trojským koněm AIDS TROJAN DISK, který byl prostřednictvím diskety odeslán cca na 7 000 adres výzkumných organizací v rámci celého světa. Po zavedení tohoto trojského koně, došlo v systému k přeházení pojmenování veškerých souborů za současného zcela zaplnění prázdného místa na disku. Následné obnovení dat bylo pak nabízeno za finanční úplatu. Tímto počinem došlo ke zrodu nového oboru nesoucího název škodlivá kryptografie. Krátce po vypuknutí tohoto incidentu byl autor trojského koně dopaden a byl odsouzen (J. Poppov, 39 let, zoolog ve státě Ohio).[18].[19]

Termín **backdoor** mnohdy označovaný jako **zadní vrátka** (výstižný název pro kódy, které po instalaci do cílového počítače umožňují jeho vzdálené řízení). Backdoor je pro hackery nástrojem číslo jedna. Objeví-li hacker *„díru"* v bezpečnosti, jeho dalším počínáním je nainstalování backdoor. Není-li tento nástroj často používán, pak je jeho odhalení velmi náročným procesem. Komunikace s nástrojem napadeného počítače probíhá za pomoci spuštěné služby na portu s vysokým číslem anebo je maskovaná jako standardní služba anebo telnet. Výše jmenované služby ve většině případů neodfiltrují ani firewally. Stávají se tedy přístupnými i přes bezpečnostní prvky sítě. Jistý komunikační komfort a lepší ukrytí komunikace využívá dnes moderní backdoor prostřednictvím interaktivních nástrojů jako je například ICQ nebo MSN messenger.[20]

Sniffer [21] (v angličtině znamená čichat, čenichat nebo čmuchat) lze označit jako program, který kvalitně odposlouchává síťový provoz (čmuchající co se kde děje). Nelze jej označit přímo za nástroj útoku, ale spíše za prostředek, který je využíván ke shromáždění informací pro jeho přípravu. Pro získání potřebných informací je stěžejní jeho umístění v síti. Problematické je jeho použití v přepínaných sítích, kde je společný segment minimalizovaný. Funkce snifferu je jednoduchá. Ve své podstatě jde o přepnutí síťového rozhraní do tzv. promiskuitního módu. Tím umožní příjem veškerých paket, které se pohybují na síti (bez jakékoli další filtrace). Pakety jsou zaznamenávány a stále více analyzovány (IP adresy, typ protokolu, MAC adresy atd.). Takto je pak možné

[18] BIČIANOVÁ, A. *Kybernetický terorizmus a počítačová kriminalita*, Zlín, 2008, s. 27.

[19] SZOR, P. *Počítačové viry: analýza útoku a obrana*, Budapešť, 2006, s. 47.

[20] BIČIANOVÁ, A. *Kybernetický terorizmus a počítačová kriminalita*, Zlín, 2008, s. 24 – 25.

[21] BIČIANOVÁ, A. *Kybernetický terorizmus a počítačová kriminalita,* Zlín, 2008, s. 25.

odposlouchávat komunikaci v síti a zachytit otevřeně přenášené citlivé údaje a hesla.[22].[23]

Mezi škodlivý software lez dále zařadit také **dialery** (jde o programy, jež vytáčejí u napadených počítačů připojených skrze modem na telefonní síť předem zvolená čísla. K jejich významnému rozšíření došlo v době, kdy začalo být vytáčené připojení široce dostupné domácnostem. Účelem je uživatele donutit k tomu, aby zaplatil za použití telefonních linek se speciálním cenovým tarifem. Vyskytují se především u porno dealerů, kdy dochází k informování uživatele o tom, že pro spojení bude použito jiné telefonní číslo, ale již není informován o budoucí ceně tohoto hovoru. Obdobný způsob je využíván i u webových stránek, které uživatele odkazují na placené služby).

Downloadery, nelo-li tzv. stahovače (jde o škodlivé programy, jež instalují na napadený počítač nové programové položky. Do systému se nejčastěji dostává jako příloha e-mailu. K napadení dochází po jeho stažení, rozpakování a spuštění). **Injektory** (jde o zvláštní druh dropperů, které většinou instalují do paměti počítače kód viru. Mnohdy jsou injektory využívány k procesu nesoucímu název seeding (rozsévání), což je proces, při němž dochází k vložení viru injektorem do velkého množství systémů. Díky tomuto může vypuknout náhlá epidemie).[24]

Droppery (jde oprogramy, jež vsazují např. do napadeného počítače jiný software – vystupují jako mezičlánek útočného procesu). **Rootkity** (jde o sady programů nebo samostatné programy, jejichž používání začíná až po ovládnutí systému, který je napaden. Plní účel skrytí útočníkovi činnosti uskutečňované na operačním systému, zakrytí stop útoku a umožnění kontinuálního ovládání systému, který je napaden. V podstatě jde o podskupinu backdoors. Mají velmi podobnou funkci. V praxi

jde většinou o běžně používané programy (např. ps, top, inetd), které jsou modifikované tak, že administrátor nic nepozná a hacker disponuje neomezeným přístupem).

[22] BIČIANOVÁ, A. *Kybernetický terorizmus a počítačová kriminalita*, Zlín, 2008, s. 25.

[23] JIROVSKÝ, V. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních,* Praha, 2007, s. 33.

[24] BASTL, M. *Kybernetický terorismus: studie nekonvenčních forem boje v kontextu soudobého válečnictví*, Brno, 2007. s. 91.

Programy na spam (jde o programy předurčené k rozšiřování pošty, která je nevyžádaná a to prostřednictvím instant Messenger, e-mailů apod.) [25.26] Mezi čistě útočný software lze zahrnout kategorie **auto-rooterů**, kdy se jedná o nástroje, které k automatizovanému průniku využívají exploity (mnohdy jde o skripty). Exploit zde vystupuje jako soubor zranitelností určité aplikace (popř. systému) nebo kód, který mádemonstrovat konkrétní zranitelnost. Lze jej využít zejména k útoku proti nezabezpečenému cíli. Zajímavostí je, že tento čistě útočný software mohou využívat také lidé, kteří mají v ICT oblasti jen malé vzdělání. Dále sem lze zahrnout **DoS attackery**, což jsou programy určené k útoku, který je cíleně zaměřen na odepření služby, nástroje určené k útoku v rámci konkrétních systémů, aplikací nebo zařízení (jež využívají konkrétní sady zranitelnosti či konkrétní zranitelnost). Zajímavou skupinou jsou také tzv. **floodery**, což jsou programy s jejichž pomocí dochází ke generování masivního síťového provozu, který způsobuje zahlcení systému. Což vede k DoS (útok odmítnutím služby), je-li tento útok veden z mnoha napadených systémů současně (tzv. zombie stroje) nazýváme je útokem DDoS (distribuovaný útok zaměřený na odmítnutí služby).

Závěrem lze zmínit také **kity** (generátory virů), jež jsou obdobným nástrojem jako autorootery, v tomto případě určené či zaměřené na vytváření, designování nových virových variant. Zde lze opět dodat, že není potřebná příliš velká znalost v ICT oblasti.[27.28]

Poslední kategorie internetových škůdců nemusí být záměrně škodlivá, avšak i přesto svým uživatelům může působit nepříjemnosti. Z tohoto důvodu i proti ní dnes existují antispamové a antivirové prostředky. Patří sem například zábavné programy, které nebývají škodlivé.

---

[25] BASTL, M. *Kybernetický terorismus: studie nekonvenčních forem boje v kontextu soudobého válečnictví*, Brno, 2007, s. 92.

[26] BIČIANOVÁ, A. *Kybernetický terorismus a počítačová kriminalita*, Zlín, 2008, s. 26.

[27] BASTL, M. *Kybernetický terorismus: studie nekonvenčních forem boje v kontextu soudobého válečnictví*, Brno, 2007, s. 92.

[28] SZOR, P. *Počítačové viry: analýza útoku a obrana*, Brno, 2006, s. 51.

Zábavné programy zasahují tím způsobem, že přerušují či mění běžné chování počítače, čímž působí rušivým a nepříjemným dojmem. Instalací těchto programů se baví například kolegové v práci. Příkladem je spořič obrazovky blokující systém apod.

Dalším typem jsou **řetězové dopisy**, jež šíří poplašné zprávy o hrozící počítačové infekci, či sbírce na operaci pro velmi nemocné dítě, za současného popudu pro ostatní příjemce, aby zprávu poslali dál.[29]

Dále sem lze zařadit také **spyware**. Jde o program, který sbírá informace o uživatelích (bez vědomí uživatele) a odesílá je přes internet firmám. Odcizovány jsou pouze data statistická a to jako přehled navštívených stránek či nainstalovaných programů. Činnost tohoto charakteru je zdůvodňována snahou zjistit zájmy a potřeby uživatele a získané informace následně využít pro cílenou reklamu. Možnost nezneužití technologie či informací nelze však nijak zaručit. Právě z tohoto důvodu je velké množství uživatelů rozhořčeno existencí a legálností spyware. Na závěr lze zařadit také **adware.** Jde o produkt znepříjemňující práci s počítačem reklamou. Příkladem může být vyskakující pop-up reklamní okna při surfování po internetu v souvislosti s vnucování určitých stránek, o které však uživatel nemá zájem.[30] Obě tyto aplikace jsou mnohdy hlavním zdrojem příjmů různých internetových obchodů. V zájmu jejich původců tedy je, aby je antivirové programy vůbec nedetekovaly.

[29] SZOR, P. *Počítačové viry: analýza útoku a obrana*, Brno, 2006, s. 52 – 53.

[30] HÁK, I. *Moderní počítačové viry*, Hradec Králové, 2005, s. 15.

3.2 Dílčí závěr

Tato kapitola podrobně charakterizuje šest nástrojů nebo metod využívaných v rámci kybernetického terorismu: logické bomby, trojské koně, červy, back boory, viry, sniffery. Již méně podobně popisuje další škodlivý software (downloadery, dealery, injektory, rootkity, droppery a programy na spam). Dále také čistý útočný software (auto-rootery, DoS attackery, floodery a kity. Jako poslední je popisována kategorie internetových škůdců, jež nemusí být záměrně škodlivý, avšak i přesto svým uživatelům můžou působit nepříjemnosti (zábavné programy, řetězové dopisy, spyware a adware).

Díky vzrůstajícímu významu ICT ve všech oblastech života vzniká nové pole působnosti pro kybernetický terorismus. Nástroje nejsou však výsadou jedinců nebo institucí, které jej zneužívají pro kybernetický terorismus. Jde o běžně využívané nástroje, které mají pro své použití v kybernetickém terorismu zcela nový rozměr.

Lze říci, že při současných bezpečnostních opatřeních jsou odráženy běžně prováděné útoky. Nárůst inovativních nástrojů však nelze brát na lehkou váhu. V současné době se inovace bezpečnostních opatření jeví jako nejlepší možná ochrana proti kybernetickému terorismu.

4 Cíle útoků - kritická informační infrastruktura

Předpoklad kybernetických útoků, aby ohrozily co nejširší spektrum civilního obyvatelstva, jsou cíleny na ty místa v kyberprostoru, která mají velký potenciál v případě své nefunkčnosti způsobit maximální možné ohrožení v reálném světě. Prvotně však musíme rozdělovat termíny kybernetického terorismu a kybernetického zločinu. Kybernetický zločin je specifický tím, že neútočí na nebojové cíle, kybernetický terorismus ano.

Za nejpravděpodobnější cíle kybernetického terorismu bývají nejčastěji uváděny objekty kritické informační infrastruktury (KII). Propojení infrastruktury, která zajišťuje každodenní fungování společnosti a udržuje životní standard prostřednictvím komunikačních a informačních technologií, vytváří širokou paletu hrozeb, které mohou přijít z lokálního i globálního kybernetického prostoru. Nejzávažnější hrozbou pro kritickou informační infrastrukturu, která patří do skupiny nových globálních hrozeb 21. století, je kyberterorismus. Na něj se v posledních letech stále více zaměřuje pozornost bezpečnostních informačních služeb.

V posledních letech se výrazně v krizovém managementu českého státu změnil pohled na celou řadu bezpečnostních hrozeb. Svědčí o tom i přijetí zákona o kybernetické bezpečnosti (zákon č. 181/2014 Sb.) a prováděcích vyhlášek k němu, účinných od 1. 1. 2015, které mnohem rozsáhleji a komplexněji než v původní podobě z roku 2007 definují kritickou informační infrastrukturu (KII) a také systém opatření na její ochranu. Z nich vychází i pojetí struktury KII, prezentované v této bakalářské práci.

Jedním z dílčích cílů této bakalářské práce je na základě nových právních norem charakterizovat současný a budoucí stav ochrany kritické informační infrastruktury a zajištění kybernetické bezpečnosti v ČR.

4.1 Struktura kritické informační infrastruktury

Kritická informační infrastruktura je součástí kritické infrastruktury, jejíž ochranou se zabývá krizové řízení a civilní nouzové plánování. Základní pojmosloví je definováno v tzv. krizovém zákoně a podrobněji specifikováno v dalších právních

předpisech (vyhláškách, nařízeních vlády a prováděcích směrnicích). Prvním dnem ledna 2015 vstoupil v účinnost zákon č. 181/2014 Sb. o kybernetické bezpečnosti a prováděcí předpisy k němu - vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích a vyhláška č. 316/2014 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti). Součástí nových právních předpisů je i novelizace nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury.

V novém zákoně o kybernetické bezpečnosti je kybernetická informační infrastruktura definována jako prvek nebo systém prvků kritické infrastruktury v odvětví komunikační a informační systémy v oblasti kybernetické bezpečnosti.[31] V zákoně je současně prostředí KII vymezeno jako kybernetické prostředí, pod kterým se rozumí digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy, a službami a sítěmi elektronických komunikací.[32]

Strukturní prvky kritické informační infrastruktury jsou definovány příslušnou vyhláškou o kritériích pro určení prvku kritické infrastruktury. Samotné vymezení prvků KII se postupem času vyvíjelo a rozšiřovalo, jak je znázorněno v porovnání v tabulce 1.

