Terorizmus a kyberkriminalita
Terrorism and Cybercrime

Bc. Erika Verešová

Diplomová práca
2015

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2014/2015

ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Erika Verešová**
Osobní číslo:	**A13871**
Studijní program:	**N3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**kombinovaná**
Téma práce:	**Terorismus a kyberkriminalita**
Téma anglicky:	**Terrorism and Cybercrime**

Zásady pro vypracování:

1. **Zpracujte rešerši literatury, která se vztahuje ke zpracovávanému tématu.**
2. **Vymezte fenomenologické a etiologické otázky spojené s terorismem, včetně sociálních a historických souvislostí.**
3. **Analyzujte aktuální situaci a možnosti aplikace moderních bezpečnostních prvků k eliminaci terorismu a jeho financování.**
4. **Zpracujte metodiku výzkumné části kvalifikační práce.**
5. **Výstupy výzkumu a analytické části kvalifikační práce využijte pro vlastní návrhy a opatření, výstupy statisticky vyhodnoťte a zpracujte**

Rozsah diplomové práce:

Rozsah příloh:

Forma zpracování diplomové práce: **tištěná/elektronická**

Seznam odborné literatury:

1. **CARR, C. Dějiny terorismu : dějiny války proti civilistům. Praha: Práh, 2002. 184 s. ISBN80-7252-063-6.**
2. **EICHLER, J. Terorismus a války na počátku 21. století. Praha: Karolinium, 2007. 354 s. ISBN 978-80-246-1317-8.**
3. **JIROVSKÝ, Václav. Kybernetická kriminalita -- nejen o hackingu, crackingu, virech a trojských koních bez tajemství. Praha: Grada, 2007. ISBN 978-80-247-1561-2.**
4. **MAREŠ, Miroslav. Terorismus v ČR. 1. vyd. Brno : Centrum strategických studií, 2005. 476 s. CSS 1. ISBN 80-903333-8-9.**
5. **POLČÁK, R., - GŘIVNA, T. Kyberkriminalita a právo (Cybercrime and the Law). Praha: AUDITORIUM, 2008. 220 pp. ISBN 987-80-903786-7-4. Zákon č. 40/2009 Sb.: Trestní zákoník. In: 40/2009 Sb. 8.1.2009.**

Vedoucí diplomové práce:	**PhDr. Mgr. Stanislav Zelinka** Ústav bezpečnostního inženýrství
Datum zadání diplomové práce:	**12. ledna 2015**
Termín odevzdání diplomové práce:	**15. května 2015**

Ve Zlíně dne 6. února 2015

L.S.

doc. Mgr. Milan Adámek, Ph.D.
děkan

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji diplomovou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- beru na vědomí, že pokud bylo k vypracování diplomové práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na diplomové práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně

.....
podpis diplomanta

ABSTRAKT

Cieľom diplomovej práce je analýza kyberútokov vo svete, v Českej a Slovenskej republike. Taktiež ich spojitosť s terorizmom a kybernetickým terorizmom a analýza aktuálnej situácie financovania terorizmu prostredníctvom počítačovej kriminality. Ďalej spôsoby, ako s týmito problémami bojujú samotné krajiny. Na záver by som rada navrhla určité zabezpečenia, ktoré by mohli situáciu kybernetického terorizmu a kybernetickej kriminality zlepšiť.

Kľúčové slová: terorizmus, kybernetický terorizmus, kyberpriestor, kybernetická kriminalita.

ABSTRACT

The aim of the thesis is the analysis of cyber-attacks in the world, the Czech Republic and Slovakia. Also their connection with terrorism and cyber-terrorism and analysis of the current situation of financing of terrorism through computer crime. Further ways to fight these problems the countries themselves . Finally, I would like to propose certain security that could make the situation cyber-terrorism and cyber-crime improve.

Keywords: terorism, cyber-terorism, cyber-space, cyber-crime.

Na tomto mieste by som rada poďakovala svojmu vedúcemu diplomovej práce Mgr. Phdr. Stanislavovi Zelinkovi za odborné pripomienky a cenné rady, ktorými prispel k jej spracovaniu.

OBSAH

ÚVOD

Nové informačné a komunikačné technológie v popredí s Internetom paria k najdôležitejším vynálezom dvadsiateho storočia. Počítačové technológie sa stali koncom dvadsiateho storočia dôležitou časťou celej spoločnosti. Tieto technológie sú súčasťou všetkých oblastí našich životov od dennej komunikácie až po riadenie procesov v jadrových elektrárňach. Tento nárast však pre nás neprináša iba pozitíva, ale aj veľkú hrozbu, ktorá vyplýva zo zneužitia týchto technológií.

Kybernetický terorizmus, alebo obecne informačné a komunikačné technológie a ich zneužívanie, vedie k ohrozeniu bežných užívateľov, ekonomických subjektov ale aj štátnych inštitúcii. Dobrá organizovanosť útokov v kyberpriestore sa zvyšuje. Problém kybernetických útokov Pentagon označil ako „hrozbu katastrofických rozmerov a vážne ohrozenie národnej bezpečnosti“ už v roku 1996. To, akú formu a rozmery má tento problém v dnešnej dobe je tiež predmetom mojej práce. Téma kybernetický terorizmus sa dostáva do popredia a je často pokladanou otázkou v médiách. Teroristické organizácie už nepoužívajú iba tradičné metódy boja, ale používajú informačné technológie, teda sa stávajú veľmi nebezpečnou súčasťou kyberpriestoru.

Táto práca sa zabýva fenoménom teroristických útokov v rámci kyberpriestoru. Budem sa venovať historickému vývoju terorizmu, ako takého, ale dôležitá časť na ktorú sa zameriam je kyberterorizmus. Venovať sa budem jeho formám, vývoju a novým metódam jeho využitia v dnešnej dobe. V praktickej časti rozoberiem momentálnu situáciu vo svete a v Českej a Slovenskej republike, hlavne najznámejšie útoky v posledných rokoch, ale tiež štatistiky kyberútokov a štatistiky s nimi spojené. Taktiež uvidíme, ako s týmto svetovým problémom bojujú najviac napádané štáty a ako sa táto situácia rieši v rámci Českej a Slovenskej republiky. Skúmanú oblasť som vymedzila na členské štáty NATO a Európsku úniu, v rozmedzí od prelomu dvadsiateho storočia až po dnešok.

I. TEORETICKÁ ČASŤ

1 TERORIZMUS

Už od dávnej minulosti sprevádza ľudskú spoločnosť násilie. Ak si na jednej strane myslia, že k povoleniu jednej strany je potrebný strach, neváhajú ho použiť. Násilie ma veľa podôb, ale tou najnebezpečnejšou je terorizmus. Terorizmus sa v poslednej dobe rozrástol do viacerých foriem. Dnes už pojem terorizmu neoznačuje len politicky motivovaný atentát, ale odráža sa v rôznych faktoroch ľudského chovania. Keďže náš vek je „informačný" objavuje sa špecifický a nebezpečný druh skrytej hrozby – kybernetický terorizmus.

1.1 Vymedzenie pojmu

Slovo teror je odvodené z latinského slova terrere, do slovenčiny ho môžeme preložiť ako hrozný, naháňať strach, zastrašovať či desiť. Pojem teror sa od pojmu terorizmus odlišuje absenciou politických cieľov a zameraním sa na konkrétne osoby. Obecne hovoríme o akomkoľvek použití organizovaného násilia, zameraného proti nezúčastneným osobám k dosiahnutiu politických, kriminálnych alebo iných cieľov. Do moderných slovníkov sa dostal až vďaka francúzskemu jazyku v 14. storočí. Teraz by som spomenula niektoré z terajších definícií:

- Hrozba alebo použitie násilia na dosiahnutie politických cieľov. Môže ho realizovať štát proti obyvateľstvu alebo organizáciám či iným štátom, alebo občania proti štátu, jeho inštitúciám, prípadne iným obyvateľom. (Kiczko a kol., s.261) [1]
- Súhrn protihumánnych metód hrubého zastrašovania politických odporcov hrozbou sily a použitia rôznych foriem násilia. Vedľa individuálneho terorizmu existuje terorizmus skupín, niektoré koordinujú svoju činnosť na medzinárodnej úrovni (medzinárodný terorizmus). (Český encyklopedický slovník, 1993) [18]
- Terorizmus – v politike používanie teroristických prostriedkov k zastrašovaniu politických odporcov a ovplyvňovaniu verejného mienenia. Cieľom terorizmu je zvyčajne vyvíjanie extrémneho politického nátlaku na jednotlivca alebo častejšie na celé skupiny obyvateľov. (Encyklopédia politiky, 1990) [19]
- Terorizmus, politické násilie zamerané na vládu, ale často ohrozujúce aj radového občana. Jeho cieľom je vytvoriť atmosféru strachu, v ktorej by vláda splnila požiadavky teroristov. (Blackwellova encyklopédia politického myslenia, 2000) [20]
- V súčasnosti sa za terorizmus označujú také akty teroru, ktoré vychádzajú od vládnych protivníkov. Rozsah činností, ktoré tento termín zahrňuje, je veľmi široký,

môžeme však vymenovať štyri hlavné formy: úkladné vraždy a atentáty, bombové útoky, držanie jednotlivcov ako rukojemníkov a v nedávnej dobe tiež únosy lietadiel. (Oxfordský slovník svetovej politiky, 2000) [21]

- Terorizmus je možné charakterizovať ako globálny jav, ktorý nie je obmedzený na konkrétny región či krajinu, ale môže zasiahnuť ktorúkoľvek krajinu na svete. Medzníkom v tomto vývoji sa stal 11. september 2001. Od tohto dátumu sa na globálnej úrovni diskutuje o príčinách terorizmu a tiež o spôsoboch ako mu čeliť. Samotné vymedzenie pojmu terorizmus prešlo určitým vývojom. V období pred druhou svetovou vojnou bol terorizmus vnímaný ako „zvláštna metóda ozbrojeného boja“ (Strmiska, 2001). [2]
- Walter Laqueur (1978) vymedzuje terorizmus ako použitie násilia, resp. hrozba násilím s cieľom dosiahnutia politických cieľov. Samotné teroristické metódy nemusia byť pritom doménou „šialencov“. Terorizmus a jeho metódy môžu byť výsledkom veľmi racionálnej kalkulácie. [3]
- Terorizmus je ekvivalentom vojenských zločinov v období mieru. (Enciklopédia svetového terorizmu, 2001)
- Terorizmus je plánované, premyslené a politicky motivované násilie, zamerané proti nezúčastneným osobám, slúži k dosiahnutiu stanovených cieľov. (Ministerstvo vnútra ČR, 2009)

Definície terorizmu sa časom menia, napríklad na začiatku boli teroristickými činmi označované aj činy kriminálne, ktoré nemali za úlohu žiadny politický cieľ ani zastrašenie protivníkov. Každopádne sú si definície podobné a to v tom, že sa jedná o útok vedený proti civilistom, inými slovami, nebojovým cieľom, za účelom dosiahnutia politického cieľa. Rozdielne sú aj definície slova „terorista“. Raz je nazývaný príslušníkom bojového hnutia, druhý krát sa označuje ako bojovník za slobodu. Zákonná definícia terorizmu podľa Alexa P. Shmida *„Terorizmus je ekvivalentom vojenských zločinov v období mieru.“* je považovaná za najvhodnejšiu z hľadiska zjednotenia postupov pri zachádzaní s teroristami a to tiež z dôvodu, že vylučuje niektoré formy násilia, ktoré v súčasnosti vlády niektorých štátov označujú slovom terorizmus. Ak by sa stalo, že medzinárodné spoločenstvo by prijalo takúto definíciu, nemôže už nikto teroristov vydávať za bojovníkov za slobodu.

Svetová encyklopédia terorizmu definuje štyri skupiny, ktoré sa líšia svojimi názormi a chápaním terorizmu: [2]

- **Vedci** – hľadajú obecný pojem, debatujú bez toho, aby sa báli bezprostredného útoku na svoje osoby.
- **Vládne autority** – hrozby a útoky sa ich priamo dotýkajú a poznamenávajú ich.
- **Verejnosť –** často mení svoje postoje, ich názor je vo veľkej miere ovplyvňovaný médiami.
- **Názory teroristov a ich sympatizantov –** veria a sú presvedčení, že žijú pod zlou nadvládou, a tak svojimi činmi toto jednanie ospravedlňujú. Cieľom teroristov je prilákať pozornosť, vyvolať atmosféru strachu, destabilizovať štát a vyprovokovať ho k tvrdej odplate či vynútiť si zmenu vnútornej alebo zahraničnej politiky.

Každý jedinec má na terorizmus iný názor. Preto sú odborníci skeptickí k vytvoreniu univerzálnej definície. Aby bolo možné lepšie pochopiť pôvod slova, je potrebné nahliadnuť do histórie.

1.2 História terorizmu

Obecne môžeme konštatovať, že skúmanie vývoja terorizmu je pomerne zložitá záležitosť, ktorá je založená skôr na subjektívnom pohľade a zhodnotení danej situácie.

Problematikou historického vymedzenia vývoja terorizmu jednoznačne priamo súvisí s históriou vedenia vojen s terorom páchaným na civilnom, v boji nezúčastnenom, obyvateľstve. Toto historické vnímanie vývoja terorizmu sa teda priamo odvíja od časového, geografického a ideového pôsobenia. [12]

1.2.1 Historická etapa (do konca 17. storočia)

Pojem terorizmus je pomerne mladý, preto niet divu, že už dlho pred tým, ako zámerné vojenské útoky na civilistov, ako metóda ovplyvňovania politického chovania štátu, začali byť terorizmom nazývané, mala táto taktika celú radu iných názvov. Už 500 rokov p.n.l čínski vojenskí vodcovia Sun-c´ a jeho potomok Sun Pin využívali postupy vyhovujúce kategórii terorizmu. Sám Sun-c´ vo svojom diele *Umenie vojny* hovoril o taktikách obvyklých či neobvyklých. K obvyklým radil učebnicové spôsoby, ktoré ale pokladal za predpokladateľné. Oproti nim pokladal neobvyklé, ktoré vychádzali z pružných a pohyblivých síl použitých vynaliezavým, netypickým a ťažko predvídateľným spôsobom. Japonský bojovník Mijamoto Musaši vo svojej práci *Kniha piatich kruhov* hovorí o stratégii „telo namiesto meča“, ktorá bola hodnotená ako teoretická forma boja. [12]

Od dôb rímskej ríše až do konca 17. storočia bolo zvažované neobvyklé použitie vojenských jednotiek v rámci tzv. *ničivých vojen*. Rimania tiež používali pojem trestná vojna.

Za určitý druh ranného terorizmu sa dá tiež považovať činnosť islamskej sekty *Haš-Iším* v dobe križiackych výprav, ktorá je známa svojou činnosťou hlavne v oblasti Perzského zálivu. Jednalo sa o skupinu stredovekých šíitských moslimov, ktorí najskôr založili sektu známu ako *ismá´ilíje,* a od nich sa pod vedením Peršana Hassani as-Sabbaha oddelila fanatická vražedná sekta moslimov, známa ako kult *asasinov*. Táto sekta zamestnávala zabijakov, ktorí často pod vplyvom drog vraždili pre dosiahnutie svojich politických cieľov. Považovali sa za božích vyslancov a svoje činy za božiu vôľu. K dosiahnutiu náboženskej extázy používali hašiš a následne vraždili kresťanov, ale aj moslimov, ktorých považovali za nepriateľov svojej viery a svojej sekty.

Podľa M. Mareša bola určitou vlnou špecifického násilia s teroristickými prvkami tiež inkvizícia. Jednalo sa v podstate o prvú inštitúciu katolíckej cirkvi či španielskych a portugalských panovníkov, ktorá sa mala vyrovnať s kacírstvom. Stredoveká inkvizícia bola spočiatku odpoveďou cirkvi na rastúci vplyv heretických hnutí, zvlášť katarov a valdenských. Cirkev v týchto hnutiach videla ohrozenie kresťanského učenia a autority cirkvi. Neskôr ale začala svoje postavenie zneužívať na získavanie majetkov a bohatstva, ktoré po odsúdení obžalovaného prepadlo v ich prospech. Inkvizícia k týmto účelom používala veľmi tvrdé praktiky, ktoré boli zložené z psychického a fyzického týrania. Nebolo málo prípadov, kedy trest končil smrťou, obesením alebo upálením.