[31] §2, odst.b) zákona č. 181/2014 Sb. o kybernetické bezpečnosti

[32] §2, odst.a) zákona č. 181/2014 Sb. o kybernetické bezpečnosti

Tabulka 1: Vývoj pojetí prvků struktury KII 2007 – 2014

Název prvku kritické infrastruktury	**Oblasti kritické infrastruktury České republiky podle Usnesení bezpečnostní rady státu č. 30/2007**	**Nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury**	**Nařízení vlády č. 315ze dne 8. prosince 2014,kterým se mění nařízení vlády č. 432/2010 Sb.,o kritériích pro určení prvku kritické infrastruktury**
VI. Komunikační a informační systémy	6.1 Služby pevných telekomunikačních sítí	A. Technologické prvky pevné sítě elektronických komunikací (Centrum řízení a podpory sítě, řídící ústředna, mezinárodní ústředna, tranzitní ústředna, datové centrum, telekomunikační vedení)	A. Technologické prvky pevné sítě elektronických komunikaci (centrum řízení a podpory sítě, řídící ústředna, mezinárodní a tranzitní ústředna, datové centrum, telekomunikační vedení)
	6.2 Služby mobilních komunikačních sítí	B. Technologické prvky mobilní sítě elektronických komunikací (centrum řízení podpory, ústředna mobilní sítě, základnová řídící jednotka sítě pokrývající strategickou lokalitu, základnová jednotka sítě pokrývající strategickou lokalitu)	B. Technologické prvky mobilní sítě elektronických komunikací (centrum řízení a podpory sítě, ústředna mobilní sítě, základnová řídící jednotka a základnová stanice sítě pokrývající strategickou lokalitu, datové centrum)

	6.3 Radiová komunikace a navigace	C. Technologické prvky sítí pro rozhlasové a televizní vysílání (vysílací zařízení pro šíření televizního a rozhlasového signálu pro informování obyvatelstva za krizových situací, řídící pracoviště provozu, datové centrum, síť pro RTV)	C. Technologické prvky sítí pro rozhlasové a televizní vysílání (vysílací zařízení pro šíření RaTV signálu určených pro informaci obyvatelstva za krizových situací s vysílacím výkonem nejméně 1kW k zajištění provozu RTV veřejnoprávního provozovatele, řídící pracoviště provozu, datové centrum, síť pro RTV k zajištění provozu veřejnoprávního provozovatele)
	6.4 Satelitní navigace	D. Technologické prvky pro satelitní komunikaci (hlavní pozemní satelitní přijímací a vysílací stanice, pozemní řídící a komunikační středisko, pozemní propojovací síť)	D. Technologické prvky pro satelitní komunikaci (hlavní pozemní přijímací a vysílací stanice, Evropský globální družicový navigační systém, pozemní řídící a komunikační středisko, pozemní propojovací síť)
	6.5 Televizní a radiové vysílání	E. Technologické prvky pro poštovní služby (centrální regionální výpočetní	E. Technologické prvky pro poštovní služby (centrální a regionální výpočetní

		středisko, středisko centrálního snímání a úložiště dat, sběrný přepravní uzel, řídící a mezinárodní pošta, poštovní dopravní infrastruktura)	středisko, středisko centrálního snímání a úložiště dat, sběrný přepravní uzel, řídící a mezinárodní pošta, poštovní dopravní infrastruktura)
	6.6 Poštovní a kurýrní služby	F. Technologické prvky informačních sítí (řídící centrum, datové centrum, síť elektronických komunikací, technologický prvek zajišťující provoz registru doménových jmen CZ a zabezpečení provozu domény CZ nejvyššího stupně	F. Technologické prvky informačních sítí (řídící centrum, datové centrum, síť elektronických komunikací, technologický prvek zajišťující provoz registru doménových jmen CZ a zabezpečení provozu domény CZ nejvyššího stupně
	6.7 Přístup k internetu a datovým službám		G. Oblast kybernetické bezpečnosti (informační nebo komunikační systém, který zcela nebo významně ovlivňuje činnost prvku kritické infrastruktury a jehož nahrazení je nepřiměřeně nákladné anebo kdy jeho výpadek přesahuje 8 hodin, informační systém orgánu veřejné moci, který spravuje údaje o více jako 300

			000 osobách, komunikační systém zajišťující připojení nebo propojení prvku kritické infrastruktury s garantovanou datovou přenosovou rychlostí nejméně 1Gbit/s.,

Zdroj: vlastní zpracování podle zdrojů v záhlaví tabulky

I když je kritická informační infrastruktura chápána jako subsystém kritické infrastruktury, je na ni v době masového využívání komunikačních a informačních systémů možné pohlížet v širším pojetí i jako na informační a komunikační prostředí, které je předpokladem fungování celého systému krizového řízení a civilního nouzového plánování. Vzhledem k důležitosti KII je v činnosti orgánů krizového řízení velká pozornost ochraně KII a významných informačních systémů před ohroženími různého druhu, ať už úmyslnými nebo neúmyslnými (nedbalostními). Za významný informační systém se považuje takový, který spravuje orgán státní moci, který ale není kritickou informační infrastrukturou, ale u něhož by v případě bezpečnostního incidentu mohlo dojít k výkonu funkcí veřejné správy.[33]

4.2 Úmyslné ohrožení kritické informační infrastruktury

Ohrožení bezpečnosti kritické informační infrastruktury (obecněji ohrožení kybernetické bezpečnosti) má celou řadu podob. V nejjednodušším členění se dají rozdělit do dvou skupin: úmyslné a neúmyslné ohrožení bezpečnosti kritické infrastruktury. V obou skupinách se pak dají detekovat aktivní a pasivní útoky na bezpečnost kritické informační infrastruktury. Aktivní útoky jsou obvykle zaměřeny na získání informací z informačních systémů, modifikaci datových toků a ovlivnění systémových prostředků informačních systémů, provozovaných v rámci KII. Pasivní útoky využívají převážně monitorování provozu informačních systémů a odkrývání

[33] Viz §2 zákona č. 181/2014 Sb. o kybernetické bezpečnosti

zpráv. Zatímco aktivní útoky jsou detekovatelné ihned anebo s malým zpožděním, pasivní útoky na kritickou informační infrastrukturu se detekují obtížně a často i s větším zpoždění. Všechny tyto případy útoků proti kritické informační struktuře patří do skupiny úmyslných ohrožení.

K nejzávažnějším úmyslným ohrožením KII patří v 21. století nová bezpečnostní hrozba, za kterou je považován kyberterorismus.

V odborné literatuře se všeobecně přijímá definice terorismu podle D. E. Deninga. Kyberterorismus je konvergencí terorismu a kyberprostoru obecně chápaný jako nezákonný útok nebo nebezpečí útoku proti počítačům, počítačovým sítím a informacím v nich skladovaným v případě, že útok je konán za účelem zastrašit nebo donutit vládu, nebo obyvatele k podporování sociálních nebo politických cílů.[34] V této definici se víceméně akcentuje pojetí kyberterorismu jako útoku proti KII, jehož cílem je získat informační nadvládu. Dále můžeme kybernetický terorismus definovat jako představitele aktivit vedených nebo koordinovaných státem s cílem získat informační převahu nebo vyřadit technologickou infrastrukturu protivníka.[35] V posledních letech byly ale ve světě i v ČR zaznamenány kyberteroristické útoky, jejichž cílem nebylo získání informační nadvlády, ale především narušení funkčnosti nebo poskytování služeb konkrétním informačním systémem, aniž by byl tento útok ze strany hackivistických skupin spojován s konkrétními politickými požadavky nebo propagací určitých politických ideologií.

Literatura, která se zabývá počítačovou kriminalitou, podrobně popisuje řadu konkrétních forem kyberterorismu. V. Jirovský jako základní formy identifikuje hacking, kybernetické výpalné, šíření materiálů se závadným obsahem, zneužití internetových stránek, sparing, warez, cracking, sniffing a cybersquatting.[36]

V posledních letech se v kyberprostoru zaznamenává stále větší počet kyberteroristických útoků, které jsou zaměřeny na tzv. odepření služby (Denial of Service – DoS: Distributed Denial of Sevices – DDoS). Tyto útoky jsou zaměřeny

[34] JANOUŠEK, M. Kyberterorismus: terorismus informační společnosti. *Obrana a strategie,* 2006, č. 2, roč. 6. s. 60-66.

[35] McQUADE III., Samuel. Encyclopedia of Cybercrime. Westport : Greenwood, 2008. s. 182.

[36] JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*, Praha, 2007, s. 45.

buďto na konkrétní počítač anebo na konkrétní síť, jejichž cílem není získat data anebo přístup do informačního, ale jen z provozu vyřadit určitou službu anebo celou síť. Princip útoku je poměrně jednoduchý a spočívá v zahlcení serveru velkým počtem žádostí o připojení v krátkém časovém úseku, což pak znemožní jeho správné fungování anebo vede ke kolapsu.

4.3 Neúmyslné ohrožení kritické informační infrastruktury

Neúmyslné ohrožení kritické informační infrastruktury a informační infrastruktury společnosti obecně je nejčastěji způsobeno lidským faktorem nebo technologickým selháním. Je poměrně těžko ovlivnitelné a předvídatelné. Podle údajů společnosti AEC Data Security, která patří k předním dodavatelům bezpečnostních řešení v oblasti IS/IT, tradiční nástroje počítačové bezpečnosti přestávají být účinné vůči nejnovějším kybernetickým hrozbám. Historicky budovanou bezpečnost na perimetru dnes musí doplňovat také zabezpečení vnitřní sítě. Ze strany vlastních uživatelů totiž dle statistik pochází přes 70 % útoků. [37]

V. Jirovský při klasifikaci neúmyslných ohrožení informační infrastruktury jako hlavní vidí tyto hrozby na straně lidského faktoru:

- nerozpoznání hrozby;
- nedokonalá normativní báze;
- slabá bezpečnostní kultura organizace;
- kooperující partneři a zaměstnanci;
- nedokonalá ochrana proti úniku informací.[38]

Ve všeobecné rovině na straně lidského faktoru svou roli často při ohrožení informační infrastruktury může hrát také nedostatečná kvalifikace, velké pracovní zatížení a nedostatečný počet zaměstnanců, které mohou dříve nebo později způsobit kybernetickou bezpečnostní událost nebo incident.

---

[37] *AEC Produkty*. [online]. [cit.2015-02-03]. Dostupné z WWW: <http://www.aec.cz/cz/produkty>.

[38] Viz JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*, Praha, 2007, s. 72.

Proti hrozbám, ať už úmyslným nebo neúmyslným, se vytváří systém ochrany kritické informační infrastruktury, který zahrnuje organizační a technická opatření.[39] Jejich cílem je především snížení zranitelnosti a zvýšení odolnosti kritické informační infrastruktury. V ochraně kritické informační infrastruktury je prvním krokem monitorování a identifikace bezpečnostních hrozeb, jimiž se v soustavě subjektů zajištění kybernetické bezpečnosti zabývají zpravodajské služby.

4.4 Využití zpravodajských služeb v kritické informační infrastruktuře

V posledních letech byly ve světě zaznamenány stovky mezinárodně koordinovaných kyberteroristických útoků na informační sítě vlád, ministerstev, armády, zpravodajských služeb a dalších strategických prvků státního organismu (např. bankovnictví a energetika, doprava). I když ve většině zemí existují specializované státní orgány pro zajištění kybernetické bezpečnosti, ukázalo se, že je potřebné boj proti kyberterorismu v různých podobách koordinovat. Příkladem koordinovaného přístupu státních orgánů jsou USA. V USA byl v systému krizového řízení nově vytvořen samostatný útvar United States Cyber Command. Ten je součástí strategického velení (U.S. Strategic Command) a přímo jej jako další útvary řídí Národní bezpečnostní agentura (NSA), která koordinuje bezpečnostní síly, výzvědnou a kontrarozvědnou činnost a předkládá návrhy na opatření v oblasti kybernetické bezpečnosti přímo prezidentovi USA.[40]

V Evropské unii existuje evropská agentura ENISA (Evropská agentura pro informační a síťovou bezpečnost), která vznikla v roce 2004. Tato agentura má na rozdíl od americké agentury víceméně poradenské a konzultační zaměření a není přímo propojena na unijní bezpečnostní a zpravodajské služby.

V České republice do roku 2011 byly otázky kybernetické bezpečnosti v kompetenci ministerstva vnitra. Usnesením vlády ČR č. 781 ze dne 19.10.2011 se hlavním gestorem za problematiku kybernetické bezpečnosti a současně národní autoritou pro tuto oblast stal Národní bezpečnostní úřad a také do jeho kompetence přešla národní agenda ENISA. Ve struktuře národního bezpečnostního úřadu je zřízeno

[39] Viz § 5 zákona č. 181/2014 Sb. o kybernetické bezpečnosti.

[40] CLARKE, R. *Cyber war*. New York : Harper Collins, 2011, s. 115-118.

Národní centrum kybernetickou bezpečnost a vládní Computer Emergency Response Team (CERT). Jako poradní orgán v ČR působí Rada pro kybernetickou bezpečnost (RKB).

České zpravodajské služby (Vojenské zpravodajství, Bezpečnostní informační služba, Úřad pro zahraniční styky a informace) ze zákona přímo odpovědnost za zajištění kybernetické bezpečnosti nemají. Protože je ale jejich úkolem shromažďování a vyhodnocování informací a identifikace aktuálních a potencionálních bezpečnostních hrozeb a jejich nositelů, je logické, že do jejich zájmové sféry bude patřit kyberprostor a kybernetická bezpečnost. O sílícím zájmu zpravodajských služeb o tuto zájmovou sféru svědčí i jejich každoroční výroční zprávy.

Ve výročních zprávách Vojenského zpravodajství je problematika kybernetické bezpečnosti v širším měřítku a bezpečnosti určitého prvku kritické informační infrastruktury sledována především z hlediska zajištění vnější bezpečnosti ČR a kybernetické bezpečnosti fungování rezortu a také z hlediska bojových operací, vedených v kyberprostoru.

Úřad pro zahraniční styky a informace ve své práci důsledně dodržuje princip utajení a ochrany zdrojů, metod a prostředků získávání informací a veřejně přístupné zprávy o své činnosti nezpracovává.

Bezpečnostní informační služba se zaměřuje především na monitorování a odhalování hrozeb pro český kyberprostor v souvislosti s politickým extremismem, mezinárodním kyberterorismem a mezinárodním organizovaným zločinem. Podle jejího zjištění a detekovaných útoků v českém kyberprostoru vůči státním orgánům za rok 2013 je znepokojivé, že se na území ČR zformovaly skupiny osob disponující schopnostmi a motivací provádět počítačové útoky, které mohou být použity i proti významnějším cílům, než jsou webové stránky veřejných činitelů.[41] Aktivity bezpečnostní informační služby byly zaměřeny v oblasti kybernetické bezpečnosti kritické informační infrastruktury především na identifikaci zranitelnosti a bezpečnostních nedostatků a rizik v komunikačních a informačních systémech ústředních orgánů státní správy, bezpečnostních složek a složek integrovaného

[41] *Výroční zpráva Bezpečnostní informační služby za rok 2013*. BIS. [online]. [cit.2015-02-05]. Dostupné z WWW: <http://www.bis.cz/n/2014-10-27-vyrocni-zprava-2013.html>.

záchranného systému. Prognóza hrozeb kybernetické bezpečnosti nejen v oblasti KII pro rok 2014 očekávala pokles aktivit domácích hacktivistických a souvisejících hackerských skupin. Tato hnutí jsou názorově nesourodá a postrádají silnější osobnosti či vedení, které by jim umožnilo získat více příznivců mezi lidmi s pokročilými znalostmi IT. Je možné, že se tyto skupiny budou snažit získat si pozornost veřejnosti podnikáním jednoduchých DDoS či defacement útoků. Zahraniční zpravodajské služby a hackeři budou nadále usilovat o získání informací z významných informačních systémů, přičemž lze očekávat, že k cíleným útokům na jejich uživatele bude stále více a sofistikovanějším způsobem zneužíváno informací dostupných prostřednictvím sociálních sítí a otevřených zdrojů.[42] Přesnost této prognózy bude možné ověřit až ve výroční zprávě za rok 2014, která bude zveřejněna ve druhé polovině letošního roku.

4.5 Prognóza kritické informační infrastruktury

Prognóza vývoje kritické informační infrastruktury a její ochrany má dvě dimenze. První je strategicko-politická, druhá je technologická, kterou se tato práce nebude zabývat. Nové přístupy k zajištění bezpečnosti kritické informační infrastruktury jsou na období let 2015 – 2020 obsaženy v Národní strategii kybernetické bezpečnosti ČR a v nových právních normách, které představuje především zákon o kybernetické bezpečnosti a které vstoupily v účinnost od 1.1.2015.

Hlavní vize Národní strategie kybernetické bezpečnosti ČR na období 2015 – 2020 je vyjádřena v několika tezích:

- Vytvořit v ČR hladce fungující informační společnost;
- Rozšířit expertní základnu kybernetické bezpečnosti tak, aby byla schopna Čelit nejnovějším kybernetickým útokům;
- Získat přední postavení v oblasti kybernetické bezpečnosti ve středoevropském regionu a Evropě;

[42] *Výroční zpráva Bezpečnostní informační služby za rok 2013*. BIS. [online]. [cit.2015-02-05]. Dostupné z WWW: <http://www.bis.cz/n/2014-10-27-vyrocni-zprava-2013.html>.

- Podporovat mezinárodní partnery a plnit kolektivní závazky v oblasti kybernetické bezpečnosti.[43]

K hlavním pětiletým cílům realizace národní strategie kybernetické bezpečnosti patří vytvoření efektivního modelu národní a mezinárodní spolupráce v oblasti kybernetické bezpečnosti a zajištění jeho efektivního fungování, vytvoření spolehlivého kyberprostoru pro sdílení informací se soukromým sektorem, podpora výzkumu a vzdělávání v oblasti kybernetické bezpečnosti, podpora rozvoje schopností Policie ČR odhalovat počítačovou kriminalitu a další utváření evropského harmonizovaného právního rámce pro zajištění kybernetické bezpečnosti. Samostatným úkolem je zajištění ochrany národní komunikační infrastruktury a významných informačních systémů plynulým zvyšováním odolnosti, integrity a důvěryhodnosti sítí KII a VIS a zvyšování schopností a kapacit národního centra kybernetické bezpečnosti v řešení kybernetických bezpečnostních incidentů.[44]

4.6 Dílčí Závěr

Kritická informační infrastruktura je důležitým systémovým a také tvořícím prvkem kritické infrastruktury, jejíž ochraně je v krizovém řízení a civilním nouzovém plánování v posledních letech věnována zvýšená pozornost. Nové přístupy k vymezení kritické informační infrastruktury jsou v kontextu zajištění kybernetické bezpečnosti společnosti vyjádřeny v souboru nových právních předpisů, účinných od ledna 2015. V těchto právních předpisech a také Národní strategii kybernetické bezpečnosti ČR je zřejmý posun od orientace na budování základních kapacit a zajištění základní kybernetické bezpečnosti hlubšímu a pokročilejšímu zabezpečení.

[43] *Národní strategie kybernetické bezpečnosti České republiky na období let 2015 – 2020.* [online].[cit.2015-02-05]. Dostupné z WWW: <http://www.cybersecurity.cz/data/navratil2014.pdf>.

[44] *Národní strategie kybernetické bezpečnosti České republiky na období let 2015 – 2020.* [online].[cit.2015-02-05]. Dostupné z WWW: <http://www.cybersecurity.cz/data/navratil2014.pdf>.

5 Případové studie

Pro aktuální pochopení síly aktérů, kybernetických zbraní a cílů, se budeme dále zabývat případovými studiemi, které pomohou pochopit účinnost kybernetického terorismu v kybernetickém prostoru. Je důležité zdůraznit, že kybernetický útok je vždy promyšlený a politicky motivovaný.[45] Všechny případové studie budou z blízké minulosti. Výběr studií byl proveden podle co možná největšího zásahu do společnosti, případně nám nejbližší oblasti. Na závěr budou shrnuty další kybernetické útoky, které v nejbližší době nastaly.

5.1 Kybernetický útok na Irán

Zřejmě jeden z nejzajímavějších incidentů se odehrál v roce 2009, kdy agent izraelských obraných sil, přesněji Jednotky 8200, která plní podobnou roli jako americká Národní bezpečnostní agentura (NSA), ochromil íránský jaderný program. Klíčem k pochopení tohoto konfliktu je dobré uvědomit si, že Izrael a jejich úhlavní spojenec USA, jsou přísně proti jakémukoliv pokroku Iránu v oblasti jaderného programu. Obě země se zavázaly striktně zamezit výrobu jaderné zbraně Iránem. Pro tyto země je to jedna z největších bezpečnostních hrozeb současného světa. USA jsou v tomto konfliktu spíše pro ekonomické sankce, naopak Izrael se nezdráhá použití vojenské síly. Vláda Iránu to kategoricky popírá a tvrdí, že uran potřebuje pro svou jadernou energetiku, zdravotnictví a výzkum. Této verzi nevěří ani Mezinárodní agentury pro atomovou bezpečnost (MAAE), které jsou přesvědčeny, že íránský jaderný program slouží k vojenským účelům.

Samotný kybernetický útok byl proveden síťovým virem Stuxnet, který byl speciálně vytvořen v roce 2005, za účelem zbrzdění íránského jaderného programu, a to ve spolupráci USA a Izraele. Stuxnet je specifický tím, že se soustředí na kontrolu průmyslových systémů. Zvládá přeprogramovat programovatelné logické automaty a své změny bezpečně ukrýt. Tento červ využíval tak zvaného nultého dne operačních systémů Microsoft Windows. To jsou zneužití, která jsou útočníkovi známá dřív, než na

[45] JANCZEWSKI, L; COLARIK, A. *Managerial Guide for Handling Cyber-Terrorism and Information Warfare*. London, 2005. s. 44.

ně přijde výrobce software. Nejvíce červ využil pro své šíření chybu čtení souborů Microsoft Windows. Jakmile se uživatel zaujímal o přenosnou USB paměť, kde byl poškozený soubor, nastalo spuštění jiného programu ve stejném adresáři a tím instalací červa do systému, kde červ dostal nové příkazy a informoval o své činnosti své útočníky. Podle expertů byl tento síťový vir jeden z nejsofistikovanějším škodlivým kódem, který byl kdy vytvořen a využíval dvaceti dosud neobjevených bezpečnostních chyb. Antivirové programy jej tak nemohly vypátrat.

Útok se zdařil díky dvojitému agentovi pracující pro Izrael. Cílem útoku byla jaderná elektrárna, či ještě spíše závod na obohacování uranu v Natanzu. Agent přinesl červa Stuxnet na flash disku, odkud byl přímo nahrán do sítě. Jakmile byl červ aktivován, infiltroval celou síť a převzal kontrolu nad určitými systémy. Bezpečnostním expertům zabralo několik měsíců, než Stuxnet objevili, zanalyzovali a byli schopni odstranit. V tomto případě se Stuxnet zaměřoval především na systémy od společnosti Siemens, které jsou používány v iránských jaderných komplexech. Tento síťový vir dále ohrozil potencionálního spojence Iránu, tedy Rusko. Tímto červem měla být infikována ruská jaderná elektrárna a pomocí flash disku Mezinárodní vesmírná stanice. Vše mělo být provedeno v roce 2010. K tomuto závěru došel počítačový odborník Jevgenij Kasperskym, ředitel a spolumajitel známe společnosti Kaspersky Lab, zaměřující se na počítačovou bezpečnost.

Tabulka 2: Shrnutí kybernetického útoku na Irán

Aktéři	Mezistátní účast
Kybernetické zbraně	Síťový vir (Stuxnet)
Cíle	Jaderné elektrárny Iránu a Ruska, Mezinárodní vesmírná stanice

Zdroj: BBC 2012, Blaunstein 2013, Shearer 2011

V tomto případě byly použity kybernetické zbraně a útok byl veden na velmi významné cíle kritické infrastruktury. Tento kybernetický útok dokazuje, že zneužití kybernetických zbraní neznamená okamžité riziko pro civilní obyvatelstvo. Daný

konflikt je příkladem kybernetického incidentu, který reagoval na události v reálném světě. Následkem bylo zvýšení kybernetické bezpečnosti a minimalizování slepých míst v kybernetickém prostoru.

5.2 Kybernetický útok na USA

Využití zbraní kybernetického terorismu nalezneme i v případě hackerské skupiny Anonymous, která zaútočila v lednu 2012 na významné instituce v USA. Hnutí Anonymous je mezinárodní skupina hackerů bez pevné organizační struktury. Aktivisté se většinou zapojují do různých druhů operací. Známá je především díky útokům na firmy, které vypověděli spolupráci neziskové mediální společnosti WikiLeaks, které zveřejňuje utajované vládní dokumenty, a to především vlády USA, při čemž využívá internet k zachování anonymity. Pro Anonymous byl útok odvetou za zablokování webu megaupload.com, který byl svého času největším serverem pro sdílení dat na internetu, měl kolem 180 miliónů registrovaných uživatelů a vydělal svému zakladateli přibližně 40 miliónu dolarů. Vedení tohoto Honkogského serveru, který založil v roce 2005 německý hacker Kim Dotcom, jehož pravé jméno je Kim Schmitz, bylo obviněno americkou justicí z porušování zákonů o duševním vlastnictví a způsobení škody přibližně půl miliardy dolarů. Skupina Anonymous po zablokování daného webu napadla webové stránky amerického ministerstva spravedlnosti, Federální úřad pro vyšetřování (FBI), Bílý dům i hudební a filmové organizace, které se zabývají ochranou autorských práv.

Při útoku skupina Anonymous využila techniku zvanou DDoS (Distributed Denial of Service). V reálu kybernetický útok probíhá vždy podle stejných pravidel. Tisíce počítačů začnou v jeden okamžik přistupovat na zcela konkrétní server. Ten nemůže zpravidla tak vysoké množství požadavků zvládnout a celý server vypadne. Pro obyčejného uživatele se potom takto napadená webová stránka tváří jako nedostupná. Do největšího kybernetického útoku toho času se zapojilo rekordních 5 635 lidí a samotných útok trval jen několik málo hodin. Hackeři při útoku ohlásili, že na podobný útok mají potencionál s několika milióny počítači a do takového globálního útoku se můžou připojit odkudkoliv a atakovat jakoukoliv stránku na světě, stačí jim k tomu

pouze mobil nebo připojení k internetu. Hnutí Anonymous při tomto kybernetickém útoku nezískali z napadených institucí žádné utajované informace.

Obrázek 1: Celosvětová odplata za Megaupload: Oranžové pole značí intenzivní kybernetické útoky

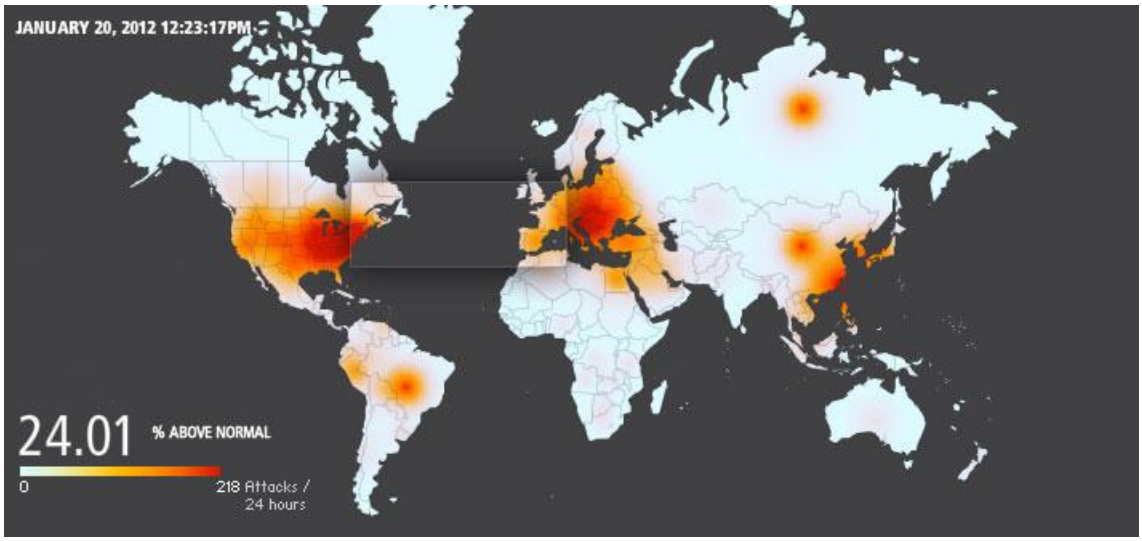

Foto:
akamai.com

http://www.akamai.com/html/technology/dataviz1.html (dostupnost kontrolována 1. dubna 2015)

Tabulka 3: Shrnutí kybernetického útoku na USA

Aktéři	Hnutí Anonymous
Kybernetické zbraně	DDoS (Distributed Denial of Service)
Cíle	Americké ministerstvo spravedlnosti, FBI, Bílý dům, filmové a hudební organizace

Zdroj: ČT24 2012, ČTK 2012, Novinky.cz 2012

Při tomto kybernetickém útoku byly plošně odstaveny významné servery institucí americké vlády a silně ziskové firmy hudebního a filmového průmyslu. Tento útok byl ukázkou síly a zranitelnosti institucí, které by měli být schopny takovému útoku potencionálně nejlépe odolat. Pro civilní obyvatelstvo tento incident nepředstavoval žádné riziko. Podle oslovených bezpečnostních specialistů je tato reakce hackerského hnutí Anonymous na zablokování serveru megaupload, jen prvním náznakem toho, jak to bude vypadat v blízké budoucnosti. Příbuzné ideologické útoky se budou vyskytovat stále častěji. Takzvaný hacktivismus, tedy aktivita hackerů v online světě, se bude stále častěji týkat státních institucí a firem s astronomickými zisky, jaké jsou například v hudebním nebo filmové průmyslu. Vlajkovou lodí, která sdílí největší obsah dat na světě, se stál nástupnický sever MEGA, který založil opět Kim Dotcom. Tento sever sídlí na Novém Zélandu a je daleko lépe zabezpečen proti případnému obvinění z krádeže duševního vlastnictví.