1.2.2 Nacionalistická etapa (začiatok 18. storočia až do roku 1913)

Medzi násilie s teroristickými aspektmi v období nacionalistickej etapy je možno radiť násilné útoky zamerané proti civilistom, ktoré boli počiatkom 18. storočia dôsledok ruskotureckej vojny vedenej na Balkáne. V roku 1716, kedy rakúska armáda porazila početné turecké sily v bitke, ktorá bola predzvesťou rakúskeho dobytia Uhier. Ruská armáda už dobila krymský chanát a potom napochodovala do Bukurešti, čím výrazne zmenšila územie, ktoré držali Turci v Európe. Pri neustálom ustupovaní sa však Turci zamerali viac na terorizovanie obyvateľov svojich zostávajúcich európskych provincii, než na boj s nepriateľom. To však viedlo k formovaniu miestneho odporu a tureckým vojakom sa začalo dostávať odplát, čím došlo k zvečneniu cyklu masových vrážd a odviet, čo charakterizuje chovanie kresťanov a moslimov v tejto oblasti dodnes. [12]

Prvky terorizmu je možné pozorovať v období kolonizácie Ameriky, kedy v priebehu niekoľko storočí podnecovali akty krutosti jednej strany odvetný teror zo strany druhej. Vzťahy medzi novými prichádzajúcimi osadníkmi a indiánmi časom degenerovali na vzájomné terorizovanie. Bitky nekončili výhrou a porážkou nepriateľa, ale úplným zmasakrovaním. Samozrejme, celú dobu vojen hnutí odporu amerických indiánov, väčšinou znova trpeli len obyčajní ľudia. Napríklad v roku 1782 zmasakrovali osadnícke domobrany mesta Gnadehutten v Ohiu pensylvánske domobrany a zajatého veliteľa plukovníka Crawforda upálili.

Nie vždy sú prvky terorizmu brané rovnako, napríklad podľa Hoffmanna, sa prvé známky terorizmu objavujú až v súvislosti s jakobínskou diktatúrou, v období Veľkej francúzskej revolúcie v rokoch 1793 až 1794. V tej dobe bol systém vedúci k presadeniu poriadku po predchádzajúcom anarchistickom období označovaný *„réégime de la terreur“*. Podľa mienenia jeho vykonávateľov, bol tento pojem paradoxne spojovaný s ideálmi cnosti a demokracie.

Nacionalizmus ako politická veličina začala naberať sily až v priebehu 19. storočia, kedy si niektorí ľudia žijúci v mnohonárodných štátoch uvedomili príslušnosť k určitej komunite. Začali si vyberať svojich vodcov a tvoriť vlastné zákony. Postupom času, tak došlo s výbuchu roztrúseného medzinárodného politického násilia, ktoré dnes niektorí historici interpretujú ako precedens, z ktorého by mohol byť vyvodený dnešný prístup k terorizmu. Páchatelia tohto násilia, hromadne nazývaný „anarchisti“, bežne využívali individuálne vraždy ako aj bombové atentáty na vojenské jednotky, policajtov a súkromné bezpečnostné sily v priemysle na upútanie pozornosti, ale aj k boju proti zvyšujúcim sa rozdielom v bohatstve a spôsobe života medzi ekonomickými triedami, ktoré vznikli v dôsledku priemyslovej revolúcie. Anarchisti šírili strach nielen medzi bohatými ľuďmi v Európe a Amerike, ale tiež medzi priemernými občanmi, ktorí bývali náhodnými obeťami vo vášnivej a dlhodobej bitke, prebiehajúcej po celom západnom svete. Je ale iróniou, že až súčasným teroristom sa podarilo vybudovať medzinárodnú armádu s nesmierne ničivým potenciálom.

1.2.3 Etapa vojen (v rokoch 1914 až 1945)

Vyhľadávať a hodnotiť prvky terorizmu v období, kedy bol svet ničený dvoma po sebe nasledujúcimi svetovými vojnami, je pomerne problematické. Významnou skutočnosťou pri skúmaní histórie terorizmu totiž je, že až do konca druhej svetovej vojny bola považovaná väčšina násilných incidentov proti civilistom páchaná vo vyhlásených otvorených

konfliktoch, zatiaľ čo terorizmus neobsahuje žiadne otvorené vyhlásené nepriateľstvá. Preto je tiež možné v súvislosti s etapou vojen chápať terorizmus ako krajné prejavy aktu násilia s cieľom donútiť protivníka, aby sa podriadil našej vôli. Ak sa budeme držať spoločenského znaku, ktorý bol pre vymedzenie teroristického chovania stanovený, dá sa konštatovať, že násilie bolo na civilnom obyvateľstve páchané neustále. Nepopierateľným dôkazom boli napríklad rozsiahle etnické čistky počas druhej svetovej vojny. V priebehu holokaustu vyvraždili Nemci vo svojich vyhladzovacích táboroch 6 miliónov Židov, milióny sovietskych zajatcov, najmenej 500 000 Rómov, homosexuálov, mentálne a fyzicky hendikepovaných ľudí.

Vedľa týchto zjavne teroristických praktík boli počas obidvoch svetových vojen volené i určité vojenské postupy, ktoré primárne neboli namierené proti civilistom, napriek tomu to na nich malo určitý negatívny vplyv.

V období 2. svetovej vojny bol najväčší aktér teroru bezpochyby nacistický vodca Adolf Hitler, ktorému sa naskytla prvá príležitosť k zámernému vedeniu vojny nie len proti armáde, ale aj proti civilistom, v rokoch 1940 a 1941 v leteckej vojne proti Británii. Druhú mu poskytol plán vyskúšaný už v Poľsku, ale zdokonalený až v roku 1941, pri útoku na Rusko, a síce zabíjať všetkých občanov na dobytom území.

V tomto období sa ale k útokom proti civilistom zámerne uchyľovali i spojenecké armády. Napríklad tzv. „strategické bombardovanie“, ktoré bolo oficiálne zamerané na zničenie nemeckej priemyslovej výroby a infraštruktúry, bolo realizované bombardovaním otvorených miest z veľkých výšok a tým prinášalo veľké straty na životoch civilistov. Priaznivcom týchto praktik bol mimo iných Winston Churchill, ktorý prehlásil, že účelom pokračujúcich náletov je „spôsobiť nepriateľovi čo najviac popálenín a krvácania“.

Ani Spojené štáty nemali pri útokoch proti civilistom príliš veľké zábrany. Dôkazom je jednanie pri odvete proti Japonsku, ako pomsta za napadnutie Pearl Harbor.

1.2.4 Etapa studenej vojny (1946 až 1989)

V posledných rokoch došlo v oblasti terorizmu k jeho veľkému rozmachu. Objavili sa nielen nové formy terorizmu, ale aj spôsoby jeho realizácie.

Pojem „studená vojna“ začali niektorí americkí politici používať už od roku 1946 a na oficiálnej úrovni ju prvý krát vyslovil Bernard Baruch. Niektorí tento pojem posúvajú ešte

pred rok 1946 a to napríklad v spojení so zhodením jadrových bômb na Hirošimu a Nagasaki.

Etapa studenej vojny sa od ostatných líši masívnym nárastom medzinárodného terorizmu. Za hlavný začiatočný podnet tohto nárastu môžeme považovať dohasínanie dvoch svetových vojen a súčasné očakávanie vzniku tretieho celosvetového konfliktu. Toto očakávanie trvalo až do udalostí spojených s pádom Berlínskej steny, rozpadom Sovietskeho zväzu a rozpustením Varšavskej zmluvy. A práve nevyhlásenie konfliktu umocnilo skutočný nárast prejavov terorizmu. [3]

Jednotlivé teroristické útoky v priebehu celého obdobia studenej vojny svojou rozmanitosťou, povahou, rozsahom spôsobených strát a škôd predstavujú už prvky vojenskej taktiky.

Koniec 60. a začiatok 70. rokov bol v znamení vrážd policajtov alebo sudcov zaoberajúcich sa vyšetrovaním terorizmu a v menšine boli zaznamenávané prvé atentáty v obchodných domoch. Neskôr sa medzi ciele teroristov dostali aj politici a zahraniční diplomati. V polovici 70. rokov sa útočníci preorientovali na veľké priemyslové firmy a ich predstaviteľov a koncom 70. rokov sa hlavným terčom teroristov stali dopravné lietadlá, vlaky, letiská a vlakové stanice. K atentátom sa skoro vždy prihlásila niektorá medzinárodná teroristická organizácia. [3]

Za významný konflikt v tomto období je považovaná vojna vo Vietname, v ktorej sa objavujú isté aspekty teroristického chovania. Spojené štáty sa totiž po skončení druhej svetovej vojny v tomto konflikte ešte jeden krát uchýlili k rozsiahlym útokom proti civilistom. Keď už sa na americké úsilie pozrieme z ktorejkoľvek stránky (na mimoriadnu statočnosť amerických vojakov či čisté úmysly, s ktorými mnohí muži a ženy vstupovali do vojenskej služby), rozkazy podávané z hora a chovanie sa operačných amerických výzvedných služieb (predovšetkým CIA) viedli k vojne proti civilistom. [3]

Začiatkom 70. rokov sa množili útoky proti diplomatom, obvykle diplomatickým zástupcom tretích strán. Teroristické skupiny napadali veľvyslanectvá v zahraničí, veľakrát len pre to, aby si zabezpečili publicitu. Atentáty mali vystrašiť tvorcov a vykonávateľov politického štátu. Koncom 70. rokov a začiatkom 80. rokov sa vedľa ľavicových skupín objavili aj skupiny pravicové (Južná Amerika, Španielsko, Taliansko). V týchto rokoch sa terorizmus veľkou mierou internacionalizoval, veľa skupín začalo operovať mimo územia štátu, na ktorom vznikli a ich ciele a zloženie nadobudlo medzinárodnú podobu. Začiatok 80. rokov je možné tiež považovať za obdobie masívneho nárastu novej formy teroristického

boja a to samovražedné útoky. Najčastejšie tieto útoky realizovali územia, ktoré boli dlhodobo okupované ako napríklad Palestína. Prvý takýto útok sa objavil po Izraelskom vpáde do Libanonu v roku 1982.

1.2.5 Etapa studeného mieru (od roku 1990 až po súčasnosť)

Po roku 1990 došlo hlavne k zmenám v motivácii terorizmu. Ideologický motivovaný terorizmus ustúpil a jeho miesto postupne nahradil terorizmus náboženský a nacionalistický. Pozornosť začala byť venovaná predovšetkým prejavom náboženského politického terorizmu, ultrapravicovému terorizmu a v neposlednej rade ZHN (niekedy tiež nazývaný superterorizmus, alebo ultraterorizmus), ktorý zahŕňa hrozbu či prípadné použitie zbraní hromadného ničenia.

Jeden z významných rysov zmeny povahy terorizmu, sa stal koncom 20. storočia, a to v rámci separatistických konfliktov, ktorých ohne sa rozšírili naprieč kontinenty. Európa tieto boje pocítila hlavne na juhu a to rozpadom Juhoslávie. Toto obdobie bolo charakteristické separatistickým terorizmom, ale tiež obráteným úsilím, a to vynakladaním veľkého úsilia na zjednotenie skôr rozdelených národov, ako Nemecka, Vietnamu či Kórey. Rozmanitosť tejto doby dokumentujú tieto tri vzájomne odlišné prípady: Východná Slavónia sa za extenzívneho medzinárodného monitorovania vrátila do Chorvátska, v Severnom Írsku bolo dosiahnutie prelomu v podobe dohody a v Kosove vypukla otvorená separatistická vojna.

Od prelomu 20. a 21. storočia je možné medzinárodný terorizmus už považovať za ozbrojený boj. Väčšinou je to tak, že jeden protivník má takú prevahu nad ostatnými, že slabá strana sa prikloní k neštandardnému riešeniu sporu. Tieto neštandardné postupy sú používané predovšetkým snahou slabšieho protivníka vyhnúť sa priamej konfrontácii. [5]

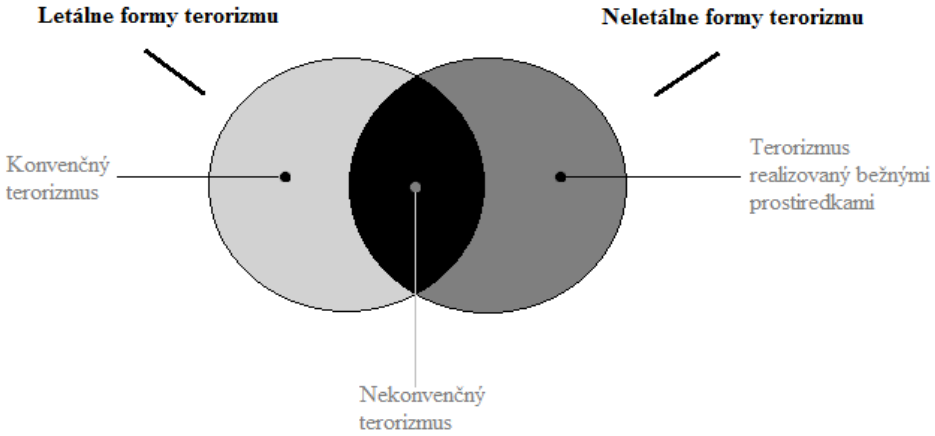
Táto etapa vývoja terorizmu je charakteristická nárastom miery využívania moderných sofistikovaných technológií, predovšetkým komunikačných, napr. mobilné telefóny alebo Internet. Ako aj vo výrobe, tak aj v terorizme to prináša veľké možnosti a terorizmus sa stáva globálnym. Jedným zo zástupcov globálneho terorizmu bol Usama bin Ládin, ktorý bol vodca skupiny sunnitských moslimov Al-Káida. Za dobu svojho pôsobenia spôsobila 29 teroristických incidentov, pri ktorých zranila 8863 osôb a 3460 zabila. Za hlavné smerovanie môžeme považovať obchodné, vládne, diplomatické a náboženské ciele. Charakteristickým rysom ich útokov je synchronizácia, tj. zasiahnutie viac cieľov súčasne. Jednalo sa napr. o súbežné útoky 7. augusta 1998 na americké veľvyslanectvo v Tanzánií a Keni,

útoky 11. septembra 2001, kedy dve unesené lietadlá zasiahli budovu Svetového obchodného centra v New Yorku a skoro súčasne jedno lietadlo zasiahlo budovu Pentagonu vo Virgínii, či synchronizovaný útok desiatich bômb umiestnených vo vlakoch, ktoré súčasne explodovali na štyroch rôznych miestach Madridu, presne po 30 mesiacoch od New Yorských útokoch, 11. marca 2004. [5]

1.3 Formy terorizmu

Teroristických útokov je v súčasnej dobe menej ako v minulosti, ale počet obetí neustále rastie. Tento nárast je spojovaný s nárastom foriem terorizmu, ktoré členíme na dve skupiny:

- letálne formy,
- neletálne formy.



Obrázok 1 - **Vzťah medzi letálnymi a neletálnymi formami terorizmu** [22]

1.3.1 Letálne formy terorizmu

Letálne formy terorizmu obsahujú základné prostriedky realizácie násilia a odlišujú sa len použitými prostriedkami. Z tohto dôvodu ich rozdeľujeme na dve podskupiny a to konvenčný a nekonvenčný terorizmus.

Do konvenčného terorizmu môžeme zaradiť tieto útoky:

- bombové útoky,

- ozbrojené útoky, podpaľačstvo, sabotáže,
- únosy osôb,
- únosy lietadiel,
- držanie rukojemníkov.

Do nekonvenčného terorizmu radíme:

- informačné operácie (Infop),
    - kyberterorizmus,
    - psychologické operácie (Psyop),
    - ekonomická vojna,
- prostriedky hromadného ničenie,
    - chemické zbrane,
    - jadrové zbrane,
    - rádiologické zbrane,
    - zbrane založené na biologickom účinku,
    - termické zbrane.

1.3.2 Neletálne formy terorizmu

Neletálne formy terorizmu tiež nazývané moderným alebo sofistikovaným terorizmom, keďže sú pri útokoch používané moderné nástroje, respektíve staré, ale novým spôsobom v kombinácii s letálnymi prostriedkami. Znova tieto formy delíme podľa prostriedkov používaných pri teroristickom útoku do dvoch podskupín, a to na: terorizmus realizovaný bežnými prostriedkami a nekonvenčný terorizmus.

Terorizmus realizovaný bežnými prostriedkami:

- pomocou výpočtovej techniky a internetu – kyberterorizmus,
- pomocou dopravných prostriedkov - napr. automobil, lietadlo, vlak, loď,
- mediálny terorizmus – psychologický terorizmus.

Do nekonvenčného terorizmu radíme:

- zbrane využívajúce optiku,
- zbrane využívajúce akustiku,
- zbrane využívajúce elektromagnetický pulz.

2 KYBERTERORIZMUS

„Terorismus ve světě představuje břečťan, který se v posledních letech "rozrostl" do nepředstavitelného množství odrůd a tvarů. Dnes již pojem terorismu neoznačuje pouze politicky motitovaný atentát či útok, ale odráží se v odporu vůči různým faktorům v mnoha různých úrovních lidského myšlení. A jelikož mírou moderní společnosti je schopnost využívání informací, objevuje se zde i velice specifický a nebezpečný druh skryté hrozby – kyberterorismus." [6]

Teroristi v dnešnej dobe používajú stále novšie a novšie techniky a prostriedky. Kybernetický terorizmus sa tak stal novou formou terorizmu. Môže mať podobu tradičného teroristického útoku, napríklad fyzickú likvidáciu budovy, ktorej každodenná prevádzka je závislá na počítačoch, ale tiež samozrejme aj virtuálnu prostredníctvom internetu. Čím vyspelejší štát, tým je možná väčšia zraniteľnosť prostredníctvom dátových sietí.