5.3 Vybrané útoky v kyberprostoru

V následující části se budeme ve zkrácené formě věnovat dalším kybernetickým útokům v období mezi roky 2013 až 2014. V této části budou zmíněny i kybernetické útoky, které zasáhly i samotnou Českou republiku.

Začátkem roku 2013 zažila Česká republika jeden z největších hackerských útoků na české zpravodajství severy, internetové stránky bank, telekomunikačních operátorů a dalších institucí. Při útoku byla využita technika DDoS. Útok byl označen za velmi sofistikovaný. Motivem byla obrovská medializace. Podle bezpečnostních expertů byl útok primárně veden z ruských sítí. Odhadované škody byly vyčísleny na deset miliónu korun.

Koncem roku 2013 byla zveřejněná zpráva, že čínští hackeři se nabourali do počítačů ministerstva zahraničí České republiky a čtyř dalších evropských zemí. Útoky již prý započaly v roce 2010. K napadení bylo využito zavirovaných e-mailových zpráv, které při otevření stáhly kód umožňující přístup k datům v osobním počítači. Podle bezpečnostních expertů není možné potvrdit, zda za útoky stála čínská vláda.

V březnu roku 2014 Rusko podniklo okupaci poloostrova Krym, který byl územím Ukrajiny. Celá situace vyústila anexí Ruska vůči Krymu. Představitelé Ukrajiny, USA a zemí západní Evropy tyto kroky považovali za nelegální anexi celého poloostrova Krym k Rusku a žádná země světa tento krok neuznala. Součástí ruské vojenské intervence na Krym byly i kybernetické útoky. Rusko napadlo komunikační infrastrukturu, rušilo i odposlouchávalo telefonní hovory. Hackeři napadli ukrajinské vládní weby a objevily se i zprávy o tom, že ruské lodě v oblasti Krymu na sobě mají nainstalovány rušičky. Rusko tímto demonstrovalo, že i v této oblastí má vysoce sofistikované schopnosti.

5.4 Dílčí závěr

Výše uvedené incidenty z části popisují oblast vedení kybernetického terorismu. U těchto kybernetických útoků jsme schopni identifikovat použité kybernetické zbraně, cíle a alespoň nepřímo aktéry těchto incidentů. V těchto případových studií jsme svědky kybernetických útoků pro zisk mediální pozornosti, utajovaných informací, finančního zisku a v neposlední řadě vojenské výhody

Nabízí se nám tedy otázka, v jakém množství nalezne kybernetický terorismus budoucí uplatnění ve zdolávání různých cílů? Jsou aktéři této techniky boje dostatečně vnitřně přesvědčeny, aby zneužili tento kritický kyberprostor vytvořený člověkem? Jakým způsobem se bude zaobírat evoluce kybernetického terorismu? V poslední části se budeme zaobírat těmito otázkami a predikcí vývoje kybernetického terorismu.

6 Predikce kybernetického terorismu

Pomocí analýz směřování se budeme dále snažit zúročit informace získané k analýze evoluce kyberteroristických aktérů, zbraní a cílů. Samotný kyberterorismus je spojen především s ICT nástroji, které mu umožňují efektivní funkci, proto se zaměříme na sledování technického trendu, který má široké spektrum uplatnění v kybernetickém terorismu. Dále se zaměříme na medializaci pojmu kybernetický terorismus, který má obrovský potenciál v užití kyberteroristických praktik. Poslední směřování se bude zaobírat politickými trendy, jenž jsou neméně důležité pro globální směřování lidstva.

6.1 Technické směřování

Kybernetický terorismus se stává v poslední době stále viditelnější realitou, respektive je mu věnován poměrně značný zájem i ze strany médií. Důvody mohou být různé, ale jedním z nich jistě je i to, že současný globalizovaný svět, spojený mnohými komunikačními prostředky, skýtá pro tento typ aktivit takové možnosti, jako jistě doposud nikdy v minulosti. Pro technickou západní společnost jsou velmi devastující případné útoky na počítačovou síť. Útoky prostřednictvím počítačových sítí představují hrozbu srovnatelnou s účinky zbraní hromadného ničení. Západ spoléhá víc a víc na počítačové sítě. To posiluje závislost – a ze závislosti se rodí zranitelnost. Zpoza počítačového terminálu lze totiž teoreticky zablokovat automatizované rozvody vody, elektřiny, plynu i ropy. Nebo naopak otevřít přehrady a zatopit přilehlé oblasti. Chaos se dá snadno vyvolat i v letecké dopravě a v plně elektronizovaných finančních operacích. Kolaps hrozí i vládním komunikačním systémům včetně vojenských.[46]

Lze důvodně předpokládat, že tento trend se v budoucnu nezmění: technologie se totiž rozvíjejí neustále a pokrývají i takové oblasti lidského života fungování lidské společnosti, kde to bylo dříve nepředstavitelné. Ač jistě není namístě zpochybňovat to, že teroristé se vážně zabývají možností získání znalostí a poté vlastní výroby zbraní hromadného ničení,[47] ničivý potenciál mohou mít i věci, jež nás běžně

[46] Typologie terorismu: Kybernetický terorismus. *Ministerstvo vnitra ČR* [online]. 2009 [cit. 2015-03-19]. Dostupné z WWW: <http://www.zakomunistu.cz/>.

[47] MIKA, O. J. *Současný terorismus: řešení krizových situací*, Praha, 2003, 92 s.

obklopují, respektive v souvislosti s rozvojem technologií se potenciálně škodlivými stát mohou.

Zde mám na mysli např. rozvíjející se „módnost“ chytrých doplňků oblečení či jiné „nositelné elektroniky,“ chytré domácí spotřebiče, jako chladničky, pračky, televize a podobně. Infikování těchto zařízení nějakou formou viru, který by umožnil např. jejich ovládání na dálku či prostě zapříčinil závažnou poruchu, která může mít nedozírné následky. Velmi škodlivým by mohlo být i „infikování“ GPS navigací – pokud by jejich záměrně chybné údaje nasměrovaly značné množství lidí např. do určitého úseku dálnice či dokonce např. přímo na její nedokončený úsek a podobně, mohlo by to nepochybně vést k velmi závažným škodám a to minimálně hmotným. Zcela jednoznačné následky by ovšem mělo násilné převzetí ovládání např. elektrárny, zejména jaderné, či přehradní nádrže – tam by teroristický útok napáchal nedozírné škody.

Značné problémy mohou být způsobeny v důsledku užívání chytrých zdravotnických doplňků a aplikací (stačí jen, aby dodávala nesprávná či nebezpečná doporučení). Zcela fatální následky by pak mohli vzniknout při napadení dálkově řízených implantátů. Již dnes se ve velkém měřítku používají implantáty, které jsou řízeny dálkově, včetně kardiostimulátorů, inzulinových pump, sluchových zařízení nebo stimulátorů mozkových funkcí.[48] Není důvodu předpokládat, že by se tento trend měl změnit, naopak – jak tato zařízení budou stále cenově dostupnější, nepochybně se stanou běžnou součástí mnoha nemocných lidí. Domnívám se, že není vyloučena možnost, že patřičně fundovaní teroristé získají přístup k ovládání takových zařízení a vypnou je – s neblahými důsledky jak pro jejich uživatele, tak mnohdy i pro jeho okolí. Tak by tomu bylo například v případě, kdy by byl takovýmto útokem zasažen např. řidič automobilu, který by se v důsledku toho stal neovladatelným. Nelze v této souvislosti nepřipomenout, že s patřičným přístupem k GPS údajům o poloze konkrétního řidiče by bylo možno atak zvolit v takovou dobu a místě, aby následný vedlejší efekt, tedy zasažení co největšího počtu ostatních účastníků silničního provozu byl co největší.

[48] Kaspersky Lab spolupracuje s biohackery. *ITBIZ* [online]. 2015 [cit. 2015-03-20]. Dostupné z WWW: <http://www.itbiz.cz/tiskove-zpravy/kaspersky-lab-spolupracuje-s-biohackery>.

Pokud jsem zmínil problematiku úmyslně způsobených útoků na vozidla, musím připomenout další hrozící nebezpečí. Zatímco v předešlém příkladu by byl útok směřován na technický doplněk, implantát v těle řidiče vozidla, zcela reálným bude i využití přímo onoho vozidla jako dálkově ovládané zbraně. Již v současnosti probíhá rozsáhlé testování automaticky řízených vozidel. Google testuje samořídící automobily již řadu let. Bez nehody tyto robotické automobily najezdily již stovky tisíc kilometrů. Doposud je musel jistit i řidič, který mohl v případě nastávajících problémů zasáhnout.[49] Ve chvíli, kdy budou taková vozidla zcela autonomní (a současně zcela nepochybně neustále on-line), bude jistě snem mnohého teroristy převzít na dálku ovládání takového vozidla či ještě spíše většího množství vozidel a rozpoutat masakr. Obdobné nebezpečí hrozí i u dronů, přičemž se nemusí jednat o hudbu příliš vzdálené budoucnosti: Jeden z největších internetových obchodů na světě Amazon testuje bezpilotní stroje, které by mohly v budoucnu nahradit pozemní způsoby doručování malých balíčků do 2,3 kilogramu. Podle generálního ředitele společnosti Jeffa Bezose by se mohla služba spustit do čtyř nebo pěti let.[50] Zdá se, že vzpomínka na 11. září 2001 již ve spojených státech poněkud vybledla, jestliže uvažují o vpuštění blíže neurčeného, ale vzhledem k velikosti společnosti Amazon[51] jistě nemalého množství potenciálních dálkově ovládaných bomb do tamního vzdušného prostoru.

Ne veškerý kybernetický terorismus musí být vázán jen na internet, respektive nějakého jeho nástupce. Nesouhlasím totiž s názorem, že je možné proniknout pouze do webového serveru nebo počítače připojeného na internet, byť je tato varianta jistě nejběžnější. Tento autor evidentně opomněl možnost infikace počítače např. pomocí

[49] Americká Nevada jako první na světě povolila provoz robotických aut. *Technet.cz* [online]. 2012 [cit. 2015-03-20]. Dostupné z WWW: <http://technet.idnes.cz/americka-nevada-jako-prvni-na-svete-povolila-provoz-robotickych-aut-1go-/tec_technika.aspx?c=A120223_171923_tec_technika_vse>.

[50] Amazon chce rozvážet balíčky vlastními létajícími drony. *IDnes.cz* [online]. 2013 [cit. 2015-03-20]. Dostupné z WWW: <http://ekonomika.idnes.cz/amazon-testuje-bezpilotni-letouny-du3-/eko-zahranicni.aspx?c=A131202_081758_eko-zahranicni_maq>.

[51] Obrat této společnosti činil např. v roce 2011 48,07 miliard USD. Zdroj: AMAZON.COM, INC.: Commission File No. 000-22513. *UNITED STATES SECURITIES AND EXCHANGE COMMISSION* [online]. [cit. 2015-03-20]. Dostupné z WWW: <http://www.sec.gov/Archives/edgar/data/1018724/000119312512032846/d269317d10k.htm>.

USB disku, či nějakou formou bezdrátového přenosu dat, jako je bluetooth či pomocí RFID čipů.

Teroristická aktivita v kyberprostoru však nemusí nutně mít za následek okamžité způsobení hmotné škody. Koncem 90. Let přišla FBI s nápadem odposlouchávat internetový provoz a vyhledávat zprávy, které si teroristé mezi sebou posílali.[52] Připustíme-li, že členy teroristických skupin se jistě stávají a stávat budou i kdo bude odposlouchávat informace bezpečnostních složek a díky tomu budou teroristé jednak schopni s předstihem reagovat, jednak budou moci své útoky v reálném světě směřovat na nejvhodnější a momentálně třeba nechráněné cíle.

Obrana proti těmto aktivitám není a nebude ani v budoucnu jednoduchá. Po technické stránce je nutno jednak se neustále snažit o co nejlepší zabezpečení všech zařízení, tedy zejména kvalitní a aktualizované antiviry, firewally a podobně, jednak, a to zejména u těch, kdo provozují nějaké potenciálně zneužitelné zařízení (pro příklad lze uvést např. elektrárnu), neustálá snaha o co nejvyšší úroveň veškerého zabezpečení a současně i kvalitu personálu, který se IT technologiemi zabývá. Nezbytným se podle mého názoru stane, aby minimálně v rámci EU byly přijaty patřičné právní předpisy, reagující na nové trendy v technologiích, a kladoucí např. na výrobce všemožných „chytrých“ zařízení jasné a striktní požadavky ohledně bezpečnosti.

Co se týče platné legislativy se domnívám, že pokrývá i takové útoky, jež jsou nyní stěží představitelné, avšak přesto zcela reálné. V současné době lze teroristické útoky a teror stíhat na podkladě ustanovení §§ 311 – 313 trestního zákoníku. Příslušná ustanovení totiž myslím dobře pokrývají i postih nebezpečí, která jsem popsal výše, kdy např. umožňují trestat toho, kdo se zmocní letadla, lodi nebo jiného prostředku osobní či nákladní dopravy nebo nad ním vykonává kontrolu, anebo zničí nebo vážně poškodí navigační zařízení nebo ve větším rozsahu zasahuje do jeho provozu nebo sdělí důležitou nepravdivou informaci, čímž ohrozí život nebo zdraví lidí, bezpečnost takového dopravního prostředku anebo vydá majetek v nebezpečí škody velkého rozsahu či toho, kdo vydá lidi v obecné nebezpečí smrti nebo těžké újmy na zdraví nebo cizí majetek v nebezpečí škody velkého rozsahu tím, že způsobí požár nebo povodeň

[52] DUNNIGAN, J. F. *Bojiště zítřka: tváří v tvář globální hrozbě kybernetického terorismu*, Praha, 2004, s. 224.

nebo škodlivý účinek výbušnin, plynu, elektřiny nebo jiných podobně nebezpečných látek nebo sil.

6.2 Mediální směřování

Jako je základním předpokladem pro kybernetický terorismus existence internetu, totéž platí o prezentaci jejich „úspěchů“ – pokud by došlo i k velmi úspěšnému útoku v určité oblasti státu či celé planety, dosah takového útoku by vždy zůstal pouze více či méně lokální, nebyla-li by možnost sdělit zprávu o tomto „úspěchu“ co největšímu počtu dalších osob. To totiž může mít několik efektů: jednak vyvolat strach u těch, které by pocítili možnost zasažení i jich samých, jednak „potěšit“ příznivce teroristů (s čímž může souviset i snaha o zapojení se do takové činnosti). Již nyní toto pozorujeme u Islámského státu, který své aktivity (jež lze nepochybně označit za teroristické) pravidelně prezentuje ve stále profesionálnější formě na internetu. Není tedy pochyb o tom, že mezi jeho příznivce nepatří jen bojovníci s kalašnikovy, ale i bojovníci s počítači. Je proto dle mého názoru jen otázkou času, kdy se jejich boj přenese i na síť. I proto, že oni sami se údajně stali naopak cílem kyberútoku (jež se však v tomto kontextu zdráhám označit za kyberterorismus: „v rámci obnovené operace "Ice ISIS" podnikli masivní útoky proti více než tisícovce islamistických webových stránek. Hackeři se rovněž zaměřili na účty radikálů na sociálních sítích Facebook, Twitter, Instagram i na YouTube a několik stovek (podle některých zahraničních médií dokonce 1500) jich už vyřadili. Přitom právě sociální sítě jsou pro Islámský stát velmi důležité, protože pomocí nich získávají nové členy a nabírají další radikály.[53] Ostatně, je myslím předmětem k úvaze, zda už sama existence takových účtů, resp. jejich využívání pro účely teroristické organizace, není též kybernetickým terorismem – dopad tohoto teroru se totiž nepochybně internetem šíří. Domnívám se, že si lze velmi dobře představit cílený útok teroristických skupin i na média, respektive narušení oficiálních stránek např. CNN a zveřejnění určitých

[53] Tvrdá rána pro Islámský stát: Anonymous podnikli masivní útok. *EuroZprávy.cz* [online]. 2015 [cit. 2015-03-20]. Dostupné z WWW: <http://zahranicni.eurozpravy.cz/blizky-vychod/113210-tvrda-rana-pro-islamsky-stat-anonymous-podnikli-masivni-utok/>.

informací, které by měly dopad na miliony, ne-li miliardy jejich „konzumentů“. Nemám ani tak na mysli např. zveřejnění falešných pochvalných článků, ale spíše vyvolání paniky zveřejněním falešných zpráv např. o jaderném výbuchu v určité části země. To by jistě vyvolalo velice bouřlivou reakci, jež by ve spojení s panikou měla značné následky. Dovedu si představit i ještě horší scénář, kdy by k takovému zkompromitování jinak důvěryhodných zpravodajských či vládních serverů docházelo tak často, že by i v ně lidé ztratili důvěru. To by mohlo mít ten efekt, že by lidé nereagovali ani na skutečné varování před nehypotetickou hrozbou – se všemi důsledky.

Obdobně by mohlo dopadnout zkompromitování různých sociálních sítí, jako je Facebook a podobně. Jejich prakticky bezprostřední dopad na doslova stamiliony až miliardy lidí, z nichž mnoho je stále online. Vyvolat u těchto osob paniku fingovanou zprávou či statutem u některého z „přátel“ by nebylo jistě nic obtížného. Pak by jistě bylo namístě uvažovat o využití § 357 trestního zákoníku, tedy trestného činu šíření poplašné zprávy: Kdo úmyslně způsobí nebezpečí vážného znepokojení alespoň části obyvatelstva nějakého místa tím, že rozšiřuje poplašnou zprávu, která je nepravdivá bude potrestán odnětím svobody až na dvě léta nebo zákazem činnosti. Zde by ovšem bylo nepochybně třeba rozsáhlé mezinárodní spolupráce (ostatně jako ve všem, co se internetu a obecně elektronických komunikací týče). Server, z něhož došlo k útoku, se zřejmě jen málokdy bude nacházet v cílové zemi útoku, a totéž bude platit o pachateli či pachatelích. Je proto zcela nezbytné za tímto účelem využívat spolupráce např. v rámci Interpolu či Europolu. V rámci Europolu ostatně již nyní funguje European Cybercrime Centre, jež je „je orgánem policejního úřadu (Europol) v Evropské unii (EU), se sídlem v Haagu, který koordinuje přeshraniční donucovací akce proti počítačové kriminalitě a působí jako centrum technického odborné znalosti v této věci.[54] Domnívám se, že důležitost tohoto úřadu bude bohužel jen narůstat.

Ohledně prevence v této oblasti platí obdobně jako v předešlé kapitole nezbytnost neustálé snahy o dosahování nejvyšší možné úrovně techniky a obranného softwaru, stejně jako kompetentních pracovníků. Velmi důležitým pak může být i to, abychom se při sledování rozličných zaručených zpráv snažili používat cosi jako

[54] European Cybercrime Centre. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2013 [cit. 2015-03-20]. Dostupné z WWW: <http://en.wikipedia.org/wiki/European_Cybercrime_Centre>.

„zdravý rozum a nepodléhali tedy každé nepodložené informaci. Nemusí to ovšem vždy být jednoduché: „Dnes (30. října 2013 – pozn. autora) je to přesně 75 let, co americké rozhlasové posluchače vyděsila adaptace románu Válka světů od H. G. Wellse. Je to vědecko-fantastický příběh o tom, jak na planetu Zemi zaútočí Marťané. Postupně se posluchači dozvěděli, že astronomové pozorovali divné úkazy na Marsu. Že na Zemi dopadl neznámý objekt, pravděpodobně meteorit. A odhaduje se, že značná část posluchačů přeladila z komediálního pořadu na jiné stanici ve chvíli, kdy mimozemšťané vystoupili z létajícího talíře a zaútočili na shromážděný dav. To vyvolalo paniku.[55] Otázkou je, co by obdobně burcující zpráva vyvolala dnes či v budoucnu, když by mohla být podložena zcela realisticky vyhlížejícími videi a podobně.

Dalším problémem „mediálního kyberterorismu“ může přítomnost novinářů přímo na bojištích, přičemž nutno si uvědomit, že „moderní bojiště je často přeplněné lidmi od novin a že je nutné se tím zabývat.[56] Jistě i mezi novináři se najdou mnozí, kteří sympatizují právě s tím, proti komu vojáci na uvedeném místě bojují, a využijí-li svých aktuálních poznatků a možnosti je za pomoci moderních technologií okamžitě rozšířit na internetu (či přímo je zaslat protivníkovi), může to mít zcela nedozírný dopad na vojenskou akci, a ovšem i na civilní obyvatelstvo v dané oblasti.

Mezinárodní spolupráce by dle mého názoru měla být co se médií poměrně snadná, alespoň co se týká velkých a známých subjektů. Zde mám na mysli např. CNN, BBC či Reuters. Problematičtější to ovšem zajisté bude v případě zpráv šířených rozličnými blogy či prostřednictvím sociálních sítí: tam je opět třeba myslet na to, že osoba, která se šíření zprávy, jejíž dopad se rovná teroristickému činu, se mlže nacházet prakticky kdekoliv na světě, s jedinou podmínkou, jíž je možnost připojení k internetu (nebo jakákoliv jiná technologie, v jejímž důsledku se příslušná zpráva na internet posléze dostane).

---

[55] Před 75 lety vyvolala rozhlasová hra Válka světů paniku z invaze mimozemšťanů. *Český rozhlas* [online]. 2013 [cit. 2015-03-20]. Dostupné z WWW: <http://www.rozhlas.cz/zpravy/historie/_zprava/pred-75-lety-vyvolala-rozhlasova-hra-valka-svetu-paniku-z-invaze-mimozemstanu--1274601>.

[56] DUNNIGAN, J. F. *Bojiště zítřka: tváří v tvář globální hrozbě kybernetického terorismu*. Vyd. 1. Praha: Baronet, 2004, 356 s. ISBN 80-721-4642-4, s. 170.

6.3 Politické směřování

Již v současnosti je mnohdy nerozhodné, zda se na určitých kyberútocích podílely jednotlivé osoby, či zda se jednalo o útok řízený některým státem. Lze to dle mého názoru jen těžko prokázat – ve světě „1“ a „0“, je možné zmanipulovat leccos, včetně důkazů o takovém jednání. Není ale myslím důvodu pochybovat o tom, že každý stát, i s těmi sebečistším úmysly, musí myslet na eventualitu napadení v kyberprostoru, některý pak jistě zváží i možnost reakce či preventivního úderu proti státu (či jinému subjektu jemu nepřátelskému. Takový útok může skýtat oproti klasické vojenské akci mnohé výhody – nemusí být tak viditelný a je tedy i lépe zpochybnitelný údaj o jeho původci.

K takovýmto aktivitám se však pravděpodobně příslušné služby nepřiznají, a proto je stěží možno předjímat, zda a kdy k útoku ze strany nějakého státu došlo. Proto se zaměřím na jinou, zcela bezprostředně související oblast činnosti státní moci, a tou je prevence proti kyberútokům. Od 1. ledna 2015 v ČR platí zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). Tento zákon poměrně podrobně upravuje problematiku, definuje základní pojmy, jako je např. kybernetický prostor, kritická informační infrastruktura a současně definuje povinnosti osob, které jsou povinny zajišťovat bezpečnost v informačních systémech (a také sankce, jež jim za neplnění jejich povinností hrozí). Důvodová zpráva k tomuto zákonu konstatuje, že „se vzrůstající závislostí společnosti na informačních technologiích pak ale na straně druhé vzrůstá i riziko zneužívání těchto technologií nebo útoky na tyto technologie, které mají rozsáhlé dopady do činnosti subjektů, které s nimi pracují, a potencionálně mohou vést ke značným škodám. Cílené útoky proti informačním technologiím jsou celosvětovým fenoménem a jejich dopad způsobuje rozsáhlé ekonomické škody ve veřejném i v soukromém sektoru a současně jsou schopny vyvolat negativní politické důsledky, a to jak v národním měřítku, tak v měřítku globálním. V případech, kdy je útok veden proti prvkům kritické infrastruktury, může být v konečném důsledku ohrožena bezpečnost nebo samotná existence státu. Útočníci se stále více zaměřují na prvky kritické infrastruktury, jako jsou energetické systémy, produktovody, zdravotnické informační systémy a informační systémy veřejné správy. S ohledem na fakt, že kybernetický prostor nezná hranic a není tedy otázkou teritoriální, je nutné útoky na informační technologie řešit z pohledu mezinárodního

společenství a s ohledem na závazky České republiky vůči státům Organizace Severoatlantické smlouvy (dále jen "NATO") a Evropské unie (dále jen "EU").“

S výše uvedeným nelze než souhlasit: jestliže by došlo např. k napadení německé rozvodné sítě elektřiny, důsledky by byly nepochybně nedozírné i pro další státy, které jsou s touto sítí propojeny, a proto je jistě v zájmu všech v mezinárodním měřítku koordinovat kroky, které by uvedenému předcházely či alespoň minimalizovaly případné škody.

Co se pak týče připomínky ohledně NATO coby vojenské organizace pak si lze představit scénář, kdy by byli např. britští poradci, kteří na Ukrajině školí místní vojáky,[57] napadeni drony ukrajinské armády,[58] nad nimiž by převzala ovládání nějaká teroristická organizace (např. již zmíněný Islámský stát), přičemž elektronické stopy by zdánlivě vedly např. k Rusku (aniž bych zpochybňoval schopnosti a pravděpodobně i ochotu právě této země se do boje v kyberprostoru zapojovat). Taková akce by mohla vést k ohromné eskalaci napětí, či ještě spíše k válce (což by mohlo být hypoteticky i cílem Islámského státu, neboť jakékoliv akce proti němu by jistě ztratili veškerou prioritu). Je nepochybně v zájmu nás všech takovým nebezpečím čelit a proto je dobře, že i NATO se touto otázkou seriózně zabývá, neboť „není pochyb o tom, že některé státy již masivně investují do kybernetických schopností, které lze aplikovat pro vojenské účely. V souladu s novým Strategickým konceptem NATO, revidovaná Politická koncepce kybernetické obrany definuje kybernetické hrozby jako potenciální zdroj kolektivní obrany, ve smyslu článku 5 Washingtonské smlouvy. Kromě toho, nová Politická koncepce a akční plán její implementace, poskytuje členským státům NATO příslušné direktivy a schválený seznam priorit, jejichž cílem je pokrok Aliance v kybernetické obraně, včetně zdokonalení koordinace mezi spojenci a s partnery NATO.[59]

---

[57] Britové už na Ukrajině cvičí vojáky. Z Moskvy zní kritika. *Novinky.cz* [online]. 2015 [cit. 2015-03-20]. Dostupné z WWW: <http://www.novinky.cz/zahranicni/evropa/364750-britove-uz-na-ukrajine-cvici-vojaky-z-moskvy-zni-kritika.html>.

[58] Američané dodají Ukrajině drony a terénní auta. *Novinky.cz* [online]. 2015 [cit. 2015-03-20]. Dostupné z WWW: <http://www.novinky.cz/zahranicni/amerika/363959-americane-dodaji-ukrajine-drony-a-terenni-auta.html>.

[59] Nové hrozby - kybernetické dimenze. *NATO Review* [online]. 2011 [cit. 2015-03-20]. Dostupné z WWW:<http://www.nato.int/docu/review/2011/11-september/Cyber-Threads/CS/index.htm>.

6.4 Dílčí závěr

K hlavním důsledkům bude dle mého názoru patřit zvýšená nejistota či nedůvěra, s níž začneme hledět na běžné věci okolo nás, jako je mobilní telefon, PC, a ovšem i chladnička, automobil.