2.1 Vymedzenie pojmu

Vznik internetu so sebou priniesol aj vznik informačnej spoločnosti. Je to spoločnosť, kde kvalita života aj perspektíva sociálnych zmien a ekonomického rozvoja závisí na informáciách a schopnosti ich využitia, tj. informácia sa stáva kľúčovým faktorom takej spoločnosti. Jedná sa teda o spoločnosť založenú na intenzívnom využívaní komunikačných a informačných technológiách.

Pojem kyberterorizmus pochádza z anglického výrazu „cyberterrorism". Je to zloženie dvoch slov a to cyber, čo znamená niečo virtuálne a terrorism, čo znamená terorizmus. Kyberterorizmus, alebo kybernetický terorizmus môžeme chápať ako premietnutie klasického, už spomínaného terorizmu do virtuálneho sveta – kyberpriestoru.

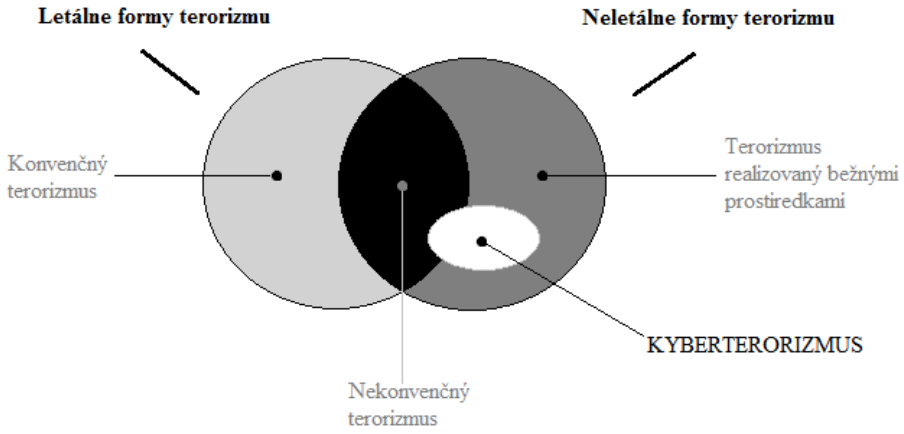
Kyberpriestor sa dá definovať ako nehmotný svet informácií, ktorý vznikne vzájomným prepojením informačných a komunikačných systémov. Toto prostredie nám slúži k vytváraniu, uchovávaniu, využívaniu a vymieňaniu informácií. Zahrňuje počítače a databázy prepojené komunikačnými systémami, ako napríklad celosvetovú sieť Internet. Kyberpriestor využíva nové možnosti komunikácie, ako sú napríklad emaily, webové stránky, počítačové siete, telefóny, faxy a videokonferencie. Jednoducho je to imaginárny priestor, na ktorý sa nevzťahujú obmedzenia fyzického sveta. Toto, okrem iného umožňuje vytváranie nových identít – užívateľ „opúšťa" svoje fyzické telo a pohybuje sa kyberpriestorom bez neho. Prostredníctvom kyberpriestoru sa dá teoreticky ohroziť infraštruktúru celého

štátu, napríklad zhodením serverov dôležitých inštitúcií. Pojem kyberpriestor je považovaný za svet virtuálnej reality, v ktorom sa odohrávajú každodenné úkony, napríklad emailová či telefonická komunikácia, alebo práve používanie internetu. Stal sa teda veľmi dôležitou súčasťou našich životov. Prvé počítače, ktoré tvorili internet, počítali s úplne iným využitím, napríklad ako nový komunikačný kanál. Postupom času sa táto sieť otvorila obyčajným užívateľom na ekonomické, marketingové a politické záujmy. Existujú samozrejme aj negatívne účinky tejto siete, napríklad závislosť na kyberpiestore, zneužívanie informácií v kyberpriestore, kybernetická kriminalita alebo kyberterorizmus ale tiež kybernetické vojny. Kyberpriestor je preto veľmi zraniteľný, veľa incidentov, ako sú špionáže, činy počítačovej kriminality či protesty proti niečomu.

Medzi základné vlastnosti kyberpriestoru patria:

- decentralizácia,
- globálnosť,
- otvorenosť,
- interaktívnosť,
- obsiahlosť veľkého množstva dát a informácií,
- riadenie iba užívateľmi,
- závislosť na infraštruktúre.

Jednou z hrozieb v kyberpriestore je kyberterorizmus. Jedná sa o neletálnu formu teroristickej činnosti realizovanej pomocou služieb, ktoré podporuje daná informačná alebo komunikačná sieť. Fyzická likvidácia inštitúcie či systému vedúca až k ľudským stratám môže byť sekundárnym dôsledkom tohto útoku. Ale väčšinou sa nejedná o primárny cieľ útoku. Preto sa dá neletálna forma považovať len za vonkajší obal.



Obrázok 2 - **Postavenie kyberterorizmu v jednotlivých formách terorizmu** [22]

Pod pojmom kyberterorizmus sú myslené teroristické aktivity, ktorých cieľom, prenášačom či použitým prostriedkom je kyberpriestor a fyzické alebo virtuálne objekty, ktoré sa v ňom nachádzajú. Oficiálna definícia kyberterorizmu bola sformulovaná Dorothou Denningovou: „Kyberterorizmus je konvergenciou terorizmu a kybepriestoru obecne chápaný ako nezákonný útok alebo nebezpečenstvo útoku proti počítačom, počítačovým sieťam a informáciám v nich skladovaných v prípade, že útok je konaný za účelom zastrašiť alebo donútiť vládu, alebo obyvateľov k podporovaniu sociálnych alebo politických cieľov.“ V prípade ďalších definícií kyberterorizmu sa už nejedná o jednoduché a jednoznačné vymedzenie tohto pojmu. Ďalšie často publikované definície:

- „Kybernetický terorizmus sa dá definovať ako predstaviteľa aktivít vedených alebo koordinovaných štátom s cieľom získať informačnú prevahu alebo vyradiť technologickú infraštruktúru protivníka.“ (A. Colarik a L.Janczewskiho)
- „Kybernetický terorizmus je kybernetický útok užívajúci či zneužívajúci počítač alebo komunikačné siete za účelom spôsobenia dostatočnej škody s cieľom zastrašiť spoločnosť a majúci ideologický podtext.“ (Severoatlantický pakt)
- „Kybernetický terorizmus je kriminálny akt vedený za pomoci počítača alebo telekomunikačného prostriedku. Cieľom je spôsobiť zmätok a neistotu za účelom ovplyvniť vládu alebo populáciu k prijatiu ideologických alebo politických či sociálnych tém.“ (Ministerstvo vnútra Spojených štátov amerických)

- „Kybernetický terorizmus predstavuje spoločné stretnutie reálnych subjektov vo virtuálnej realite v tzv. kyberpriestore.“ (D. Denningová)
- „Kyberterorizmus je politicky motivovaný útok na nástroje a/alebo proces získavania a/alebo spracovania elektronických dát, ktorý vo svojom dôsledku znamená násilie alebo hrozbu násilia proti nevojenským cieľom a ktorého účelom je určitým spôsobom ovplyvniť širší okruh recipientov, ako sú priame obete takého útoku.“ (Ministerstvo kultúry Českej republiky)

Presne ako u pojmu terorizmus, ani pri kyberterorizme neexistuje konsenzus na jednej teórii. Neexistuje žiadna medzinárodná definícia pre to, čo to kybernetický terorizmus vlastne je. Myriam Cavelty ilustruje nebezpečnosť útokov do pomyselného rebríčku, kedy na najnižšom stupni stojí kybernetický vandalizmus (napríklad napadnutie webových stránok), nasledujú kybernetické zločiny a kybernetické vyzvedačstvo, tie zasahujú hlavne subjekty v ekonomickom sektore. Posledné dva stupne tvorí kybernetický terorizmus a na vrchole stojí kybernetická vojna.

Možné dôsledky kyberterorizmu sú:

- krádež dát,
- zničenie dát,
- destabilizácia systému,
- nedostupnosť služby,
- blokovanie systémových prostriedkov atď.

2.2 Nástroje, technika a metódy kybeterorizmu

Kyberterorizmus môže voči informačným technológiám pôsobiť tromi nižšie uvedenými spôsobmi:

- **Priamym teroristickým útokom na lokálnu technológiu –** špecifický druh kybernetického terorizmu závisí na umiestnení a význame konkrétnej technológie.
- **Súbežným teroristickým útokom –** najnebezpečnejší teroristický útok, a to z toho dôvodu, že dochádza k množstvu súbežných teroristických útokov na rôznych miestach a úrovniach. Dá sa použiť ako časť prípravy na útok, alebo podpora pre dezorientáciu protivníka.

- **Zničením technológie k riadeniu teroristickej organizácie –** jedná sa o harmóniu medzi teroristickými skupinami a ich činnosťami z globálneho hľadiska, príkladom môže byť steganografia, ktorá značí ukrývanie textu do obrázku.

Základom kyberterorizmu je zneužívanie dôveryhodnosti, integrity a dostupnosti počítačových systémov. Narastajúcim vývojom technológií sa tieto metódy zdokonaľujú. Prostriedky kyberútokov spočívajú v používaní tzv. malware, teda škodlivého softwaru, do tejto skupiny patria:

- **Adware –** jedná sa zvláštny softwarový prostriedok, ktorého primárnou činnosťou je získavanie dát, údajov alebo informácií. Taktiež sa používa na odpočúvanie na koncových bodoch počítačových sietí.
- **Spyware –** mimoriadny softwarový prostriedok, pomocou ktorého dochádza k utajovanému zasielaniu informácií užívateľa.
- **Trojské kone –** druh počítačových vírusov skrývajúce svoju identitu, vo väčšine prípadov majú schopnosť zadných vrátok so schopnosťou spustenia určitej operácie v určitý čas a to bez vedomia užívateľa.
- **Počítačové vírusy** - tieto prostriedky znemožňujú funkcie určitých služieb alebo procesov v počítači.

Ďalšie prostriedky zo skupiny malware sú napr. červy, rootkity, hijackery alebo dialery.

K ďalším metódam kyberterorizmu patria hlavne:

2.2.1 Hacking

Jedná sa o neoprávnené získavanie prístupu k dátam, tzv. prienik do systému inou ako štandardnou cestou. Pomocou hackingu sa dá zistiť veľa informácií, hesiel a pod. Môže byť legálny alebo nelegálny. Základom hackingu je hacker, je to zjednodušene programátor, ktorý tvorí vlastné programy, špeciálnych PHP skript atď. [14]

2.2.2 Technika sociálneho inžinierstva

Je ovplyvňovanie a presviedčanie ľudí s cieľom oklamať ich tak , aby uverili, že sociálny inžinier je osoba totožnosti, ktorú predstiera, ktorú si vytvoril pre potreby manipulácie. Vďaka tomu, že sociálny inžinier je schopný využívať ľudí, s ktorými komunikuje, prípadne dodatočné technologické prostriedky, aby získali hľadané informácie. Užívateľovi na-

príklad príde e-mail a odosielateľ je subjekt s vyššou autoritou, obsah sľubuje nevídané zľavy alebo niečo zdarma. [14]

2.2.3 Phreaking

Činnosť, ktorá útočníkovi dovoľuje bezplatne využívať telefónne linky, či zadarmo si napojiť internet. Hovory sú na účet niekoho iného alebo na telekomunikačné firmy. Patrí sem aj odpočúvanie hovorov, alebo napríklad výroba odpočúvacích zariadení. Ide o trestnú činnosť. Pre zaujímavosť za túto činnosť nebol ešte nikto odsúdený. [14]

2.2.4 Phishing alebo „brad spoofing“

Jedná sa bežnú krádež identity, spočíva v získavaní obecných privátnych citlivých informácií týkajúcich sa jedinca, týmito údajmi môžu byť napr. údaje o platobnej karte alebo krádež prístupového mena a hesla do internetových služieb, pomocou ktorými sa dá manipulovať s bankovým účtom. Tieto nelegálne získané informácie sú prostriedkom pre nasledujúce vykrádanie účtov, prevody peňazí, internetové nákupy a pod. [14]

2.2.5 Pharming

Spočíva v prekladaní URL adresy do formátu IP adresy prostredníctvom DNS serverov, útočníci sa pokúšajú nájsť zle zabezpečené servery, v ktorých prepíšu IP adresu určenú napríklad pre URL banky IP adresou falošnej stránky. Ľudia si potom myslia, že sú na stránkach svojej banky a jednoducho útočníkovi napíšu svoje prihlasovacie údaje do internet bankingu. [14]

2.2.6 Defacement

Pretvorenie, modifikovanie alebo nahradenie internetových stránok serveru iným obsahom. Jedná sa o skupinu tzv. psychologického infoware. Podstatou tejto metódy je presmerovanie primárnej internetovej stránky, čo vedie k dezorientácií užívateľa. [14]

2.2.7 Spam

Spamom rozumieme nevyžiadanú poštu v e-mailovej schránke. E-mailové stránky už vyvinuli rozpoznávanie spamovej pošty a hneď po príchode tejto pošty ju presmeruje do zvláštnej záložky. [14]

2.2.8 Hoax

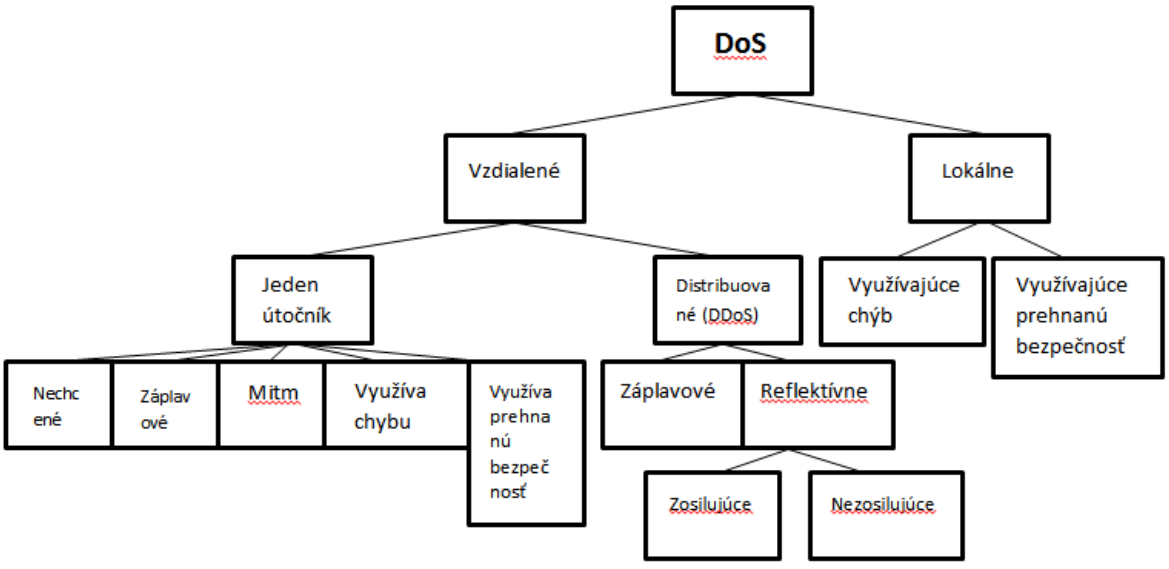
Falošná poplachová správa varujúca užívateľa pred prípadným nebezpečenstvom. Môže mať formu napríklad e-mailových správ, ktoré užívateľa vyzývajú k ďalšiemu rozposielaniu a varovaniu ostatných užívateľov. Jedná sa o tzv. reťazové e-maily.

Ku charakteristickým znakom hoaxingu patri napríklad:

- obťažovanie príjemcu,
- nebezpečné rady,
- nadbytočné zaťažovanie liniek a serverov,
- strata dôveryhodnosti šíriteľa,
- prezradzovanie dôveryhodných informácií,
- preťažovanie konkrétne cieľovej e-mailovej schránky,
- poškodenie konkrétnej inštitúcie.

2.2.9 DoS útok

Súčasná najväčšia kybernetická hrozba je určite tzv. „odoprenie služby“ (anglicky „Denial of Service“ označovaný skratkou „DoS“), pretože sa jedná o najpoužívanejšiu a tiež najnebezpečnejšiu formu kyberútokov.