Každý z těchto předmětů (a mnohé další, které jsou v tomto okamžiku teprve testovány ve společnostech Apple, Google, Xiaomi a mnohých jiných, zatím třeba i zcela neznámých) bude totiž potenciálně velmi nebezpečný, a to mnohdy i způsobem, jež si nyní nedokážeme ani představit.

Každý z těchto předmětů bude se značnou pravděpodobností schopen čerpat data z internetu, a současně na internet odesílat informace o své činnosti, prostředí, kde se nachází, jakož i o svém uživateli, a to včetně např. informací o jeho zdravotním stavu. Mnohé z toho bude současně schopen v menší či větší míře i ovlivňovat, a to jak v kladném smyslu, tak i v záporném (jak jsem nastínil výše). Nepochybně přitom tento předmět bude ovlivněn škodlivým obsahem na internetu, což je výraz, který „jen zdánlivě odkazuje na ucelenou, snadno vymezitelnou skupinu jevů. Vzhledem k překotnému vývoji internetu navíc nelze předpokládat, že bychom mohli být schopni jednoznačně určit i do budoucna, co je či naopak není škodlivým obsahem na internetu.[60]

V tom dle mého názoru tkví základní problém: kompetentní osoby, instituce a státy mají samozřejmě reagovat na to, co již existuje. Při rozvoji technologií lze však velmi těžko předjímat, co vše bude v oblasti počítačů (a dalších souvisejících zařízení) možné za několik let. Zřejmě jen málokdo si dovedl u prvních mobilních telefonů představit, že z poněkud monstrózního přístroje, jehož jedinou schopností bylo uskutečnění telefonního hovoru, se stane multifunkční zařízení, spojující funkce telefonu, fotoaparátu, videokamery, navigace a nabízející také možnost použít jej jako dálkový odpalovač bomby.[61]

---

[60] LUKÁŠOVÁ, K. *Škodlivý obsah na internetu*. In: *AUC IURIDICA: Kybernetická kriminalita*. Praha, 2013, roč. 2012, č. 4, s. 9.

[61] Gang vyráběl bomby, které šlo odpálit mobilem. *Novinky.cz* [online]. 2006 [cit. 2015-03-20]. Dostupné z WWW: <http://www.novinky.cz/krimi/104504-gang-vyrabel-bomby-ktere-slo-odpalit-mobilem.html>.

Stejně tak málokdo tušil, jaké převratné změny do komunikace přinese například Facebook. Uvedené skýtá jak velké možnosti kladné, tak i záporné – a mnohdy zcela netušené. Problém je tedy v tom, že jestliže přijde technologie natolik nová, lze stěží předjímat jak její přínos, tak potenciální rizika – a u informačních technologií a terorismu to jistě platí ve značné míře. Je tedy třeba, aby se zejména v bezpečnostních složkách této problematice věnovali opravdoví odborníci – a aby jejich názory a požadavky byly slyšeny ze strany politiků, zejména pak zákonodárců. Na hrozby je třeba reagovat včas, dokud je alespoň určitá šance jejich možný dopad minimalizovat. Proto je nepochybně třeba, aby byly jak v ČR, tak i v EU zkoumány hrozby možnosti teroristických útoků v kyberprostoru a obrana proti nim, na základě příslušných právních předpisů (s opatřeními důsledně realizovanými v praxi). Je dobře, že byl přijat zákon o kybernetické bezpečnosti, avšak zejména je třeba prosazovat jeho dodržování a průběžně zkoumat, zda stále vyhovuje „technologické realitě“ doby. Obdobné platí o EU a jistě i o NATO, neboť boj či teror v kyberprostoru může lehce přerůst v boj v realitě.

Jsem přesvědčen o tom, že tyto hrozby nesmíme podceňovat: například již zmíněný očekávaný rozmach automaticky řízených vozidel může být určitým testem toho, zda jsme ochotni obětovat něco z možného budoucího komfortu (tedy pohodlí, spojeného s tím, že nás vozidlo, do cíle doveze bez nutnosti našeho řízení) za eliminaci rizika, že se toto vozidlo s námi uvnitř stane dálkově řízenou zbraní. Obdobné platí o dronech – nejsem přesvědčen o tom, že možnost mít doručeno zboží v řádu hodin od objednání vyváží riziko zneužití dronů teroristy.

Dle mne je namístě tyto i další technologické inovace pečlivě posoudit a přijmout příslušné právní předpisy, které by tuto problematiku upravovaly, a to i v rámci mezinárodního práva. Tak by tomu u vozidel mohlo být určitou obdobou současné Úmluvy o silničním provozu (Vídeň 1968), z jejíž preambule vyplývá, že smluvní strany uznávají, že je nutné usnadnit mezinárodní silniční provoz a zvýšit bezpečnost na silnicích přijetím jednotných pravidel silničního provozu. Obdobně se jistě lze shodnout i v tom, že je nezbytné přijmout jednotná pravidla pro eventuální umožnění (či naopak zakázání) provozu automaticky řízených vozidel. Bude-li pak provoz takových vozidel umožněn, je třeba přijmout striktní pravidla pro zajištění co

největší bezpečnosti a maximální možné eliminace rizika převzetí jejich ovládání teroristy.

A obdobně by tomu mělo být u všech nových informačních technologií, které se v budoucnu objeví. V opačném případě hrozí, že s každou další věcí, schopnou nějak fungovat v kyberprostoru a původně jistě určenou k usnadnění či zpříjemnění života či fungování společnosti, se rozšíří škála možností, jichž budou moci teroristé zneužít.

7 Metody zpracování dat

7.1 Rozhovor s odborníkem na kyberprostor Ing. Jiřím Kachyňou

Autor poprosil specialistu v oblasti kyberprostoru o řízený rozhovor, který byl využit pro účely této práce. Tento mezinárodně zasvěcený a transparentní odborník z virtuálního prostředí, poskytl autorovi odpovědi na aktuální otázky ohledně kyberprostoru, které nám pomohou pochopit svět virtuálních sítí.

Dobrý den, pane inženýre, začneme první otázkou. Proč je tolik oblíbené hackování?

Pro hackera je to taková logická hra se správcem, programátorem sítě, při níž dokáže vyhrát ten chytřejší, který dokáže využít danou aplikaci, nebo případně obejít její zabezpečení. Ovšem od určité finanční částky už jde o byznys. Může to být dobrý přivýdělek, který dokáže hackera uživit. V poslední době jsou také velmi často v oblibě ideologické útoky.

Jakým způsobem si může vydělávat osamocený hacker?

Většina útočníků nezačíná hned ve velkém obchodovat například s kreditními kartami, ale začíná vítězit v internetových soutěžích, protože je to pro mě velice snadný způsob výdělku. Pokud není soutěž zfalšovaná od provozovatele, což je minimálně 40% všech soutěží na internetu, tak v 99% vyhraje vždy člověk zdatný v oblasti informačních technologií. Dále si může vydělat například krádeží dat, které umí snadno ukrást, ale neumí je zpeněžit jinak než tím, že je prodá v internetové aukci. Například prolomení hesla na facebook stojí asi dva tisíce korun. Cena není zpravidla vysoká pro nakupujícího, ale spíše pro hackera, aby si vydělal.

Jaké další ilegální služby hacker nejčastěji provádí?

Jde o hackování emailů, DDoS útoky, crackování hesel, nabourání se do počítače. Velmi často jsou hackeři oslovování pro útok na internetový obchod. Konkurence platí za to, že se hacker naboural do jejich konkurence a získá databázi klientů, kteří jsou pak lobováni do jejich internetového obchodu. Ve vánočních časech jsou velmi oblíbené

DDoS útoky na konkurenční obchody, kterým znemožníte funkčnost jejich webů, následně probíhá přechod zákazníků ke konkurenci.

Jaký může být odhadovaný počet hackerů v celosvětovém měřítku?

Je velmi obtížné zjistit přibližný počet osob zapojených do kybernetické kriminality. Tyto osoby se neprozrazují, nesdělují statistické údaje, neplatí daně a udělají vše proto, aby za sebou zametli stopy. Odhadem půjde o desítky tisíc osob. Oproti tomu kybernetických lékařů v podobě zaměstnanců antivirových společností je pouze pár tisíc. Kriminálníků je tedy minimálně desetkrát více než kybernetických lékařů.

Na kolik procent odhadujete úspěšnost antivirových programů, které nás mají primárně chránit před útoky škodlivého softwaru?

Účinnost virů je přibližně 80%. Tvůrci virů si při jejich výrobě stahují jednotlivé verze antivirových programů a testují je až do jejich překonání. Takto upravené viry pak pošlou do sítě.

Jak velký je finanční obrat jednotlivých druhů softwarů?

Obrat škodlivého průmyslového softwarů se blíží částce 100 miliard dolarů ročně. Tento obrat se odhaduje na pětinásobný oproti oblasti počítačové bezpečnosti.

Myslíte si, že internet je skutečnou hrozbou naší civilizace?

Internet se zcela vstřebal do lidské civilizace. Mezilidská, osobní, pracovní a státnická komunikace je propletená internetem. Nebezpečí, které se může více a více šířit, může kompletně ovládnout telekomunikační provoz internetu, kde běží vše – od finančních transakcí přes vědecké statě až po mezilidské vztahy. Je to nový způsob kontroly toku informací.

Jaké nebezpečí hrozí soukromí a lidským právům?

Je zde zcela nepředstavitelná celosvětová dystopie. Omezování svobody se týká všech zemí připojených k internetu. Například Americká Národní bezpečnostní agentura (NSA) denně sleduje 1,8 miliardy položek. Je to obrovská moc nad obyvatelstvem planety.

Jakou roli dnes hraje v kyberprostoru společnost Google?

Google například ví, co jste vyhledával před rokem, před měsícem a vy si to již nepamatujete. Ostatně stejný problém mají všichni, se kterými jste komunikoval. Bohužel existuje jen velmi málo prostoru pro to, co chcete dělat, aniž by to o Vás případně nechtěli vědět.

Jak by mohl internet pomoci naší civilizaci a nikoliv ohrožovat její práva a svobody?

Lidé si musí uvědomit, že musejí být daleko obezřetnější ve způsobu online komunikace. Musíme vědět, že informace sbírají vlády jednotlivých zemí, které je poskytují nejen státním službám, ale i soukromým firmám, se kterými spolupracují tajné služby. Možnost obrany je v použití kryptografických technologií, které nás mohou uchránit před „Velkým Bratrem“.

Pane inženýre Kachyňo, děkuji za rozhovor a budu se snažit, aby i tento rozhovor přispěl k objasnění virtuálního světa v této bakalářské práci.

Také děkuji. Na shledanou.

7.2 Dotazníkové průzkum

K objektivnímu zjištění skutečného pochopení kybernetického terorismu veřejností byl zpracován a předložen v období od 24. ledna 2015 do 1. února 2015 v rámci průzkumu k vyplnění anonymní dotazník. Tohoto dotazníkového průzkumu se zúčastnilo celkem 100 občanů nastupující generace, různého pohlaví a minimálně středoškolského vzdělání. Anonymní dotazník byl sestaven jednoduchou srozumitelnou formou otázek, nabízejících několik možných variant odpovědí, ze kterých bylo možné vybrat pouze jednu odpověď, která se nejvíce přiblížila vlastnímu názoru respondenta.

Tento dotazník byl zkoncipován pouze na uzavřené otázky. V dotazníku respondenti v počtu 100 osob na položené otázky odpovídali vyznačeným „X“ do takto ☐ značené kolonky. Předávání, zpracování i odevzdání dotazníků proběhlo anonymním způsobem, a to z důvodu toho, aby se metodou podařilo získat co nejvyššího počtu pravdivě zodpovězených odpovědí, kdy zmíněný anonymní způsob zpracování vyhovoval bez výhrad všem zúčastněným respondentům.

V rámci průzkumu bylo respondentům předáno celkem 100 dotazníků, kdy zpět byly tyto vráceny v počtu 91 kusů. Návratnost vyplněných dotazníků byla tedy ve výši 91%.

Výsledky průzkumu

Dotazníkového šetření a průzkumu se tedy nakonec zúčastnilo celkem 91 respondentů, kteří byli orientování do nastupující generace, měli různé pohlaví a minimálně středoškolské vzdělání.

Pro srozumitelnější, přehlednější a snadnější orientaci v údajích vycházejících z výsledků průzkumu, byla každá otázka dotazníku vyhodnocena zvlášť. U otázek je pro zpřehlednění sestavena tabulka s uvedením odpovědí respondentů. Z tabulek jsou zřejmé statistické údaje k otázkám, na které byli respondenti v dotazníku dotazováni.

Otázka č. 1

Můžete se během dne kdykoliv připojit na internet?

Znázornění odpovědí respondentů jsou obsahem tabulky č. 1

Tabulka č. 1

	Ano		Ne	
	počet	**%**	**počet**	**%**
Respondenti	**81**	**89,01**	**10**	**10,99**

Z odpovědí v tabulce č. 1 je zřejmé, že nejvíce respondentů v počtu 81 (89,01%) se může kdykoliv připojit k internetové síti. Jen 10 dotazovaných (10,99%) uvedlo, že nemůže být během dne kdykoliv připojeno k internetu.

Otázka č. 2

Byl(a) jste někdy obětí kyberšikany?

Znázornění odpovědí respondentů jsou obsahem tabulky č. 2

Tabulka č. 2

	Ano		Ne	
	počet	**%**	**počet**	**%**
Respondenti	**8**	**8,79**	**83**	**91,21**

Z odpovědí vyplynulo, že pouze 8 respondentů (8,79%) má negativní zkušenosti s virtuálním prostředím, přesněji kyberšikanou. Většina 83 dotazovaných (91,21%) se s touto ilegální činností nikdy nesetkala.

Otázka č. 3

Máte na svém počítači nebo mobilu nainstalovaný antivir?

Znázornění odpovědí respondentů jsou obsahem tabulky č. 3

Tabulka č. 3

	Ano		**Ne**	
	počet	**%**	**počet**	**%**
Respondenti	**85**	**93,41**	**6**	**6,59**

Z odpovědí vyplynulo, že naprostá většina 85 respondentů (93,41%) má své virtuální zařízení chráněno antivirem. Pouze minimum 6 dotazovaných (6,59%) nemá své zařízení ochráněno.

Otázka č. 4

Měl(a) jste někdy zavirovaný počítač?

Znázornění odpovědí respondentů jsou obsahem tabulky č. 4

Tabulka č. 4

	Ano		**Ne**	
	počet	**%**	**počet**	**%**
Respondenti	**71**	**78,02**	**20**	**21,98**

Z odpovědí vyplynulo, že velká část 71 respondentů (78,02%) má již zkušenosti s virtuálním útokem. Jen minimum 20 dotazovaných (21,98%) nemělo zařízení zavirováno.

Otázka č. 5

Používáte internetové bankovnictví?

Znázornění odpovědí respondentů jsou obsahem tabulky č. 5

Tabulka č. 5

	Ano		**Ne**	
	počet	**%**	**počet**	**%**
Respondenti	**84**	**92,31**	**7**	**7,69**

Z odpovědí vyplynulo, že 84 respondentů (92,31%) využívá moderní způsob bankovnictví. Pouze minimum 7 dotazovaných (7,69%) tuto službu nemá zavedenou.

Otázka č. 6

Prošel/prošla jste nějakým školením o informační technologii?

Znázornění odpovědí respondentů jsou obsahem tabulky č. 6

Tabulka č. 6

	Ano, u zaměstnavatele i v civilním sektoru.		**Ano, ale pouze u zaměstnavatele.**		**Ne, vůbec žádným školením.**	
	počet	**%**	**počet**	**%**	**počet**	**%**
Respondenti	**65**	**71,43**	**26**	**28,57**	**0**	**0**

Z odpovědí vyplynulo, že 65 respondentů (71,43%) bylo proškoleno v civilním i zaměstnaneckém sektoru. Dalších 26 dotazovaných (28,57%) bylo proškoleno pouze v rámci zaměstnavatele. Nevyskytl se žádný neproškolený respondent.

Otázka č. 7

Podporujete vzdělávání v oblasti informačních technologií?

Znázornění odpovědí respondentů jsou obsahem tabulky č. 7

Tabulka č. 7

	Ano, již na základních školách.		**Ano, spíše až na středních školách.**		**Ne, vzdělávání až v dospělosti.**	
	počet	**%**	**počet**	**%**	**počet**	**%**
Respondenti	**72**	**79,12**	**8**	**8,79**	**11**	**12,09**

Z odpovědí vyplynulo, že 72 respondentů (79,12%) je pro vzdělání v oblasti informačních technologií již na základních školách. Menšina 8 dotazovaných (8,79%) bylo pro školení na středních školách. Zbylých 11 respondentů (12,09%) je pro seznámení s virtuálním prostředím až v dospělosti.

Otázka č. 8

Přijímáte velké množství nevyžádaných emailů?

Znázornění odpovědí respondentů jsou obsahem tabulky č. 8

Tabulka č. 8

	Ano, velké množství.	**Ano, ale pouze malé množství.**	**Ne, nepřijímám .**

	počet	%	počet	%	počet	%
Respondenti	**46**	**50,55**	**35**	**38,46**	**10**	**10,99**

Z odpovědí vyplynulo, že 46 respondentů (50,55%) dostává pravidelně nevyžádanou poštu. Druhá nejpočetnější skupina 35 dotazovaných (8,79%) obdrží pravidelně pouze malé množství spamu. Zbylých 10 respondentů (10,99%) není obtěžováno spamem.

Otázka č. 9

Používáte nelegální software?

Znázornění odpovědí respondentů jsou obsahem tabulky č. 9

Tabulka č. 9

	Ano		Ne	
	počet	**%**	**počet**	**%**
Respondenti	**34**	**37,36**	**57**	**62,64**

Z odpovědí vyplynulo, že 34 respondentů (37,36%) využívá nelegální software. Větší skupina 57 dotazovaných (62,64%) používá pouze legální verze softwaru.

Otázka č. 10

Jaký máte názor na hnutí Anonymous?

Znázornění odpovědí respondentů jsou obsahem tabulky č. 10

Tabulka č. 10

	Sympatizuji s nimi.		Mám neutrální postoj.		Neuznávám toto hnutí.	
	počet	%	počet	%	počet	%
Respondenti	**62**	**68,13**	**8**	**8,79**	**11**	**12,09**

Z odpovědí vyplynulo, že 62 respondentů (68,13%) sympatizuje s hnutím Anonymous. Pro dalších 8 dotazovaných (8,79%) jsou k hnutí neutrální. Pouze 11 respondentů (12,09%) vnímá toto hnutí negativně.

Výsledky dotazníkového průzkumu

Výsledky dotazníkového průzkumu vyjadřují následující závěry:

Podle výsledků dotazníkového šetření lze konstatovat, že oslovení respondenti mohou být v podstatě neustále připojení k internetové síti a plně využívat její služby. Pouze 8 dotazovaných už mělo zkušenost s temnější stránkou virtuálních sítí, tedy kyberšikanou. Velká část respondentů využívá minimálně primární ochranu svého počítače nebo mobilního zařízení v podobě antivirových programů. I přes velkou snahu uživatelů s instalací antivirových programů již většina získala zkušenost se zavirováním svého zařízení. Velká část této generace také plně využívá ke spravování svých financí službu internetového bankovnictví. V otázkách informovanosti v informačních technologiích je velká většina dotazovaných zcela proškolena, z toho velká část u zaměstnavatele i v civilním prostoru. Případné vzdělávání budoucích generací podporuje většina respondentů a to již na základních školách. Problém s nevyžádanou online poštou má velmi široké spektrum dotazovaných, kde polovina má pro ně až nadměrný příjem tohoto spamu. Další problémem společnosti v podobě používání nelegálního softwaru přiznala více jak třetina oslovených. U poslední ideologické otázky ohledně hnutí Anonymous vyjádřilo této hackerské skupině podporu většina respondentů a jen malá skupina je v tomto ohledu neutrální nebo toto hutí zcela neuznává.

DISKUSE

Na základě rozhovoru s odborníkem na kyberprostor a zjištěných informací v rámci dotazníkového průzkumu vyplynulo, že i když je otázka kyberterorismu obecně spojená s prevencí a veřejnou informovaností, stále převažuje mírné podceňování této globální hrozby, která pak může přerůst až ke kybernetické kriminalitě či kybernetickému terorismu. Diskutabilní otázkou pak může být míra rizika ve srovnání se společenskými hodnotami. Většina respondentů se přikláněla k názoru, že s případnými primárními riziky mají zkušenost a ví, jak se s nimi v laickém kontextu vypořádat. Z názorů odborníka na kyberprostor vyplynulo, že případná prevence, profesionální přístup a moc na straně bezpečnostních institucí nejsou zárukou virtuální bezpečnosti. Velkým hnacím motorem tohoto nepředvídatelného nebezpečí je vlastní negativní zkušenost, která přinutí poškozené k protiopatřením. Teprve poté je daná problematika řešena určujícím způsobem. Za jeden z těchto způsobů můžeme pokládat osvětlení a následné pochopení jednotlivých součástí a mechanismů kyberprostoru. Systém, který je populaci dobrým sluhou, se může s využitím daných prostředků přeměnit až v odstrašující hrozbu. Ekonomická stránka, mocenský přístup, politické, náboženské nebo ideologické cíle často převládají před jakoukoliv možností ochrany, s čímž se ztotožnil také oslovený odborník. Většina respondentů nám také potvrdila, že jsou zcela zapojeny, případně z velké části odkázány na virtuální síť, která tak získává neustále vyšší prioritu a moc. Krátký dotazníkový průzkum dále poukázal na skutečnost, jak je společnost vázána a propletena s virtuálními sítěmi, případně atakována různými druhy nástrojů, a to už od velkého množství spamů až po méně častou kyberšikanu. Případná hra zasvěcených hackerů či pracovníků profesionálních kybernetických jednotek různého určení nám naopak ukázala nejvyšší možnou úroveň boje sofistikovaných a finančně náročných aktérů.

Je potřeba, aby si široká veřejnost, ale i politicky zodpovědní lidé uvědomili, že je potřeba neustále efektivně investovat do osvěty informačních technologií, bezpečnosti virtuálního prostoru nebo dodržování a tvorby legislativy.

ZÁVĚR

Kybernetický terorismus prochází ve všech sledovaných součástech neutuchající evolucí. Využití a potencionální síle jednotlivce je v souvislosti s tímto tématem neustále kladen velký význam. Velmi schopný jednotlivec může těžit ze svého výjimečného umu a může najít uplatnění svých schopností u různých institucí, států nebo teroristických organizací, které tím zacelují své vlastní personální nedostatky. Myšlenka zařazení úrovně státu do výčtu aktéru kybernetického terorismu je zcela neoddiskutovatelná, ale v rámci pochopení virtuálního světa velmi obtížně prokazatelná. Existují zcela jasné podezření z možného zapojení státu do kyberteroristických bojů, ale samotný stát nemůžeme zařadit do výčtu aktérů kybernetického terorismu, protože o přímém ani nepřímém zapojení státu do teroristických aktivit neexistují usvědčující důkazy.

V kapitole zabývající se problematikou nástrojů založených na ICT, které se mohou proměnit ve virtuální zbraně v kybernetickém světě, byla ukázána různorodost jejich využití. V prvotní myšlence může pokrok v ICT přinést nové možnosti efektivnější obrany. Naopak protipólem je jeho zneužití za účelem kyberterorismu. Možný neúspěch kybernetického útoku lze vysvětlit jako efektivní převahu bezpečnostních prostředků nad zbraněmi kyberteroristů, nebo případnou neschopnost provést daný útok. V těchto případech se jedná o selhání a neschopnost aktérů kybernetického terorismu uskutečnit kyberteroristický útok, který by splňoval definiční znaky. Pasivní využití kybernetických nástrojů je možné sledovat především v médiích určených pro vzájemnou komunikaci, sdílení dat, propagandu a propagaci. Tento smysl použití nelze popřít díky mnoha důkazům, díky nimž byl tento závěr prokázán.

Otázka vývoje cílů kybernetického terorismu je spojena s jejich využitelností v oblasti ICT. Kritická informační infrastruktura je brána jako prvotní možný cíl kyberteroristických útoků. Inovace nových součástí kritické infrastruktury, které jsou odkázány na ICT, tuto potencionální paletu rozšiřují. Je důležité si uvědomit, že v případě úspěšného útoku na oblast ICT jsou možné velké ztráty na civilním obyvatelstvu kvůli jeho případné nefunkčnosti. Objekty ICT jsou však řízeny prostřednictvím vnitřních sítí, které eliminují závislost na internetu, nebo mají vysokou prioritu zabezpečení. Potencionální ohrožením pro tuto širokou oblast ICT, je využití

tajného agenta. Díky jeho útoku by mohlo dojít k odstavení či ovládnutí systému a ohrožení bezpečnosti fungování ICT. Objekty ICT jsou primárně vybaveny bezpečnostními systémy, které mají vysokou úroveň zabezpečení. Pro úspěšný útok je nutnost znát detailní fungování všech úrovní včetně kontrolních údajů a autorizačních oprávnění.

Predikce uplatnění kyberterorismu prostřednictvím ekonomicky, politicky, nábožensky nebo ideologicky motivovaných skupin a jednotlivců proti informačním a počítačovým systémům, počítačovým datům a programům, kde tíženým výsledkem je způsobit násilí na straně nebojových cílů, lze vidět spíše v užití pasivních zbraní kybernetického terorismu, které mohou získat utajovaná data, které by mohl být dále využity pro vedení tradičního způsobu boje. Kybernetický terorismus je patrný hlavně díky globální internetové síti, která je sdělovacím a komunikačním médiem a rozvoj tohoto trendu se očekává i v budoucnu.

Virtuální prostor se už plnohodnotně dostal do zájmu bezpečnostně – politických institucí, které v něm spatřují citelnou možnost využití či zneužití pro diverzní akce nebo terorismus. Zvýšený mediální zájem vzbuzuje kybernetický terorismus díky útokům na státy, organizace či veřejný sektor. Pojetí kyberterorismu a jemu blízkému kybernetického zločinu trpí zaměřováním těchto definicí. Díky tomuto nesprávnému určování, které je způsobeno i prostřednictvím médiím, může dojít v očích veřejností k nesprávnému vnímání skutečnosti. To může mít za následek neúměrné vnímání kyberterorismu vzhledem k jeho současným možnostem.

Přítomné riziko potencionálních kybernetických útoků a jeho následků je vysoké. Šance na jeho provedení díky výše uvedeným důvodům je nezanedbatelné. Aktuální bezpečnostní opatření jsou při nejmenším v námi známém světě brány jako dostatečná. Tomuto závěru se vymyká několik incidentů, které jsou demonstrací vysoké schopnosti jedinců a hackerských skupin. Jestliže bude pokračovat vysoký zájem v oblasti protiteroristické politiky, legislativy a preventivních bezpečnostních opatření tak je předpoklad, že současný stav bude s největší pravděpodobností zachován.

SEZNAM POUŽITÝCH ZDROJŮ

Literární zdroje

● CLARKE, R. *Cyber war*. New York : Harper Collins, 2011. 320 s. ISBN 978-0-06-196223-3.

● DUNNIGAN, J. F. *Bojiště zítřka: tváří v tvář globální hrozbě kybernetického terorismu*. Vyd. 1. Praha: Baronet, 2004, 356 s. ISBN 80-721-4642-4, s. 224.

● GOLDSMITH, J. a WU, T. *Kdo řídí Internet? Iluze o světě bez hranic.* Praha : Dokořán a Argo, 2008. 270 s. ISBN 978-80-7363-184-0.

● HOS, M. Terorismus a počítače. In. *Terorismus a my*. Praha: Computer Press, 2001. 216 s. ISBN 80-7226-584-9.

● JANCZEWSKI, L; COLARIK, A. *Managerial Guide for Handling Cyber-Terrorism and Information Warfare*. London: IGI Global, 2005. 229 s. ISBN 978-1-59140-991-5.

● JIROVSKÝ, V. *Kybernetický kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemstvích.* Praha : Granada, 2007. 284 s. ISBN 978-8024715612.

● MCQUADE III., S. *Encyklopedia of Cybercrime.* Westport : Greenwood, 2008. 232s. ISBN 978-0-313-33974-5.

● MIKA, O. J. *Současný terorismus: řešení krizových situací*. Vyd. 1. Praha: Triton, 2003, 92 s. ISBN 80-725-4409-8.

● POŽÁR, Josef a kol.: *Základy teorie informační bezpečnosti*. 1. vyd. Praha : Vydavatelství Policejní akademie ČR, 2007. 219 s. ISBN 978-80-7251-2.