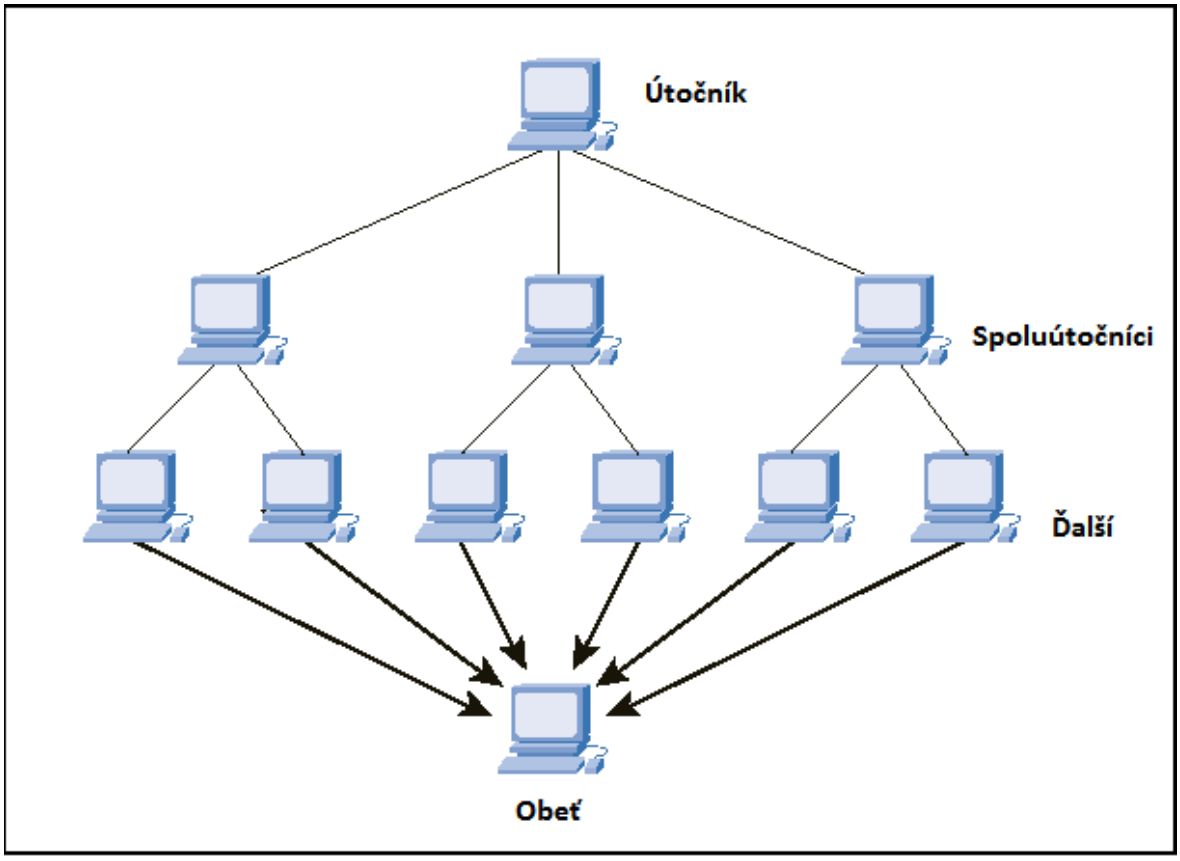
Obrázok 3 – **Rozdelenie DoS útokov** (vlastné spracovanie)

DoS predstavuje preťažovanie cieľovej stanice požiadavkami dovtedy, kým sa systém nespomalí, či dokonca neodstaví úplne. Takéto preťažovanie serveru má väčšinou za následok jeho zrútenie, prípadne zahltenie a reštartovanie vzdialeného počítača.

Skupina CERT (Computer Emergency Response Team) charakterizuje DoS útoky ako explicitné pokusy útočníkov smerované k legitímnym užívateľským službám a k zabráneniu ich používaniu. Jednoducho sa dá povedať, že sa jedná o zabránenie prístupu k informáciám, alebo služby zákonných užívateľov (napríklad prístupu k e-mailu, webovým stránkam, on-line účtom). K DoS útokom podľa skupiny CERT patrí:

- pokusy o zahltenie siete, ktoré majú zabrániť legitímnej prevádzke siete,
- pokusy o narušenie spojenia medzi dvoma zariadeniami, ktoré majú zabrániť prístupu k službe,
- pokusy zabrániť konkrétnej osobe k prístupu ku službe,
- pokusy o narušenie služby pre určitý systém alebo osobu.

Niektoré z vyššie spomenutých útokov nemusia vždy znamenať použitie DoS útoku. Niekedy sa jedná o tzv. asymetrické útoky, kedy k uskutočňovaniu DoS útokov dochádza len s obmedzenými zdrojmi. Môžu však napadnúť veľké sofistikované siete, napríklad útočník so starým a pomalým počítačom môže zakázať omnoho rýchlejšiu sieť.



Obrázok 4 – **Schéma bežného DoS útoku** [23]

DoS útoky majú rôzne druhy a sú zamerané na veľké množstvo služieb. Rozdeliť ich môžeme na nasledujúce druhy DoS útokov:

- spotrebu vzácnych, obmedzených alebo neobnoviteľných zdrojov,
- zničenie alebo zmenu informácií o konfigurácií,
- fyzické zničenie alebo zmenu sieťových komponentov.

Pre realizáciu DoS útokov v podobe spotreby vzácnych, obmedzených či neovplyvniteľných zdrojov sú nutné určité prostriedky počítača alebo siete – napríklad šírka pásma, pamäť a miesto disku, čas procesoru, dátové štruktúry, prístup k ostatným počítačom a sieťam, poprípade aj niektoré ekologické zdroje. Základným predpokladom je ale pripojenie k sieti. Tento druh DoS útokov začína naviazaním spojenia útočníka s počítačom obeti, pričom nedochádza k dokončeniu tohto spojenia. Zatiaľ čo obeť čaká na dokončenie falošného a čiastočne otvoreného spojenia, legitímne spojenia sú odmietnuté. Ďalším spôsobom DoS útokov v podobe spotreby vzácnych, obmedzených alebo neobnoviteľných zdrojov je použitie vlastných prostriedkov zo strany útočníka – tieto DoS útoky sú nazývané ako zaplavovanie. Vo väčšine prípadov sú tieto útoky nečakané. Spočívajú v posielaní

veľkého množstva dátových balíkov prostredníctvom internetového protokolu UDP, ktorý nevyžaduje spoľahlivý príjem zaslaných dát. Pakety vyťažujú kapacitu komunikačnej linky a pracovný výkon cieľovej stanice, čo môže mať za následok spomalenie, či úplnú nedostupnosť stanice a služieb na nej konfigurovaných. Ďalším typom DoS útoku sú nároky útočníka na šírku pásma. Útočník vo väčšine prípadov koordinuje i niekoľko strojov v rôznych sieťach. Okrem šírky pásma môžu útočníci využívať tiež iné zdroje – napríklad počty dátových štruktúr. Útočník spotrebuje dátové štruktúry za pomoci jednoduchého programu či skriptu, ktorý opakovane vytvára kópie seba samého.

Útočník môže tiež využívať:

- generovanie nadmerného množstva e-mailových správ,
- zámerného generovania chýb, pre ktoré je treba sa prihlásiť,
- umiestnenie súborov FTP protokol (File Transfer Protokol), slúžiaci pre prenos súborov medzi počítačmi pomocou počítačovej siete alebo sa zdieľané sieťové priečinky pre informácie o právnej konfigurácií pre anonymné FTP protokoly.

V súčasnej dobe existuje veľa spôsobov, ktorými sa dá po určitom počte neúspešných pokusov o prihlásenie uzamknúť akýkoľvek účet. Pre útočníka toto ale nie je žiadna prekážka, lebo môžu legitímnemu užívateľovi zabrániť v prihlásení a to v niektorých prípadoch tiež na privilegované účty. K DoS útokom sa dá zaradiť tiež napadnutie ďalších zdrojov zo strany útočníkov – napríklad tlačiarne, páskových pripojení a pod. DoS útoky v podobe zničenia alebo pozmenenia informácií o konfigurácií spočívajú v likvidácií alebo zmenách konfiguračných dát, čo má za následok zabránenie používania počítača alebo siete.

Varianta DoS útoku je tzv. distribuovaný DoS *(„Distributed Denial o Service“* označovaný skratkou *„DDoS“*) alebo tiež tzv. reflektívne útoky. Tieto DDoS útoky sú prevádzané súbežne z veľkého množstva počítačov spadajúcich do tzv. siete internetových robotov (botnet). Ide o veľmi efektívne útoky, uskutočňované práve týmito stanicami, ktorých môžu byť desiatky ale aj milióny.

DDos útoky a ich rozdelenie podľa spôsobu ich uskutočňovania. Dajú sa klasifikovať nasledujúcim spôsobom:

- Zaplavovanie (flood attacks) – viď. vyššie.
- Silnejúce útoky (DNS amplification attacks) – jedná sa o útoky využívajúce chyby v počítačových sieťach, prostredníctvom ktorých dochádza k premene vstupných

požiadaviek malej veľkosti na požiadavky veľkej veľkosti. Tieto útoky sú obvykle zamerané na celú sieť, odpoveď je nastavená na IP adresu obeti.

- SYN záplavy (SYN flood) – tieto kyberútoky využívajú zoznam počítačov, ktoré útočník využije k falošnému naviazaniu spojenia „útočník začne posielať TCP pakety s nastaveným príznakom SYN a zdrojovou IP adresou nastavenú na IP adresu obeti, tieto servery si myslia, že sa s nimi obeť snaží nadviazať spojenie a pošlú jej späť TCP paket s príznakmi SYN a ACK. Obeť samozrejme nič také nečaká. Normálne by poslala TCP paket s príznakom RST. Samozrejme v dnešnej dobe toto pravidlo nie je dodržiavané, alebo filtrované, takže obeť nič také neodošle, server (použitý ako prostredník) si myslí, že jeho TCP paket s príznakmi SYN a ACK sa asi niekde stratil, tak ho odošle znova, a tak to ide ďalej.

3 TRENDY POČÍTAČOVEJ KRIMINALITY

Novým rysom kyberterorizmu v budúcnosti bude plošnosť a brutalita. Politický terorizmus sa až na výnimky zameriaval na vybrané individuálne ciele – štátnych predstaviteľov a hospodárskej moci. Tradičný terorista chcel, aby veľa ľudí prihliadalo, ale málo umieralo. Účelom útoku nového teroru je naopak zabiť čo najviac ľudí, spôsobiť rozsiahle materiálne škody a hospodárske straty. Účelom je vyvolať celosvetovú paniku, hrôzu a strach, otriasť psychikou spoločnosti, poškodiť vieru ľudí v schopnosť vlády chrániť svojich občanov.

Možnosť využitia počítačov i ku páchaniu kriminálnej činnosti si odborníci uvedomili veľmi rýchlo. Preto vznikol pojem kyberterorizmus. Faktom však zatiaľ ostáva to, že teroristické skupiny využívajú zatiaľ internet viac k propagácií a k vzájomnej komunikácii a nie ku kybernetickým útokom. Výskum a vývoj technológií prináša stále nové elektronické prostriedky, výpočtovú techniku, komunikačné prostriedky a možnosti kódovania a šifrovania prenosu dát, ale aj nové zbraňové systémy. To všetko je predmetom záujmu teroristických skupín. Pokúsim sa načrtnúť predpovede, vývoje a trendy v kyberterorizme a možnosti ako im predísť.

- Počet trestných činov hlásených polícii, ktoré sa týkajú ICT a ukladania dát v elektronických médiách podstatne zvýši požiadavky na zmenu priorít pre prideľovanie zdrojov. Preto bude nutné organizovať kvalitatívne nový obsah školení a vzdelávania policajtov a vyšetrovateľov. Bude nutný vznik a použitie nových policajných špecializácií. Tak isto aj štátny zástupcovia a sudcovia musia získať a osvojiť si nové znalosti v tejto kategórii trestných činov.
- Rozsiahla problematika počítačovej kriminality bude ovplyvňovať zákonnosť, kedy sa bude zvyšovať počet obetí trestných činov a finančných strát v súvislosti s internetovými podvodmi, vrátane krádeží pomocou zmenenej identity páchateľa. To znamená, že problematika počítačovej kriminality bude ovplyvňovať štátnych zamestnancov, ktorí sa stanú predmetom tejto trestnej činnosti a finančnými stratami. Súčasne budú narastať podvody na internete, vrátane podvodov súvisiacich so zmenou identity.
- K virtuálnym útokom a kriminalite kyberteroristov bude dochádzať so zvýšenou frekvenciou. Tieto závažné trestné činy majú charakter hrozby psychologickej informačnej vojny. Príkladom môže byť počítačové chatovanie a správy, hrozby, etnické zastrašovanie. Bude preto nutné prijať nové zákony v oblasti informačnej

bezpečnosti. Súčasne tiež všetky orgány budú aplikovať nové metódy a prostriedky pre vyšetrovanie, prevenciu a vzdelávanie či výcviku.

- Charakter špionáže sa bude rozširovať do oblasti informačnej vojny, ekonomickej špionáže a krádeží duševného vlastníctva. Vzniknú tak nové vzorce, procesy, komponenty, štruktúry a aplikácie nových technológií spojené s marketingom, výrobou a predajom tovaru alebo služieb.
- Skupina organizovaného zločinu a teroristi budú stále viac používať počítač ako nástroj kriminálnej činnosti a zaisťovanie komunikácie.
- Teroristické skupiny budú stále viac používať globálne siete ako nástroj pre dosiahnutie svojich cieľov. Zahrňuje to používanie internetu pre utajenú komunikáciu a koordináciu cieľov vrátane ako šifrovania tak aj steganografiu, rovnako ako využiť prístup do siete systému kritických infraštruktúr v záujme vytvorení chaosu, dezinformáciu a zničenie súborov.
- Zločinci, teroristi a anarchisti budú vo zvýšenej miere využívať informačné a komunikačné technológie ako základné nástroje a metódy kedy môžu získať alebo narušiť dáta /informácie alebo zničiť komunikačné prostriedky, informačné procesy alebo dátové sklady. Príkladom môžu byť elektromagnetické pulzy, vysoké rádiové frekvencie, malígny software ako vírusy, červy, trojské kone a spyware.

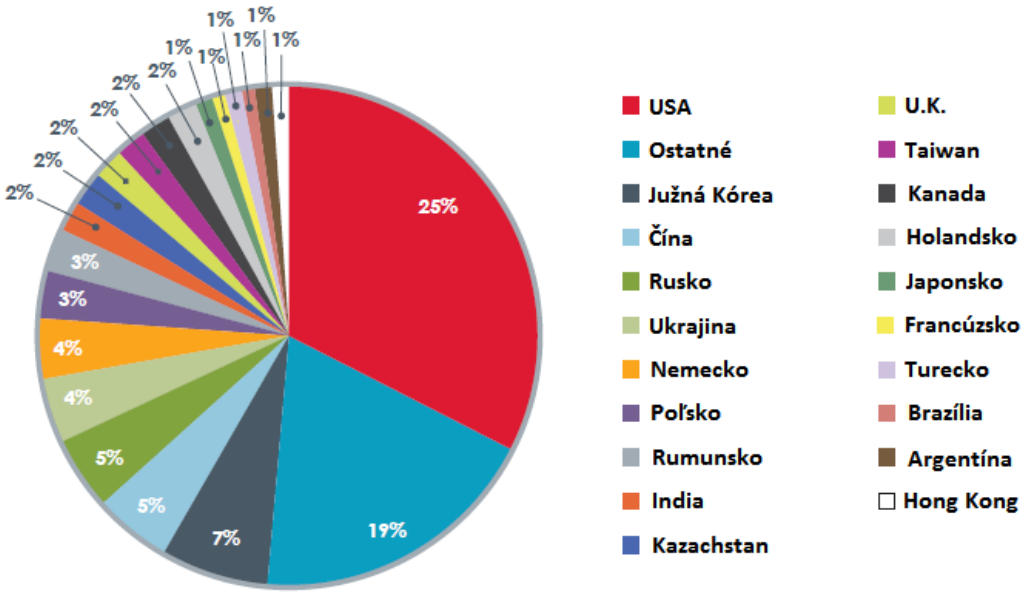
II. PRAKTICKÁ ČASŤ

4 ŠTATISTIKY A ANALÝZY KYBERÚTOKOV

V tejto kapitole sa chcem venovať verejne prístupným štatistikám kybernetických útokov a postupne ich analyzovať a uviesť na akej úrovni je v dnešnej dobe bezpečnosť informačných systémov. Teda ako sa vyvíjajú postupy a mechanizmy, ktorých citlivé informácie a služby musia byť chránené pred zverejnením, poškodením alebo zneužitím neoprávnenou činnosťou. Taktiež, ako k tomuto problému pristupujú úrady vo svete a hlavne v Českej a Slovenskej republike.