● STRMISKA, Maxmilián. Terorismus a demokracie. Brno: Masarykova univerzita, 2001. ISBN 80-210-2755-X.

● SZOR, Peter. *Počítačové viry – analýza útoku a obrana.* Brno: Zoner press, 2006. 608 s. ISBN 80-86815-04-8.

● VERTON, D. *Zpovědi mladých hackerů.* Praha : Helion S.A., 2002. 224 s. ISBN 83-7361-243-2.

Legislativní zdroje

● ČESKO. Zákon č. 181/2014 Sb. o kybernetické bezpečnosti v platném znění. In *Zákony pro lidi*. Dostupné z WWW: < http://www.zakonyprolidi.cz/cs/2014-181#cast1>.

Tištěné dokumenty

● BARBER, R. *Hacking Techniques. The tools that hackers use, and how they are evolving to become more sophisticated.* Computer. Fraud and Security. 2003, č. 3, p. 9-10.

● JANOUŠEK, M. Kyberterorismus: terorismus informační společnosti. In. Obrana a strategie rok 2006, č. 2, roč. 6. str. 60-66. ISSN 1214-6463.

● LUKÁŠOVÁ, K. *Škodlivý obsah na internetu*. In: *AUC IURIDICA: Kybernetická kriminalita*. Praha: Karolinum, 2013, roč. 2012, č. 4, str. 7 – 22. ISSN 03230619.

Kvalifikační práce

● ABERLE, P. *Budoucnost kybernetického terorismu*. Brno, 2010. Diplomová práce. Fakulta sociálních studií Masarykovi univerzity, Katedra politologie. Vedoucí diplomové práce : Mgr. Martin Bastl, Ph. D.

● BASTL, M. *Kybernetický terorismus: studie nekonvenčních forem boje v kontextu soudobého válečnictví.* Brno, 2007. Disertační práce. Fakulta sociálních studií Masarykovi univerzity, Katedra politologie. Vedoucí disertační práce : prof. PhDr. Maxmilián Strmiska, PhD.

● BIČIANOVÁ, A. *Kybernetický terorizmus a počítačová kriminalita.* Zlín, 2008. Diplomová práce. Univerzita Tomáše Bati ve Zlíně, Fakulta aplikované informatiky. Vedoucí diplomové práce : Ing. Radek Šilhavý, Ph. D.

● HÁK,I. *Moderní počítačové viry.* Hradec Králové, 2005. Bakalářská práce. Univerzita Hradec Králové, Fakulta informatiky a managementu, Katedra informatiky a kvantitativních metod. Vedoucí diplomové práce : Doc. RNDr. Josef Zelenka, CSc.

Elektronické zdroje

● *AEC Produkty*. [online]. [cit.2015-02-03]. Dostupné z WWW: <http://www.aec.cz/cz/produkty>.

● Amazon chce rozvážet balíčky vlastními létajícími drony. *IDnes.cz* [online]. 2013 [cit. 2015-03-20]. Dostupné z WWW: <http://ekonomika.idnes.cz/amazon-testuje-bezpilotni-letouny-du3-/ekozahranicni.aspx?c=A131202_081758_ekozahranicni_maq>.

● Americká Nevada jako první na světě povolila provoz robotických aut. *Technet.cz* [online]. 2012 [cit. 2015-03-20]. Dostupné z WWW: < http://technet.idnes.cz/americka-nevada-jako-prvni-na-svete-povolila-provoz-robotickych-aut-1go /tec_technika.aspx?c=A120223_171923_tec_technika_vse>.

● Američané dodají Ukrajině drony a terénní auta. *Novinky.cz* [online]. 2015 [cit. 2015-03-20]. Dostupné z WWW: <http://www.novinky.cz/zahranicni/amerika/363959-americane-dodaji-ukrajine-drony-a-terenni-auta.html>.

● BBC News. Iran 'fends off new Stuxnet cyber attack'. BBC News [online]. 25. December 2012, [cit. 2015-01-03]. Dostupný z WWW: <http://www.bbc.com/news/world-middle-east-20842113>.

● BIS. *Výroční zpráva Bezpečnostní informační služby za rok 2013*. BIS. [online]. [cit.2015-01-05]. Dostupné z WWW: <http://www.bis.cz/n/2014-10-27-vyrocni-zprava-2013.html>.

● Blaunstein, Max. Virus Stuxnet zasáhl ruskou jadernou elektrárnu i Mezinárodní vesmírnou stanici. [online]. 12. November 2013, [cit. 2015-01-03]. Dostupný z WWW: <http://eretz.cz/2013/11/virus-stuxnet-zasahl-ruskou-jadernou-elektrarnu-mezinarodni-vesmirnou-stanici-video/>.

● Britové už na Ukrajině cvičí vojáky. Z Moskvy zní kritika. *Novinky.cz* [online]. 2015 [cit. 2015-03-20]. Dostupné z WWW: <http://www.novinky.cz/zahranicni/evropa/364750-britove-uz-na-ukrajine-cvici-vojaky-z-moskvy-zni-kritika.html>.

● Český rozhlas. Před 75 lety vyvolala rozhlasová hra Válka světů paniku z invaze mimozemšťanů. *Český rozhlas* [online]. 2013 [cit. 2015-03-20]. Dostupné z WWW: <http://www.rozhlas.cz/zpravy/historie/_zprava/pred-75-lety-vyvolala-rozhlasova-hra-valka-svetu-paniku-z-invaze-mimozemstanu--1274601>.

● Český rozhlas. Rada pro kybernetickou bezpečnost bude řešit útoky na české weby. [online]. 12. března 2013, [cit. 2015-01-03]. Dostupný z WWW: <http://www.rozhlas.cz/zpravy/politika/_zprava/rada-pro-kybernetickou-bezpecnost-bude-resit-utoky-na-ceske-weby--1186318>.

● ČT24. Hackeři se mstí za odstavení serveru megaupload.com. *Česká televize* [online]. 20. ledna 2012, [cit. 2015-01-03]. Dostupný z WWW: <http://www.ceskatelevize.cz/ct24/svet/161230-hackeri-se-msti-za-odstaveni-serveru-megaupload-com/>.

● European Cybercrime Centre. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2013 [cit. 2015-03-20]. Dostupné z WWW: <http://en.wikipedia.org/wiki/European_Cybercrime_Centre>.

● Gang vyráběl bomby, které šlo odpálit mobilem. *Novinky.cz* [online]. 2006 [cit. 2015-03-20]. Dostupné z WWW: <http://www.novinky.cz/krimi/104504-gang-vyrabel-bomby-ktere-slo-odpalit-mobilem.html>.

● Kaspersky Lab spolupracuje s biohackery. *ITBIZ* [online]. 2015 [cit. 2015-03-20]. Dostupné z WWW: <http://www.itbiz.cz/tiskove-zpravy/kaspersky-lab-spolupracuje-s-biohackery>.

● Národní strategie kybernetické bezpečnosti České republiky na období let 2015 – 2020. [online].[cit.2015-01-05]. Dostupné z WWW: <http://www.cybersecurity.cz/data/navratil2014.pdf>.

● Největší hackerský útok v dějinách internetu zasáhl Bílý dům i FBI. [online]. 20. ledna 2012, [cit. 2015-01-03]. Dostupný z WWW: <http://www.novinky.cz/internet-a-pc/bezpecnost/256763-nejvetsi-hackersky-utok-v-dejinach-internetu-zasahl-bily-dum-i-fbi.html>.

● New York Times Asia Pacific. China Is Tied to Spying on Europe Diplomats. [online]. 10. prosince 2013, [cit. 2015-01-03]. Dostupný z WWW: <http://www.nytimes.com/2013/12/10/world/asia/china-is-tied-to-spying-on-european-diplomats.html>.

● Nové hrozby - kybernetické dimenze. *NATO Review* [online]. 2011 [cit. 2015-03-20]. Dostupné z WWW: <http://www.nato.int/docu/review/2011/11-september/Cyber-Threads/CS/index.htm>.

● Obrat této společnosti činil např. v roce 2011 48,07 miliard USD. Zdroj: AMAZON.COM, INC.: Commission File No. 000-22513. *UNITED STATES SECURITIES AND EXCHANGE COMMISSION* [online]. [cit. 2015-03-20]. Dostupné z WWW: <http://www.sec.gov/Archives/edgar/data/1018724/000119312512032846/d269317d10k.htm>.

● Shearer, Jarrad. W32.Stuxnet. [online]. 5. May 2011, [cit. 2015-01-03]. Dostupný z WWW: <http://www.symantec.com/security_response/writeup.jsp?docid= 2010-071400-3123-99>.

● Šéf NBU: Rusové použili na Krymu i kybernetické útoky. [online]. 5. března 2014, [cit. 2015-01-03]. Dostupný z WWW: <http://www.parlamentnilisty.cz/arena/monitor/Sef-NBU-Rusove-pouzili-na-Krymu-i-kyberneticke-utoky-306204>.

● Tvrdá rána pro Islámský stát: Anonymous podnikli masivní útok. *EuroZprávy.cz* [online]. 2015 [cit. 2015-03-20]. Dostupné z WWW: <http://zahranicni.eurozpravy.cz/blizky-vychod/113210-tvrda-rana-pro-islamsky-stat-anonymous-podnikli-masivni-utok/>.

● Typologie terorismu: Kybernetický terorismus. *Ministerstvo vnitra ČR* [online]. 2011 [cit. 2015-03-19]. Dostupné z WWW: <http://www.zakomunistu.cz/>.

Ostatní zdroje

● Rozhovor s panem Ing. Jiřím Kachyňou, IT specialistou firmy Letoplast s.r.o., ze dne 1. března 2015.

SEZNAM TABULEK A OBRÁZKŮ

SEZNAM PŘÍLOH

Příloha I.

Pojmový aparát

Vybrané pojmy z textu byly zpracovány na základě několika elektronických zdrojů, jejichž seznam je dostupný na konci pojmového aparátu v oddílu použité zdroje. Některé pojmy jsou doslovně citovány, vždy s uvedením zdroje odkud doslovná citace pochází. Dostupnost všech zdrojů byla překontrolována k datu 30. března 2015.

Cracking: dle významu anglického slova (lámat) se jedná o prolamování softwarového zabezpečení. Často bývá spojováno s otázkou pirátství.

Cybersquatting: je označení pro registraci a následné užívání doménového jména ve zlé víře na úkor obchodní značky, názvu anebo jména jiné osoby.

Cyberstalking: použití Internetu nebo jiného elektronického prostředku, který využívá jedna osoba k obtěžování jiného uživatele (Airdump).

Červ: Podtřída viru. Červ se obvykle šíří bez účasti uživatele, přičemž distribuuje své úplné kopie (případně pozměněné) v rámci sítí. Může spotřebovávat paměť nebo šířku pásma sítě, což může vést ke zhroucení počítače (Microsoft).

Deface útok: je v informatice druh zranitelnosti webové aplikace. Cílem útočníka je nahradit odpověď od serveru podvrženým dokumentem.

DDoS, DoS: (česky odmítnutí služby) je technika útoku na internetové služby nebo stránky, při nichž dochází k přehlcení požadavky a pádu nebo minimálně nefunkčnosti a nedostupnosti pro ostatní uživatele (Airdump).

Hacker: je počítačový specialista či programátor s detailními znalostmi fungování systému, dokážou ho výborně používat, ale především si ho upravit i podle svých potřeb.

Hacking: neautorizované pronikání do cizích počítačů, sítí nebo systémů. Cílů této činnosti může být více: od finančního zisku prodejem dat nebo získáním výhody plynoucí z vlastnictví těchto dat až po např. cílené poškození daného subjektu (Slovník cizích slov).

Phising: podvodná technika používaná na Internetu k získávání citlivých údajů (hesla, čísla kreditních karet atd.) od obětí útoku. Jejím principem je rozesílání e-mailových zpráv, které se tváří jako oficiální žádost banky či jiné podobné instituce a vyzývají adresáta k zadání jeho údajů na odkazovanou stránku (Saferinternet).

Piráctví: Nejčastěji vnímáno ve spojitosti s porušováním autorského práva. Jedná se o úmyslnou distribuci počítačových dat, které jsou chráněny autorským zákonem.

Phreaking: souhrnný termín vloupávání se telefonních systémů, převážně za účelem vedení bezplatných hovorů, odposlouchávání nebo narušování telefonních služeb (Airdump).

Spam: Nevyžádaná reklama zasílaná elektronickou cestou (převážně e-mailem) náhodně vybranému počtu lidí z databáze za účelem obchodního sdělení. V české legislativně SPAM upravuje předpis č. 480/2004 Sb. § 7 Šíření obchodních sdělení, který zakazuje zaslání elektronické pošty za účelem šíření obchodního sdělení v případě, že není jasně označena jako obchodní sdělení, utajuje totožnost odesilatele a je zaslána bez platné adresy, kde je možné provést zrušení tohoto zasílání.

Škodlivý software: Škodlivý software (označovaný jako malware) je takový software, který byl vyvinut s úmyslem způsobit škody. Tento software může zahrnovat viry, červy, spyware a jiné škodlivé programy, které se mohou skrývat v počítači a značně zpomalit jeho výkon. Lze jej rovněž využít ke sledování zvyklostí týkajících se procházení Internetu, krádežím hesel a dokonce může umožnit útočníkovi získat vládu nad počítačem (Microsoft).

Trojský kůň: Počítačový program, který se jeví jako užitečný, ale ve skutečnosti působí škody. Trojští koně se šíří tím, že jsou uživatelé zlákáni k otevření programu, protože si myslí, že pochází z legitimního zdroje. Tento typ software může umožnit dálkovou správu počítače útočníkem (Microsoft).

Y2Y (Year 2 Kilo): označuje problém roku 2000, respektive problémy související s přechodem do druhého tisíciletí. Především se kvůli vysoké ceně hardware v osmdesátých a počátkem devadesátých let šetřilo každým bitem. Proto se i datum ukládalo v podobě dd-mm-yy, tedy „19“ se v letopočtu vynechávala. Další příčinou Y2K byla i snaha programátorů si zjednodušovat práci, neboť s dvoumístným letopočtem bylo mnohem snazší pracovat.

Warez: je termín počítačového slangu označující autorská díla, se kterými je nakládáno nelegálně, zejména v rozporu s autorským právem.

Použité zdroje:

Airdump: http://www.airdump.cz

Microsoft: http://www.microsoft.com/cs-cz/

Slovník cizích slov: http://www.slovnik-cizich-slov.net

Safeinternet: http://www.safeinternet.cz