4.1 Štatistiky a analýzy kyberútokov vo svete

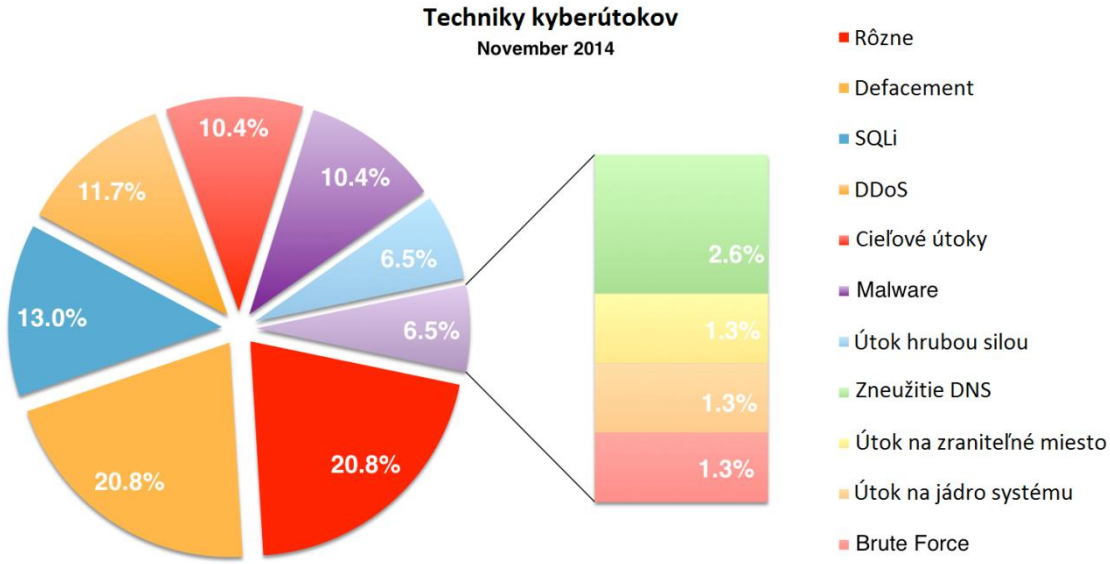
Na portály heckmageddon.com pravidelne každý rok od roku 2011 pribúdajú nové štatistiky ohľadne kyberútokov vo svete. V nasledujúcej kapitole chcem rozobrať grafy a čísla z roku 2014. Počty týchto kyberútokov každým rokom rastú, preto je tento problém veľmi častou témou, či už v médiách, alebo obecne.



Obrázok 5 – **Krajiny s najväčšími počtami kyberútokov za rok 2014** [16]

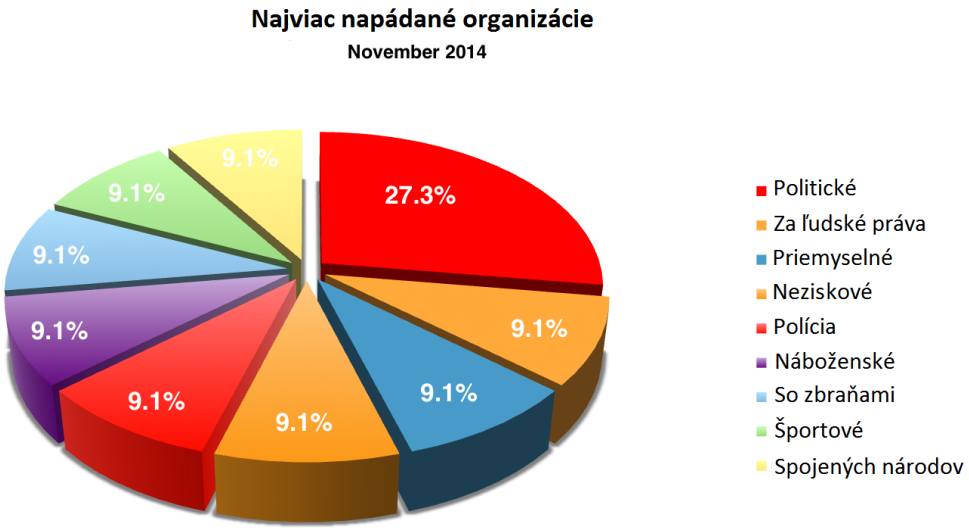
Začneme s grafom, ktorý znázorňuje počty kyberútokov v rôznych krajinách v roku 2014. Ukazuje sa, že Spojené štáty americké sú bezkonkurenčne na vrchole. Tie spolu s Čínou a Ruskom patria medzi štáty, ktoré sa najviac venujú využitiu kyberpriestoru za účelom či už obrany alebo útoku. Aj napriek tomu, že je v dnešnej dobe zatiaľ veľmi zložité dobre prevedený útok s istotou vystopovať až k pôvodnému autorovi, je možné, že útoky boli prevedené s podporou štátnych aktérov. Medzi najznámejšie patria Rusko-estónsky kon-

flikt v roku 2007 alebo Rusko-gruzínsky v roku 2008. Rusko a USA sa dlhšiu dobu navzájom obviňujú z kybernetických útokov. Taktiež Čína je jeden z lídrov tohto celosvetového problému, má na svedomí najdlhší útok v histórii, ktorý trval 5 rokov a nabúral 72 sietí medzi ktorými boli aj podniky obranného priemyslu, OSN alebo Medzinárodný olympijský výbor.



Obrázok 6 – **Najpoužívanejšie techniky kyberútokov za november 2014** [16]

Pre veľký počet kyberútokov a pre ich rozmanitosť si za príkladný vezmeme mesiac november. V tento mesiac najväčšie percentá a to 20,8% zabrali technické útoky rôznych typov. Na druhom mieste sú SQLi útoky a hneď za nimi sa nachádzajú už spomínané DDoS útoky. DDoS útok je obľúbený obecne vďaka svojím masívnym účinkom. Útočník je schopný využiť ku svojím aktivitám počítač akéhokoľvek užívateľa. Hlavným nástrojom k šíreniu sú botnety, ktoré plnia rozkazy útočníka na inom počítači.



Obrázok 7 – **Najviac napádané organizácie za november 2014** [16]

Za zmienku určite stoja aj ciele kyberútokov, kde sa na popredných priečkach už niekoľko rokov držia politické organizácie. Už spomínaný Rusko-estónsky konflikt bol zameraný hlavne na weby estónskych politických strán, ďalej aj na médiá a internetové stránky bánk. Pri tomto bode je vhodné spomenúť skupinu Anonymous, ktorá je zložená z hackerov po celom svete. Je to združenie bez štruktúry a vedenia, často sú ich útoky iba vyhrážkou pre vyššie postavených ľudí v krajinách. Podieľali sa na mnohých demonštráciách spojených s prezidentskými voľbami, prevratmi v Tunisku a Egypte a pod.

Tieto štatistiky musia byť brané s nadhľadom, pretože sa vzťahujú len na kyberútoky, ktoré sú zverejnené, alebo nájdené na internete s dostupných informácií. V médiách dostávajú priestor hlavne krajiny, kde je kyberterorizmus veľký problém, preto nemôžeme vedieť o všetkých útokoch.

4.1.1 Najväčšie kyberútoky na svete

- **Flamer**

Tiež známy ako „Skywiper“ alebo „Plamer“. Je to modulárny počítačový malware, ktorý bol objavený v roku 2012, ako vírus určený k útokom na počítačové systémy v krajinách blízkeho východu. Napadal užívateľov operačného systému Microsoft Windows. Hackery ho používali za účelom špionáže v miestnej sieti LAN alebo USB, kam patrili tisíce počítačov od súkromných osôb, cez vzdelávacie inštitúcie, až po vládne organizácie. Flamer zaznamenával napríklad Skype konverzácie, činnosť klávesnice, obrazovky ale aj činnosti

na internete. Zaistený bol 28. mája 2012 spoločnosťou „Computer Emergency Response Team“ (CERT). [8]

- **Kyberútoky z júla 2009**

Jednalo sa o sériu koordinovaných útokov proti vláde, finančným internetovým stránkam a stránkam spravodajských agentúr, ako Spojených štátov amerických tak Južnej Kórey. Jednalo sa o zaplavenie serverov pomocou DDoS útokov. Uniklo mnoho informácií z viacej ako 200 000 počítačov. [8]

- **Útok na PayPal**

Internetoví aktivisti Anonymous, spustili pod názvom „Operation Payback“ kybernetický útok proti PayPal, Mastercard a Visa. Tieto spoločnosti zakázali platby v prospechu Wiki-Leaks, ktorý zverejňuje tajné správy americkej diplomacie. [8]

- **Útok v Indii**

India v roku 2011 oznámila narušenie počítačovej bezpečnosti. K najväčšiemu útoku došlo 12. júla 2012, kedy hackery prenikli na e-mailové účty viac ako 12 000 užívateľov. Medzi ktorými boli hlavne vysoko postavené osoby z obranného výskumu a rozvojovej organizácie (DRDO), pohraničnej Indo-tibetskej polície (ITBT), ministerstva vnútra a ministerstva zahraničných vecí. [8]

- **Stuxnet**

Počítačový vírus, objavený v roku 2010, šíriaci sa v prostredí Microsoft Windows a napadajúci priemyslové software spoločnosti Siemens. Tento vírus v roku 2010 napadol jadrové zariadenie v Iráne. Teheránu zničil 1000 jadrových odstrediviek a posunul tak ich jadrový program aspoň o dva roky späť. Napadol okolo 60 000 počítačov. Za jeho vytvorenie by mali byť zodpovedný Spojené štáty a Izrael, ale nikto sa k nemu nehlási. [8]

- **Útok na Spamhaus**

Považovaný za najväčší kybernetický útok v histórií je napadnutie Spamhaus, čo je program na filtrovanie spamových mailov. O tomto DDoS útoku sa veľa hovorilo v súvislosti s tým, že bol tak obsiahly, že mohol zahltiť hlavné siete a teda „spomaliť internet“. [8]

- **Útok na Citigroup**

Citigroup je jeden z najväčších finančných gigantov na svete, preto je častým terčom hackerov. Spoločnosťou denne prejde veľa peňazí ale aj citlivých informácií. V roku 2011, sa

hackery dostali k viac ako 200 000 kontaktných údajov, čo malo za následok stratu spoločnosti až 2 700 000 dolárov. [8]

- **Útok na Playstation**

V roku 2011 získali hackery prístup k informáciám o účtoch v sieti Playstation Network a Sony Online Entertainment vrátane informácií o kreditných a debetných kartách. Odcudzili viac ako 77 000 000 dolárov. Škody za odstavenie sietí a za vniknutie sa vyčísľuje na miliardy dolárov. [8]

- **Útok na iCloud**

V poslednom čase, čím ďalej, tým viac ľudí používa webové úložisko pre svoje dáta. Je to jednoduché a ku svojim súborom máte prístup odkiaľkoľvek. Spoločnosť Apple má takéto úložisko s názvom iCloud. V roku 2014 bolo napadnuté hackermi, ktorý sa dostali k súkromným súborom známych celebrít. Nakoniec sa ale ukázalo že hackeri nemierili na celý iCloud, ale na konkrétne kontá celebrít.

- **Logic Bomb**

V čase studenej vojny v roku 1982, CIA prišla na spôsob ako narušiť prevádzku ruského plynovodu bez použitia tradičných výbušných zariadení. Namiesto toho zostavili časť kódu v počítačovom systéme, ktorý riadil činnosť tohto plynovodu. Nazvali ho „logická bomba“. Chaos, ktorý nasledoval bol monumentálny, výbuch bol vidieť dokonca z vesmíru. [8]

4.2 Štatistiky a analýzy kyberútokov v Českej republike

Česká republika patrí medzi štáty, ktoré nie sú pod veľkým tlakom kybernetických útokov v porovnaní napríklad s USA, Ruskom alebo Čínou. Patrila medzi posledné vyspelé štáty, ktoré implementovali kybernetickú bezpečnosť na národnú úroveň. Problematikou kybernetickej bezpečnosti sa aktívne začala zaujímať od roku 2011, kedy vláda prijala uznesenie č. 781 o ustanovení Národného bezpečnostného úradu. Na základe prijatého uznesenia vzniklo Národné centrum kybernetickej bezpečnosti (NCKB) so sídlom v Brne. Hlavné oblasti činnosti tohto centra sú:

- prevádzka národnej CERT Českej republiky,
- spolupráca s ostatnými národnými CERT tímami a CSIRT tímami,
- spolupráca s medzinárodnými CERT a CSIRT tímami,
- príprava bezpečnostných štandardov pre jednotlivé kategórie organizácií v ČR,

- podpora vzdelávania v oblasti kybernetickej bezpečnosti,
- výskum a vývoj v oblasti kybernetickej bezpečnosti.

Pre kybernetickú bezpečnosť je samozrejme dôležitá spolupráca týchto tímov. Spolupráca v rámci Českej republiky je zaistená národnou PoC (Point of Contact, ktorého rolu momentálne plní CSIRT.CZ) ktorá sprostredkuje kontakty a predáva informácie medzi tímami. Ďalej je dôležitá výmena a distribúcia informácií. Medzi aktívne činnosti zložiek kybernetickej bezpečnosti v Českej republike patria:

- **Botnet Feed**

Nástroj vyvíjaný za účelom zberu a spracovania informácií na koncových uzloch zapojených do botnetov. Má prístup k záznamom obsahujúcim IP adresy všetkých nakazených strojov v Českej republike. Prejde ním približne 250 000 záznamov denne.

- **Incident Handing Automation Project**

Zadržiava dáta od bezpečnostných tímov, veľkých spoločností, univerzít a výskumných laboratórií. Záznamy obsahujú IP adresy reportovaných strojov. Približne 7 000 záznamov denne.

- **OSINT (Open – Source Intelligence)**

Zber informácií z otvorených zdrojov. Má na starosti distribúciu relevantných informácií k subjektom ako je zraniteľnosť, malware kampane, krádeže užívateľských údajov a podobne. Taktiež publikuje správy a aktivity prostredníctvom GovCERT.cz.

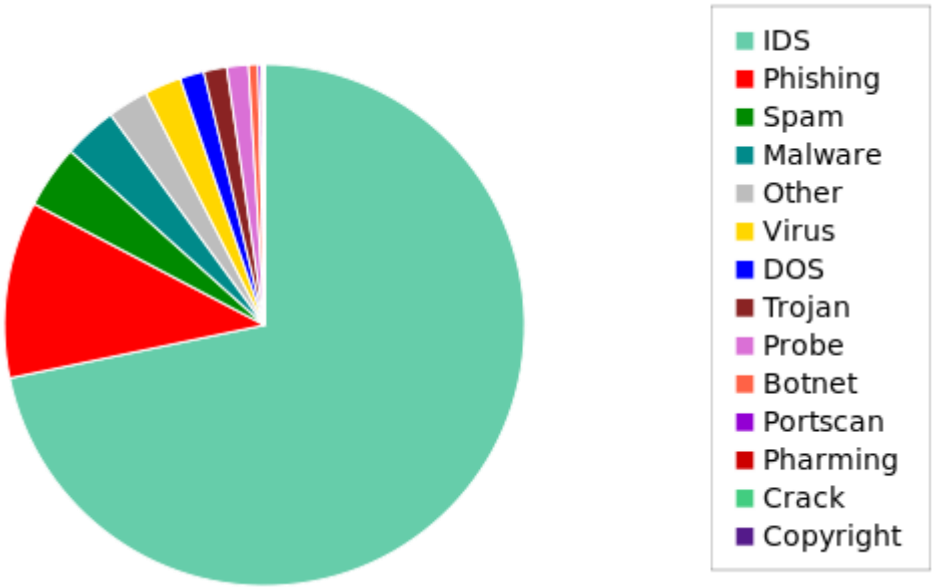
Národná CSIRT (Computer Security Incident Response Team – bezpečnostný tým pre koordináciu riešenia bezpečnostných incidentov v počítačových sieťach iniciovaných v Českej republike). Do skupiny tímov CSIRT patrí vládna CERT, ktorá hrá kľúčovú rolu pri ochrane kritickej informačnej infraštruktúry a zákona o kybernetickej bezpečnosti. Prostredníctvom svojich internetový stránok CSIRT.CZ uvádzajú štatistiky kyberútokov z obdobia 2008-2015. [15]

	2008	2009	2010	2011	2012	2013	2014	2015	súčet
IDS	-	-	-	491	3924	2121	2380	511	9427
Phishing	65	220	209	144	159	175	368	100	1440
Spam	47	28	103	26	43	73	160	35	515
Malware	53	97	42	9	19	44	117	55	436
Ostatné	1	5	8	62	13	75	100	67	331
Vírusy	-	121	178	1	1	-	-	-	301
DoS	1	4	2	2	68	72	32	15	196
Trojské kone	66	6	26	5	5	12	56	13	189
Kyber sondy	-	3	14	25	12	26	86	10	176
Botnet	-	3	46	5	8	15	-	-	77
Portscan	10	4	1	6	1	3	2	-	27
Pharming	-	-	-	-	-	-	18	-	18
Crack	1	-	4	-	-	-	-	-	5
Copyright	-	-	1	-	1	-	-	-	2
súčet	244	491	634	776	4254	2616	2616	806	13140

Tabuľka 1 – **Kybernetické útoky ČR (2008-2015)** [15]

V tabuľke môžeme vidieť, že počet kyberútokov v Českej Republike stále rastie. Najväčší prelom bol v roku 2012, kedy sa počet napadnutí počítačových sietí oproti predchádzajúcemu roku 2011 zvýšil o 3478 kyberútokov. Najväčší počet kyberútokov je od roku 2001 zaznamenaný Systémom detekcie prieniku (Intrusion Detection System – IDS). K tabuľke 1 sa vzťahuje obrázok 5 nižšie znázorňujúci pošty otvorených a uzatvorených incidentov podľa typu v období 2008-2015 a ďalej obrázok 6 nižšie, ktorý zobrazuje celkový počet otvorených a uzatvorených incidentov kyberútokov.

Obrázok 8 – **Počet incidentov ČR ročne** [15]



Obrázok 9 – **Celkový počet incidentov ČR** [15]

Hlavné je pripomenúť, že tieto čísla nie sú ani konečné ani presné, pretože sa jedná o incidenty nahlásené alebo zverejnené. Veľa útokov nie je zaznamenaných, ale aj napriek tomu z toho môžeme určiť závery. Stále rastúce čísla poukazujú na to, že problematika kyberkriminality už dávno nie je aktuálna len pre veľké krajiny ako je USA alebo Čína.

Najväčší počet incidentov sa prikladá systému IDS. IDS je skratka obranného systému, ktorý je určený na monitorovanie sietí a odhalenie podozrivých aktivít. V Českej republike tento systém už používa každá väčšia spoločnosť. Incidenty zaznamenané týmto systémom

sú na vedúcej priečke v štatistikách CSIRT už od roku 2001. Veľmi obľúbeným spôsobom pre útočníkov je phishing, je ťažké ho odhaliť a hlavne má veľkú úspešnosť. Častým kybernetickým útokom je aj útok DoS, ktorý v základe posiela len bežnú požiadavku na službu, jeho sila spočíva v neustálom opakovaní. Ďalej spomeniem spam, ktorého podiel v e-mailovej komunikácii rastie každým rokom. Čísla za rok 2015 odhadujú, jeho zvýšenie oproti roku 2014 o 66,8%. Populárnym sa stáva spam imitujúci e-mail poslaný z mobilného zariadenia, ktorý obsahuje krátky text a škodlivú prílohu.

4.2.1 Národná stratégia kybernetickej bezpečnosti Českej republiky na obdobie rokov 2015 až 2020

Táto stratégia je najnovším počinom Národného centra pre kybernetickú bezpečnosť, ktorá predstavuje základný koncepčný princíp vlády Českej republiky pre príslušnú oblasť. V krátkosti by som rada spomenula niektoré vízie ďalšieho boja proti kybernetickému nebezpečenstvu, ktoré tento dokument obsahuje:

- Česká republika zaistí v rámci kyberpriestoru podmienky pre hladko fungujúcu informačnú spoločnosť. [17]
- Česká republika, ako moderný stredoeurópsky štát a aktívny člen Európskej únie, Severoatlantickej aliancie, Organizácie spojených národov a ďalších medzinárodných organizácií, bude v najbližšej dobe aspirovať na predné postavenie v oblasti kybernetickej bezpečnosti, a to ako v rámci svojho regiónu tak aj celej Európy.
- Česká republika bude usilovať o budovanie dôvery a efektívneho modelu spolupráce s národným CERT a zároveň pôsobiť ako opora pre ďalšie tímy typu CERT/CSIRT. [17]
- Česká republika bude spolupracovať so subjektmi zo súkromnej sféry na výskume a vývoji zabezpečenia informačných a komunikačných technológií. [17]
- Česká republika sa bude snažiť dosiahnuť čo najvyššieho zabezpečenia kybepriestoru. Zároveň bude podporovať výskum a vývoj špičkových technológii a prispievať tým k zvýšeniu technologickej úrovni v Českej republike.[17]

4.2.2 Najväčšie kyberútoky na české servery

- **30. september 2008**

DDos útok na spravodajské weby, pri ktorom boli servery zahltené veľkým množstvom dotazov a nefungovali. Postihol weby Blesk.cz a DenikSport.cz, ktoré patria vydavateľstvu Ringier.

- **29. máj 2011**

Hacker napadol deň pred zahájením písomnej časti maturít internetovej stránky s ukážkovými testami a informáciami o skúške. Nefungovali ani stránky organizácie Cermat, ktorá maturity zaisťuje, útočníci nahrali na web vlastný obsah.

- **Január a február 2012**

Počas schvaľovania kontroverznej dohody proti ACTA napadli ľudia hlásiaci sa k hnutiu Anonymous, celú radu českých webov. Terčom útoku boli internetové stránky autorských organizácií (Ochranného zväzu autorského, Medzinárodnú federáciu hudobného priemyslu IFPI či Intergramu), ale aj web ODS alebo stránky Poslaneckej snemovne a vlády. Intenzita a druh útokov boli rôzne, vedľa zahltených serverov sa hackerom podarilo napríklad získať osobné dáta tisícov členov ODS.

- **14. október 2012**

Internetovú stránku komunistov z Brna napadli hackeri z hnutia Anonymous. Takmer na deň na ňu umiestnili nápis, podľa čoho sú voliči KSČM „obmedzený idioti“. Web pozmenili po krajských voľbách, a to v reakcii na úspech komunistov, ktorý v nich dosiahli.

- **16. november 2012**

Hackeri získali databázu z webu exekútorskej komory a dáta umiestnili na internete. Skupina Czechurity na svojom webe uviedla, že zabavili databázu, lebo exekútori zabavujú majetok občanom. Web komory bol na krátku dobu po oznámení útoku nefunkčný.

- **Marec 2012**

Od 4. marca napadli neznámi útočníci pomocou DDoS útoku, kedy zahltili servery obrovským množstvom požiadaviek, najskôr veľké české spravodajské weby. Napadnutý bol portál Seznam.cz aj ďalšie stránky. Neskôr čelili napadnutiu stránky českých bánk vrátane internetového bankovníctva.

- **Marec 2013**

V tomto čase čelili rozsiahlym DDoS útokom niektoré významné spravodajské servery ale hlavne rada veľkých českých bánk. NBÚ vtedy vyzval všetky zasiahnuté subjekty k spolupráci a hlásenie týchto incidentov skupinám CERT alebo CSIRT.

- **Júl 2014**

V Českej republike vznikla prvá virtuálna mena s názvom Czech Crown Coin, ktorá umožňuje platby cez internet. Jej začiatky sprevádzalo množstvo kyberútokov. Po rušných začiatkoch sa táto mena v roku 2015 začala používať.

4.3 Štatistiky a analýzy kyberútokov na Slovensku

Problematika kybernetickej bezpečnosti v Slovenskej republike na národnej strategickej úrovni ešte nie je vyriešená uceleným konzistentným spôsobom. Vo februári 2015 prijala Česká republika a tak isto aj USA novú bezpečnostnú stratégiu, kde sa podrobne venujú kybernetickej bezpečnosti. Podobný dokument pre Slovenskú republiku čoskoro oslávi 10 rokov, no aj napriek tomu je jeho nová verzia v nedohľadne. Slovenská vláda si zjavne neuvedomuje problémy, aké počítačová kriminalita prináša. Malá krajina ako Slovensko môže byť použitá ako testovací objekt veľkých kyberútokov.

Téme kybernetickej bezpečnosti je čiastočne venovaná pozornosť v dokumente „Národná stratégia pre informačnú bezpečnosť“ a v nadväznom „Akčnom pláne informačnej bezpečnosti“. Tento problém ďalej rieši dokument „Príprava Slovenskej republiky na plnenie úloh v oblasti kybernetickej obrany, vyplývajúcich z cieľov spôsobilostí Slovenskej republiky“, ktorý definuje spôsobilosti Slovenskej republiky v oblasti kybernetickej bezpečnosti, ktoré bude nevyhnutné vybudovať do konca roka 2017. Pre Národný bezpečnostný úrad z tohto dokumentu vyplýva povinnosť zabezpečiť a koordinovať vybudovanie spôsobilosti Slovenskej republiky v oblasti kybernetickej bezpečnosti. Ďalšími strategickými dokumentmi, ktoré sa čiastočne venujú kybernetickej bezpečnosti sú:

- Operačný program Integrovaná infraštruktúra 2014-2020, schválený uznesením vlády SR č 325/2013,
- Správa o bezpečnosti Slovenskej republiky za rok 2013, schválená uznesením vlády SR č. 276/2014.

Najväčší problém je, že Slovensko nemá ani jeden zákon, ktorý by sa venoval výhradne kybernetickej bezpečnosti. Ak by sme chceli porovnať situáciu v Českej republike a na Slovensku, je hneď jasné, ktorý z týchto „bratských" štátov je na tom lepšie. Ako som už spomínala, Česká republika má úplné novú stratégiu, ktorá sa problémom venuje podrobne a taktiež na toto zameraný samostatný zákon. Už od roku má stanovený Národný bezpečnostný úrad ako autoritu v oblasti kybernetickej bezpečnosti. Na Slovensku si túto kompetenciu okrem NBÚ, ktorý je poverený prípravou koncepcie kybernetickej bezpečnosti, delia viaceré úrady – ministerstvo obrany, ministerstvo financií, Slovenská informačná služba, Národná agentúra pre sieťové a elektronické služby, ministerstvo hospodárstva. Toto delenie kompetencií spôsobuje chaos a neorganizovanosť v riešení tohto závažného problému. Riešenie kybernetickej bezpečnosti na Slovensku rozdelím do nasledujúcich bodov:

- **Prevencia a pripravenosť**

Cieľom je zabezpečiť primeranú úroveň ochrany informačnej a komunikačnej infraštruktúry, kritickej infraštruktúry a jej technologických prvkov. Prioritným predmetom riešenia v roku 2014 bolo poskytovanie služieb potrebných na zvládnutie bezpečnostných počítačových incidentov, na odstránenie ich následkov a na následnú obnovu informačných systémov. Okrem týchto služieb Ministerstvo financií SR, prostredníctvom Špecializovaného útvaru pre riešenie počítačových incidentov CSIRT.SK zabezpečovalo poskytovanie služieb preventívneho a vzdelávacieho charakteru, vrátane spolupráce pri riešení incidentov.

- **Spolupráca na národnej úrovni**

Už spomínaná spolupráca Ministerstva obrany SR, Ministerstva vnútra SR, Ministerstva zahraničných vecí a európskych záležitostí SR, Národného bezpečnostného úradu a Slovenskej informačnej služby v oblastiach riešenia bezpečnostných incidentov. Taktiež CSIRT.SK v rámci poskytovania preventívnych služieb spolupracuje s ďalšími inštitúciami verejnej správy, akademickým a súkromným sektorom v rozsahu problematiky.

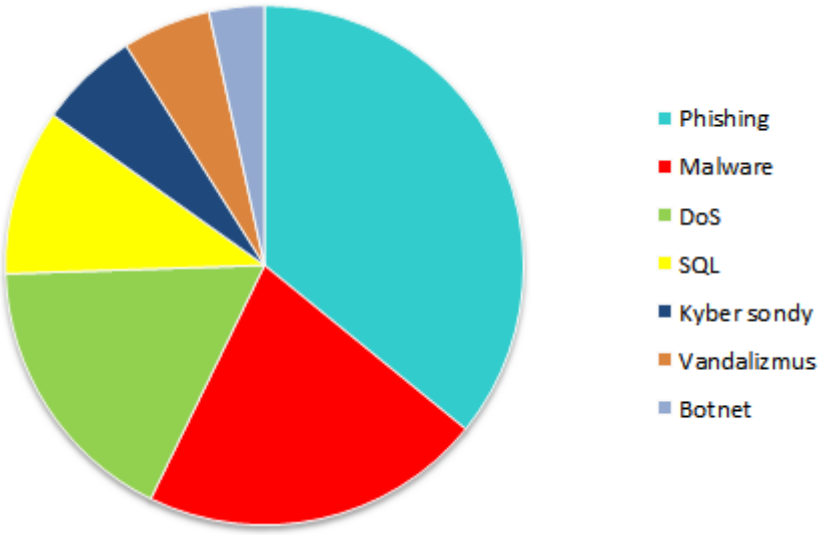
- **Spolupráca na medzinárodnej úrovni**

Na riešení problematiky informačnej bezpečnosti spolupracuje Slovenská republika na pôde Európskej agentúry pre informačnú a sieťovú bezpečnosť a Organizácie pre bezpečnosť a spoluprácu v Európe. Taktiež bola rozšírená spolupráca vďaka tímu CSIRT.SK so zahraničnými subjektmi typu CSIRT/CERT z Rakúska, Nemecka, Maďarska, Českej republiky či Poľska.

Špecializovaný útvar riešil bezpečnostné počítačové incidenty v IP adresnom priestore Slovenskej republiky. V roku 2014 bolo nahlásených 145 závažných počítačových incidentov, ktoré boli nahlásené zahraničnými partnermi, subjektmi SR alebo zistené predbežným monitoringom CSIRT.SK. Z tohto počtu bolo zaznamenaných 31 incidentov typu malware. V 51 prípadoch bol zaznamenaný výrazný nárast počtu prípadov e-mailov, v ktorých bol umiestnený formulár na získanie prihlasovacích údajov používateľov – phishing.

	súčet
Phishing	52
Malware	31
DoS	25
SQL	15
Kyber sondy	9
Vandalizmus	8
Botnet	5
súčet	145

Tabuľka 2 – **Kybernetické útoky SR (2014)** (vlastné spracovanie)



Obrázok 10 – **Počet incidentov SR (2014)** (vlastné spracovanie)

V rámci vytvárania včasného varovania, reakcie na incidenty a zverejňovania informácií, bola vykonaná aktualizácia DataCentra a CSIRT.SK. Vďaka týmto prevádzkam sú identifikované bezpečnostné anomálie a teda sú priebežne riešené.

4.3.1 Najväčšie kybernetické útoky na slovenské servery

Medzi najčastejších vinníkov patrili malé a stredné podniky v odvetví kreatívneho priemyslu, technologickom sektore a v oblasti služieb, ktoré pri svojej podnikateľskej činnosti

využívajú profesionálne softwarové produkty. Na Slovensku je v súčasnosti monitorovaných viac ako 92 firiem pre podozrenie na používanie nelegálneho softwaru. V poslednej dobe sú najviac aktívny slovenskí alebo aj českí Anonymous, ktorý demonštrujú pravidelne prostredníctvom internetu.

- **16. jún 2003**

Útok na telekomunikačnú firmu (dnešný Telecom). Útočníkovi sa podarilo získať aktívny prístup k takmer všetkým prvkom siete telekomunikačného operátora. To mu umožnilo sledovať elektronickú poštu zamestnancov, dáta klientov, ako sú banky, poisťovne, či vládne inštitúcie. Hacker získal a zverejnil dva roky starú databázu čísiel pevných liniek.

- **31. január 2012**

DDoS útok zo strany Anonymous na webovú stránku slovenského parlamentu. Stránka bola nefunkčná skoro celý deň, nasledovala demonštrácia pred budovou NR SR. Škody boli vyčíslené do výšky až 5 000 eur.

- **9. marec 2012**

Útočníci Anonymous zaútočili na internetové stránky Smer-SD, SDKÚ-DS, KDH a 99 percent. Týmto DDoS útokom chceli prejaviť nesúhlas s kauzami z poslednej doby. DDos útoku predchádzalo informatívne video od útočníkov s výrokom: „Už dlhšie nemôžeme sledovať to, čo sa na Slovensku deje. Tisícky ľudí demonštrovali v mnohých mestách a takto demonštrujeme my. Internet je naším mestom a webové stránky našou ulicou.“ Útok sa konal v predvolebnom období a webové stránky politických strán boli napádané až do volieb.

4.3.2 Porovnanie momentálnej situácie s Českou republikou

Počty závažných kyberútokov sú na Slovensku značne menšie, no ak by sme to prepočítali napríklad na počet občanov vznikli by podobné čísla. Obidve tieto krajiny sú v riešení kybernetickej bezpečnosti nováčikovia, no Česká republika je stále o krok popredu.

V rámci medzinárodnej bezpečnosti krajiny spolu spolupracujú hlavne vďaka CSIRT a CERT tímom, ktorá spája väčšinu európskych štátov v boji za lepšiu informačnú bezpečnosť. Konajú sa aj spoločné testy tejto bezpečnosti, ktoré majú za úlohu overiť pripravenosť obrany proti kybernetickým útokom.

Čo sa týka legislatívy je Česká republika na tom omnoho lepšie, či už vďaka samostatnému zákonu týkajúceho sa danej problematiky ale aj vďaka novej stratégie na roky 2015-2020, ktorá rieši problémy spojene s kybernetickou bezpečnosťou.

Na národnej úrovni sú kompetencie kybernetickej bezpečnosti rozdelené medzi viacero orgánov a inštitúcií, čo asi pôsobí len zbytočné problémy. Krajiny ako USA či Rusko, majú stanovený hlavný orgán, ktorý sa venuje informačnej bezpečnosti, či už z hľadiska prevencie, riešenia incidentov alebo obnovy systému po kybernetickom útoku. Na Slovensku je to rozdelené na viacero orgánov, v Českej republike už väčšina povinností s týmto spojených prešla na zodpovednosť Národného bezpečnostného úradu.

Z môjho pohľadu je úroveň kybernetického nebezpečenstva v Českej a Slovenskej republike rovnaký, no aj napriek tomu je Česka republika v oblasti kybernetickej bezpečnosti na vyššej úrovni. Národný bezpečnostný úrad Slovenskej republiky by mal zapracovať na svojej stratégii ohľadom počítačovej bezpečnosti a Slovenská vláda zas na novom zákone, popisujúcom právne následky takýchto činov.

5 SPOLUPRÁCA MEDZINÁRODNÝCH ORGANIZÁCIÍ V BOJI PROTI KYBERTERORIZMU

Táto kapitola je zameraná na problematiku medzinárodnej spolupráce v oblasti boja proti kyberterorizmu prostredníctvom vybraných medzinárodných organizácií. Kyberterorizmus sa dá obecne považovať za trestný čin, ktorého definícia sa v právnych systémoch rozličných štátov líši. Táto skutočnosť preto môže mať negatívny vplyv na prístupy a vzájomnú spoluprácu organizácií, ktoré sa snažia bojovať proti kyberterorizmu. V dôsledku závažnosti problematiky hroziaceho kyberterorizmu sa jednotlivé organizácie Európskej únie a Severoatlantickej aliancie snažia o uzavieranie medzinárodných dohôd s cieľom harmonizácie legislatívy a aplikácie štandardizovaných postupov v boji proti kyberterorizmu. Do akej miery je tento súlad zaistený je ale diskutabilné.

5.1 Európska únia

V rámci európskej únie bola vypracovaná ***„Stratégia kybernetickej bezpečnosti Európskej únie: Otvorený, bezpečný a chránený kyberpriestor“.***

Táto stratégia predstavuje víziu Európskej únie v oblasti kybernetickej bezpečnosti, objasňuje úlohy a povinnosti a predstavuje opatrenia, ktoré sú na základe silnej a účinnej ochrany a podpory práv občanov nutná k tomu, aby sa on-line prostredie Európskej únie stalo najbezpečnejším na svete. Podľa tejto stratégie by sa mala riadiť politika kybernetickej bezpečnosti nielen v Európskej únii, ale tiež na medzinárodnej úrovni. [9]

Stratégia kybernetickej bezpečnosti Európskej únie sa opiera o základné práva a slobody zakotvené v Listine základných práv Európskej únie a o základné hodnoty Európskej únie, vrátane harmonizácie s právnymi predpismi Európskej únie o ochrane údajov. [9]

K základným víziám tejto stratégie patria priority:

- dosiahnutie kybernetickej odolnosti,
- výrazné obmedzenie kyberkriminality,
- rozvoj politiky a kapacít kybernetickej obrany v súvislosti so spoločnou bezpečnosťou a ochrannou politikou,
- rozvoj priemyslových a technologických zdrojov pre kybernetickú bezpečnosť,
- zavedenie súdržnej medzinárodnej politiky Európskej únie týkajúcej sa kyberpriestoru a podpora základných hodnôt Európskej únie. [9]

Pre dosiahnutie vyššie uvedených cieľov Stratégie kybernetickej bezpečnosti Európskej únie je definované množstvo opatrení krátkodobého či dlhodobého charakteru, zahrňujúcich množstvo politických nástrojov a rôznych subjektov v podobe orgánov Európskej únie, členských štátov alebo odvetví.

5.1.1 Európska agentúra pre bezpečnosť sietí a informácií (European Network and Information Security Agency – ENISA)

Poslaním tejto agentúry je dosiahnutie vysokej a účinnej úrovne bezpečnosti sietí a informácií v rámci Európskej únie. Spolu s orgánmi Európskej únie a členských štátov usiluje o vytvorenie kulttúry bezpečnosti sietí a informácií v prospech občanov, spotrebiteľov, podnikov a organizácií verejného sektoru v Európskej únii.

5.1.2 Computer Emergency Response Team (CERT-EU)

Jedná sa o tým tvorený z IT bezpečnostných odborníkov z hlavných inštitúcií Európskej únie (napr. Európskej komisie, generálneho sekretariátu Rady, Európskeho parlamentu, Výboru regiónov, Hospodárskeho a sociálneho výboru), ktorý úzko spolupracuje s ostatnými skupinami CERT v členských štátoch a s ďalšími špecializovanými IT bezpečnostnými spoločnosťami.

5.1.3 Európske centrum pre boj proti kyberkriminalite (EC3)

Toto centrum funguje od roku 2012 a jeho sídlom je Európsky policajný úrad (teda ústredie Europolu) v holandskom Haagu. Cieľom tohto centra je chrániť občanov a podniky Európskej únie pred trestnou činnosťou páchanou prostredníctvom internetu.

5.1.4 Európska policajná akadémia

Táto inštitúcia združuje vyšších policajných dôstojníkov európskych policajných síl, podporuje rozvoj siete a cezhraničnú spoluprácu v boji proti trestnej činnosti, udržuje verejnú bezpečnosť a verejný poriadok v organizovaní vzdelávacích aktivít a výskumných zistení.

V súvislosti s kyberterorizmom je úlohou Európskej policajnej akadémie koordinácia podoby a plánovanie kurzov, ktoré by mali pracovníkov donucovacích orgánov vybaviť znalosťami a odbornými poznatkami pre účinný boj proti kybekriminalite.

5.1.5 Európska obranná agentúra

Dá sa tiež uviesť činnosť Európskej obrannej agentúry, ktorá posudzuje operačné požiadavky kybernetickej obrany Európskej únie a podporuje rozvoj odborníkov technológií Európskej únie týkajúce sa kybernetickej obrany (napr. z oblasti riadenia, organizácia, odbornej prípravy, infraštruktúry, dopravy a pod.).

Zjednodušene sa dá povedať, že spolupráca Európskej únie je v oblasti kyberkriminality a kyberterorizmu riešená na troch základných úrovniach – na vnútroštátnej úrovni, na úrovni Európskej únie a na úrovni medzinárodnej. Na *vnútroštátnej úrovni* sa jedná o zaistenie kybernetickej odolnosti, kyberkriminality a obrany z hľadiska členských štátov a ich vnútroštátnych subjektov. Veľmi dôležitá je ale aj vzájomná spolupráca a predávanie informácií medzi vnútroštátnymi subjektmi jednotlivých členských štátov a súkromným sektorom. Na *úrovni Európskej únie* sa jedná o spoluprácu už spomínanej Európskej agentúry pre bezpečnosť sietí a informácií, Európskeho centra pre boj proti kyberkriminalite, Európskej obrannej agentúry, skupiny CERT-EU, Európskej policajnej akadémie a Eurojust.

Medzinárodná úroveň v boji proti kyberkriminalite a kyberterorizmu je založená na vzájomne spolupráci nižšie uvedených organizácií:

- Rada Európy (Council of Europe – CE),
- Organizácia pre hospodársku spoluprácu a rozvoj (Organization for Economic and Cooperation and Development – OECD),
- Organizácia spojených národov (United Nations – OSN),
- Organizácia pre bezpečnosť a spoluprácu v Európe (Organization for Security and Co Cooperation in Europe – OBCE),
- Severoatlantická aliancia (North Atlantic Treaty Organization – NATO)

Špecifické predpisy Európskej únie vzťahujúce sa k problematike kyberterorizmu a kyberkriminality sú dokumenty **Komisie Európskych spoločností:**

- KOM/2006/251 Stratégia pre bezpečnú informačnú spoločnosť – „Dialóg partnerstva a posila účasti“,
- KOM/2006/688 Boj proti spamu a špionážnemu spyware a škodlivému softwaru („malicious software“),
- KOM/2007/267 k obecnej politike v boji proti počítačovej kriminalite,

- KOM/2009/149 o ochrane kritickej informačnej infraštruktúry – „Ochrana Európy pred rozsiahlymi počítačovými útokmi a narušením: zvyšujeme pripravenosť, bezpečnosť a odolnosť,
- KOM/2011/163 o ochrane kritickej infraštruktúry – „Dosiahnuté výsledky a ďalšie kroky: smerom ku globálnej kybernetickej bezpečnosti,
- KOM/2010/245 Digitálne agenda pre Európu,
- KOM/2010/673 Stratégia vnútornej bezpečnosti Európskej únie: päť krokov smerom k bezpečnej Európe,
- 2002465/JHA o spoločenských vyšetrovacích tímoch,
- Uznesenie Rady 2003/C 43/02 o spoločnom prístupe a zvláštnych opatreniach v oblasti bezpečnosti sietí a informácií,
- Rámcové rozhodnutie Rady 2005/222/SVV o útokoch proti informačným systémom,
- Uznesenie Rady2009/C321/01 o spoločnom európskom prístupe k bezpečnosti sietí a informácií. [10,11]

V súvislosti s kybekriminalitou a kyberterorizmom sa dajú uviesť niektoré dokumenty **Rady Európy**: Dohoda Rady Európy č. 185 o kybernetickej kriminalite, Dohoda Rady Európy č. 196 o prevencii terorizmu, Odporučenie Parlamentného zhromaždenia č. 1706 (2005) o médiách a terorizme a mnoho ďalších.

5.2 Organizácia Severoatlantickej zmluvy

Organizácia Severoatlantickej zmluvy (North Atlantic Treaty Organization – NATO) vznikla na základe Severoatlantickej zmluvy 4. 4. 1949 vo Washingtone. Zmluva bola podpísaná celkom 12 nezávislými štátmi, ktorým zaručovala vzájomnú pomoc v prípade ich napadnutia. Postupom času sa k tejto zmluve pripojovali ďalšie štáty Európy. V roku 1999 sa k Severoatlantickej zmluve pripojila aj Česká Republika a v roku 2004 Slovenská Republika.

V súčasnosti je členom NATO 26 štátov na európskom a severoeurópskom svetadiele. Cieľom organizácie NATO je zaistenie bezpečnosti všetkých členských štátov pri ozbrojených útokoch, ktorými sa rozumie ozbrojený zásah proti územiu členských štátov a proti ostrovom, lodiam alebo lietadlám ktorejkoľvek zmluvnej strany v Atlantickom oceáne na sever od obratníku Raka.

S rozvojom teroristických hrozieb rozšírila NATO svoju pôsobnosť. Na základe realizovaných masívnych kyberútokov na Estónsku národnú internetovú infraštruktúru, ku ktorým došlo v roku 2007, bol v roku 2008 v Bukurešti uskutočnený Summit NATO, kde bola prijatá „Politika v oblasti kybernetickej obrany*"*. [11]

O dva roky neskôr sa konal Summit v Lisabonu, kde bola prijatá „Lisabonská deklarácia" týkajúca sa tiež kybernetickej obrany. [11]

V júny roku 2011 bol prijatý „akčný plán", ktorý je založený na koordinovanom prístupe k počítačovej obrane celej aliancie. Zameriava sa na prevenciu kybernetických útokov a zvyšovanie odolnosti. Všetky štruktúry NATO sú začlenené do centralizovanej ochrany. V rámci tejto revidovanej kybernetickej obrannej politiky sú rovnako stanovené zásady NATO pre kybernetickú obrannú spoluprácu s partnerskými krajinami, medzinárodnými organizáciami, súkromným sektorom a akadémiou obcí. Kybernetická obrana je tak začlenená do „Národného procesu obranného plánovania" (NATO Defence Planning Preocess – NDPP). V oblasti kybernetickej obrany sú v rámci Severoatlantickej aliancie zriadené nasledujúce inštitúcie: [11]

- Poradná skupina NATO pre priemysel (NATO Indrustrial Advisory Group – NIAG),
- NATO Cooperative Cyber Defence Centre of Excellence – NATO CCD-COE,
- NATO Cyber Defence Management Board – CDMB,
- NATO Consultation, Control and Command – NC3,
- NATO Military Authorities – NMA,
- NATO Communications and Information – NCI.

Obecne sa dá zhodnotiť, že spolupráca organizácií Európskej únie a organizácií Severoatlantickej zmluvy je rozmanitá, avšak stále sa hľadajú nové spôsoby zefektívňovania ich vzájomnej kooperácie, aby kybernetická obrana bola čo najúčinnejšia.

5.3 Kybernetická bezpečnosť vo vybraných krajinách

Predchádzajúce podkapitoly boli zamerané na medzinárodnú spoluprácu významných organizácií Európskej únie a Severoatlantickej zmluvy v oblasti bezpečnosti a boji proti kyberterorizmu a kyberkriminality. Táto podkapitola sa zaoberá vplyvom spomínaných organizácií na bezpečnostné politiky nielen jednotlivých členských krajín Európskej únie, ale tiež ostatnými krajinami v oblasti kyberkriminality. Kybernetická bezpečnosť je vo vybra-

ných krajinách zabezpečená hlavne skupinami CERT (Computer Emergency Response Team):

- **Belgicko**

Kybernetickú bezpečnosť v Belgicku zaisťuje skupina CERT.be, ktorá je prevádzkovaná belgickou sieťou národného výskumu BELNET. V minulosti bola kybernetická bezpečnosť zaisťovaná Federálnou verejnou službou pre informačné a komunikačné technológie v spolupráci s Belgickým inštitútom pre poštovné služby a telekomunikácie (Belgium Institute Postal Services and Telecommunications – BIPT).

- **Dánsko**

V Dánsku je kybernetická bezpečnosť zabezpečovaná skupinou DK.CERT (Danish Computer Emergency Responce Team), ktoré bola založená v roku 1991 dánskym Centrom informačných technológií, ktorá spadá pod Ministerstvo školstva Dánska. V Dánsku tiež pôsobí Danish GowCERT, ktorý e riadený Ministerstvom obrany.

- **Estónsko**

Kybernetická bezpečnosť je v Estónsku zaistená skupinou CERT-EE spadajúca do Ministerstva hospodárstva a komunikácií.

- **Litva**

V Litve pôsobí skupina CERT-LT (Lithuanian National Computer Emergency Response Team), ktorá je prevádzkovaná The Communications Regulatory Authority of the Republic of Lithuania.

- **Maďarsko**

Maďarsko zaisťuje kybernetickú bezpečnosť pomocou skupiny CERT-Hungary, ktorá od roku 2010 funguje ako Centrum kybernetickej bezpečnosti Maďarska.

- **Nemecko**

Kybernetická bezpečnosť v Nemecku je zaistená skupinou CERT-BUND, ktorá plní funkciu vládneho tímu.

- **Nórsko**

V Nórsku bol roku 2006 zariadený NorCERT, ktorý je operačným oddelením Národného bezpečnostného úradu Nórska skladajúceho sa z Nórskeho systému pre upozornenie na skoré varovanie systémov digitálnej infraštruktúry a Sekcie pre Incident Handling.

- **Poľsko**

V Poľsku pre zaistenie kybernetickej bezpečnosti funguje tým CERT.GOV.PL.

- **Rakúsko**

V Rakúsku pôsobí v rámci zaistenia kybernetickej bezpečnosti skupiny CERT.at (Computer Emergency Response Team Austria).

- **Spojené kráľovstvo**

Kybernetická bezpečnosť je vo Veľkej Británii riešená skupinou GovCertUK.

- **Spojené štáty Americké**

V Spojených štátoch amerických funguje skupina US-CERT.

- **Španielsko**

V Španielsku existuje niekoľko skupín zaisťujúcich kybernetikú bezpečnosť – napríklad IRIS-CERT, CCN-CERT, INTECO-CERT, CESICAT, CSIRT-GV či ANDULACIA-CERT.

Kybernetická bezpečnosť je niektorých vybraných krajinách zaistená tiež prostredníctvom ďalších inštitúcií či organizácií:

- **Estónsko**

V Estónsku bolo v roku 2008 zriadené NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) so štatútom medzinárodnej vojenskej organizácie, ktoré je akreditované, ako NATO Centre of Excellence.

- **Litva**

Kybernetickú bezpečnosť v Litve tiež zaisťuje Ministerstvo vnútra.

- **Holandsko**

V Holandsku pôsobí tím NCSC-NL (National Cyber Security Centrum), ktoré je pod záštitou Ministerstva bezpečnosti a spravodlivosti.

- **Spojené kráľovstvo**

Jedná sa o Ministerstvo obrany s Operačnou skupinou pre kybernetickú obranu spolupracujúcu s Vládnym veliteľstvom pre komunikácie, ďalej Stredisko globálnych operácií a bezpečnostné kontroly, Centrum pre ochranu národnej infraštruktúry a Centrum výmeny informácií.

- **Spojené štáty americké**

Existuje separátne jednotné kybernetické veliteľstvo (US USCyber Command), ktoré je podriadené hlavnému US veliteľstvu (US Strategic Command), ktoré zdieľa radu právomocí s Ministerstvom pre národnú bezpečnosť. Ďalej sa jedná o National Security Agency (NSA), ktorá je súčasťou Ministerstva obrany.

Vyššie uvedené inštitúcie a organizácie zaisťujú vo vybraných štátoch kybernetickú bezpečnosť spracovávaním dokumentov týkajúcich sa boja proti kybernetickej kriminalite a kyberterorizmu. Sú to hlavne:

- **Litva**

Ide o dokument „Program rozvoja bezpečnosti elektrickej informácie (kybernetickej bezpečnosti) na obdobie 2011-2019“.

- **Nemecko**

Nemecko ma vypracovanú „Stratégiu pre kybernetickú bezpečnosť“, ktorej základom je činnosť Centra pre kybernetickú obranu, ktoré podlieha Spolkovému úradu pre informačnú bezpečnosť a Rady kybernetickej bezpečnosti.

- **Poľsko**

Jedná sa o „Vládny program ochrany kebyrpriestoru Poľskej republiky v rokoch 2011 až 2019“.

- **Spojené kráľovstvo**

Veľká Británia schválila „Stratégiu kybernetickej bezpečnosti do roku 2015“. Ďalej je na obdobie 4 rokov vypracovaný „Národný program kybernetickej bezpečnosti“ s rozpočtom 650 000 000 GBP.

- **Spojené štáty americké**

V Spojených štátoch amerických bol v roku 2009 spracovaný strategicky dokument „Cyberspace Policy Review“, v roku 2010 potom „Národná bezpečnostná stratégia (NSS)“ a „Obranná doktrína (QDR)“. V roku 2011 boli prijaté dokumenty „National strategy for Trusted Identities in Cyberspace (NSTIC)“, „International Strategy for Cyberspace“. „Defense Strategy for Cyberspace“ a „Quadrennial Homeland Security Review“.

5.4 Terorizmus a boj proti jeho financovaniu v informačnom veku

Všetky opatrenia krajín proti kybernetickej kriminalite sa týkajú aj boja proti kyberterorizmu alebo terorizmu. V dnešnej dobe rozvoja technológií sa všetko v našich životoch presúva do kyberpriestoru. Rovnako, ako tento rozvoj pomáha a zjednodušuje náš život je tomu aj v rámci svetového terorizmu. Tento nový druh terorizmu nazývame informačný terorizmus, ktorého účinky nemajú taký ničivý účinok, každopádne jeho sekundárny devastačný efekt je niekedy zrovnateľný so zbraňami hromadného ničenia. Financovanie kyberterorizmu sa zabezpečuje viacerými spôsobmi, medzi ktoré patria nasledujúce body.

5.4.1 Falošné webové stránky

Kyberpriestor radikálne zjednodušil teroristom získavanie financií. Na internete môžeme nájsť veľké množstvo webových stránok, ktoré vystupujú ako nadačné, charitatívne s islamom spojené organizácie, ktoré pod zámienkou zbierok peňazí na vzdelanie, vieru a podobne, získavajú prostriedky, z ktorých veľká časť končí na potreby teroristov. Krajiny s týmto tipom financovania terorizmu zatiaľ nevedia bojovať, pretože stránok je veľa a často menia svoju pôsobnosť.

5.4.2 Pranie špinavých peňazí

Patrí medzi najzávažnejšie svetové problémy a to hlavne vďaka rozvoju informačných technológií, pretože základom tohto procesu je mať bezhotovostné peniaze, teda použitie internetbankingu. Páchatelia sa vyhýbajú odhaleniu trestných činov tak, že svoje nelegálne získané prostriedky „vyperú“. Tento proces ma tri etapy:

- umiestnenie –táto etapa spočíva v umiestnení prostriedkov do obehu, najčastejšie prostredníctvom uloženia pomocou internetbankingu na účet,
- presun – zakrytie pôvodu finančných prostriedkov, jedná sa o rôzne internetové transakcie, nákupy alebo predaj nehnuteľností alebo cenných papierov,

- návrat – prevedenie zisku naspäť majiteľovi.

Financovanie terorizmu touto formou predstavuje dve formy:

- zhromažďovanie peňazí alebo iného majetku s vedomím, že bude použitý k spáchaniu trestného činu teroru, teroristického útoku alebo trestného činu, alebo k podpore osoby alebo skupiny k spáchaniu takéhoto činu,
  alebo
- jednanie vedúce k poskytovaní odmeny alebo odškodného páchateľa trestného činu teroru, teroristického útoku alebo trestného činu.

V januári roku 2015 Európska únia pripravila smernicu proti praniu špinavých peňazí, pretože sa snaží zastaviť financovanie terorizmu pomocou internetbankingu. Začalo to medzinárodnou dohodou USA a Českej republiky FATCA, vtedy Česká republika prisľúbila predávanie citlivých informácií o finančných transakciách do USA. Neskôr európska únia žiadala o možnosť sledovania menších anonymných presunov peňazí slúžiacich k podpore teroristických skupín.

V informačnom veku sa teroristom jednoznačne otvorili nové možnosti, nie len v jeho financovaní, ale tiež propagácií. Teroristi využívajú tiež internet na veľké množstvo návodov na výrobu strelnej bavlny, dynamitu, nitroglycerinu či tritolu. Nájsť sa dá aj výroba bomby, časovačov a tiež samostatná konštrukcia pum. Z hľadiska plánovania teroristom pomáhajú všetky druhy médií, lebo venujú týmto správam veľkú pozornosť

6 NÁVRHY ZABEZPEČENIA PROTI KYBERTERORIZMU

Na záver chcem zhrnúť hlavné problémy kyberterorizmu a kyberkriminality, prípadne navrhnúť možnosti zlepšenia.

6.1 Návrhy a zabezpečenia všeobecné

Keď chceme zlepšiť ochranu proti kriminalite v kyberpriestore je dôležité poznať chyby a problémy, ktoré v existujú, rátať s nimi a prípadne im predchádzať.

- Najväčší problém je to, že informačné a komunikačné technológie sa stali nenahraditeľnou súčasťou našich životov. Na internete začala byť závislá súkromné aj verejná sféra. Napríklad internet používa až 97% firiem v Českej republike.
- Stúpa počet užívateľov mobilných zariadení a s nimi stúpa aj počet mobilných malware.
- Stále viac výrobcov sa zameralo na výrobu hardware. V toľkom množstve dodávateľov, je možnosť kúpenia zariadenia od výrobcu, ktorý je potom určený na sledovanie alebo získavanie dôležitých či osobných a citlivých dát.
- Užívateľov internetu je stále viac a viac, ale veľakrát sa stane, že majú slabé povedomie o digitálnej hygiene. Nevedia ako sa v on-line prostredí pohybovať a ako zabezpečiť zariadenie.
- Riziká sa spájajú s neustálou elektronizáciou dôležitých častí štátnej správy.
- Ochrana a zabezpečenie dát je veľmi dôležité, hlavne kvôli predchádzajúcemu bodu. Dáta užívateľov sú v tomto prípade veľmi dôležité. Začali sme preto využívať nové formy ukladania dát, napríklad cloudové úložiská. S nimi prichádza veľké riziko straty dát, dôveryhodnosť je teda často sporná.
- Nejedná sa len o kyberkriminalitu pri ktorej dochádza k ekonomickému prospechu. Musíme rátať aj s kybernetickou špionážou, vandalizmom a hľadanie slabého miesta významných informačných systémov. Útočníci sa stále zameriavajú na dôležité systémy napríklad v zdravotníctve, čo môže mať fatálne následky.
- Škodlivý software sa rozvíja rovnakou rýchlosťou ako všetky technológie a všetko s tým spojené. Vyšetrovatelia, ktorý takýto zločin musia byť vyškolený na kybernetickú bezpečnosť, aby mali aspoň malú šancu nájsť vinníka.

6.1.1 Hlavné ciele v boji proti kyberterorizmu

- **Zaistenie efektivity a posilňovanie všetkých štruktúr, procesov a spolupráce pri zaiťovaní kybernetickej bezpečnosti**

Je potrebné vytvoriť model spolupráce ako na národnej tak aj na medzinárodnej úrovni. Národné zložky ako CSIRT a CERT musia neustále zlepšovať spôsob riešenia incidentov a tiež komunikáciu pre lepší priebeh počas nich. Udržovať jednotný postoj všetkých zložiek smerom k ostatným rezortom zainteresovaných do problematiky kybernetickej bezpečnosti. Zohľadňovať odpovedajúcim spôsobom neustále sa vyvíjajúcu problematiku kybernetických hrozieb v rámci tvorby bezpečnostne - strategických materiálov.

- **Aktívna spolupráca na medzinárodnej úrovni**

Ako členský štát patriaci do Európskej únie, Severoatlantickej aliancie či Organizácie spojených národov, musíme z tejto skutočnosti ťažiť čo najviac. Byť aktívny člen týchto spoločností a podieľať sa na medzinárodných činnostiach. Organizovať medzinárodné cvičenia a školenia pre odborníkov z tohto odvetvia. V neposlednej rade sa musíme podieľať na tvorbe medzinárodného štandardu v rámci oficiálnych aj neoficiálnych kanálov ohľadom právnych noriem a chovania sa v kybepriestore, zaistenia otvorenosti internetu či ľudských práv a slobôd.

- **Koordinácia verejného a súkromného sektoru**

Vytvoriť spoľahlivý priestor na šírenie informácií, výskum a vývoj a zaistiť bezpečnú informačnú infraštruktúru. Vzdelávať sa neustále v oblasti kybernetickej bezpečnosti a poskytnúť potrebné vedomie, ako sa správne chovať nielen pri mimoriadnych situáciách, respektíve kybernetických incidentoch, ale aj pri každodennej činnosti. Vytvoriť medzi týmito dvoma sektormi dôveru a to tým, že sa vytvorí systém na národnej úrovni pre výmenu informácií o hrozbách incidentoch a aktuálnej situácií.

- **Výskum a vývoj**

Podieľať sa na spolupráci s akademickým sektorom a zabezpečiť vývoj technológií využívaných štátom k zaisteniu maximálneho zabezpečenia. Zabezpečiť prostriedky pre rozvoj tohto sektoru a testovanie týchto technológií. Určiť tento rozvoj a investície ako prioritu.

- **Vzdelávanie a rozvoj informačnej spoločnosti**

Zlepšovať povedomie a schopnosti v otázkach kybernetickej bezpečnosti u žiakov a študentov základných a stredných škôl. Neustále modernizovať študijné programy a plány výučby, ktoré by mali vytvárať experti v tejto oblasti. Taktiež vzdelávať aj učiteľov a profesorov v problematike kybernetickej bezpečnosti a informačnej kriminality.

- **Podpora rozvoja schopnosti polície**

Posilniť jednotlivé policajné oddelenia o odborníkov v informačnej kriminalite a tiež modernizovať technologické vybavenia na policajných pracoviskách. Dôležité je spolupracovať so zahraničnými subjektmi a predávať si informácie k informačnej kriminalite a v oblasti vzdelávania. Vybudovať program vzdelávania policajtov špecialistami.

- **Právne predpisy pre kybernetickú bezpečnosť**

Vytvárať právne predpisy priamo pre kybernetickú kriminalitu, ktoré by boli vytvorené priamo pre daný problém. Taktiež je potrebné vzdelávanie v problematike kybernetickej bezpečnosti v rámci justičných orgánov.

6.2 Technické návrhy a zabezpečenia

6.2.1 Zabezpečenia proti DoS útokom

Základom kybernetickej bezpečnosti je zabezpečenie dostupnosti, integrity a dôveryhodnosti informácií. Intenzívne DoS útoky v roku 2013 vedené v niekoľkých vlnách proti známym webovým serverom a službám v Českej republike výrazným spôsobom obmedzili prvú zásadu kybernetickej bezpečnosti – dostupnosť služieb a tým spojených informácií. To je možné urobiť na aspoň jednej súčasti samotného systému: výpočtovej kapacite, operačne pamäti alebo sieťovému pásmu.

Pre začiatok je dobré pochopiť, či sa jedná o útok typu DoS (Denial of Service) alebo DDoS (Distributed Denial of Service). Aj keď je výsledok v obidvoch prípadoch rovnaký, zásadne sa odlišujú počtom zdrojov, ktoré útok generujú. Pakety môžu prichádzať k cieľu z rôznych zdrojov, k čomu sa najčastejšie využívajú botnety. Detekcia sa tak stáva pomerne náročná pretože nie je možné jednoducho definovať zdroj DDoS a zamedziť tak útok. Napríklad s využitím blokácie IP rozsahov, ktoré zahlcujú systém obeti.

DoS resp. DDoS útok je obvykle smerovaný na jednu zo sieťových vrstiev. Cez každú vrstvu je možné nejakým spôsobom službu vyradiť z prevádzky, avšak zabezpečenie jed-

nej vrstvy často nezabráni útoku na inú. Preto je nevyhnutné venovať pozornosť každej vrstve zvlášť. Podľa toho na ktorú z OSI vrstiev sa útočník zameria sa odlišuje tiež samotný spôsob útoku. [24]

Aby sme mohli útok zaznamenať, je potrebné vedieť, čo sa v sieti odohráva. K tomu slúži pasívne monitorovanie siete. Prevádzkari by mali pasívne monitorovať prevádzku na svojich smerovačoch optimálne až exportom NetFlow/sFlow. Tieto exporty im umožňujú zaznamenávať informácie o prevádzke. Dáta slúžia na prípadnú spätnú identifikácie útoku. Mimo pasívnej ochrany, by sa mala využívať aj ochrana aktívna. K aktívnej ochrane pristupujeme, ak chceme podozrivý tok dát odfiltrovať. Aby tak pozorovatelia siete učinili, je nevyhnutné mať k dispozícii aspoň zdrojovú a sieťovú IP adresu a TCP/UDP porty.[24]

Jednou z možností ako zastaviť pakety ešte pred tým, ako dorazí do siete, je technika známa ako Remotely-Triggeled Black hole. Ta využíva možnosti BGP protokolu k tomu aby obmedzila pakety odosielané na rozsah obete zo smeru, ktorý daná relácia obsahuje. [24]

Vrstva OSI	Využívaný protokol a služby	Príklad techniky útoku	Zmiernenie uvedeného príkladu
Aplikačná vrstva	**FTP, DNS, DHCP, POP3, SMTP, SSH, Telnet, TFTP**	**HTTP get/post - prihlasovanie do aplikácie, upload videa, zasielanie komentárov**	**monitorovanie aplikácie, CAPTCHA**
Prezentačná vrstva	**komprimácia, šifrovania, konvertovanie**	**útok pomocou upravených SSL dotazov**	**presmerovanie SSL dotazov z pôvodnej infraštruktúry cez iný zdroj**
Relačná vrstva	**zahájenie a ukončenie relačného spojenia**	**obmedzenie služieb inak prístupných cez Telnet**	**útok je možný v dôsledku zraniteľnosti, ktorá môže byt updatom odstránená**
Transportná vrstva	**TCP, UDP**	**SYN flood, Smurf attack. Obmedzuje počet sieťových pripojení na zariadeniach.**	**informovanie o blackholingu u svojho poskytovateľa pripojenia**
Sieťová vrstva	**smerovanie a sieťové adresovanie**	**ICMP flooding**	**stanovenie limitu na ICMP**
Linková vrstva	**smerovače a prepínače**	**MAC flooding**	**obmedzenie počtu MAC adries ktoré môžu porty prijímať**
Fyzická vrstva	**sieťové káble**	**fyzická manipulácia s vedením**	**obmedzenie fyzického prístupu**

Tabuľka 3 – **Ochrana vrstiev OSI pred DoS/DDoS útokmi** [24]

6.2.2 Základné minimum zabezpečenia webovej stránky

V súčasnosti sú požiadavky na webové aplikácie veľmi vysoké, ako zo stravy užívateľov ale aj zo strany prevádzkovateľov. Aj napriek tomu, že správcovia stránok majú dobré vedomosti o tom ako majú byť stránky zabezpečené, veľakrát narazíme na ich absenciu. Nižšie si povieme niekoľko hlavných bodov pri zabezpečení webovej stránky.

- **Pravidelné aktualizácie a sledovanie zraniteľnosti**

Bez ohľadu na to aký CMS, webový server či doplnky sú používané, je dôležité mať všetky verzie pravidelne aktualizované. Zraniteľnosť pre jednotlivé verzie nie je žiadne tajomstvo a práve nedôslednosť pri aktualizáciách sa často využíva pri útokoch.

- **Nezverejňovanie informácií o použitých platformách**

Nie je vhodné zverejňovať informácie o softwarových doplnkoch ktoré sú na webovej stránke použité. Ako som spomínala v predchádzajúcom bode, pre každú verziu sú na internete zverejnené jej slabé stránky.

- **Šifrované spojenie a certifikáty**

Toto sa v dnešnej dobe už stalo viac menej štandardom, na webových stránkach, kde prebieha výmena informácií. Tieto informácie, sú šifrované a teda nie je možné ich treťou osobou odchytiť, či zneužiť.

- **Ošetrenie všetkých vstupov**

Aj napriek filtrov na strane prehliadača je nevyhnutné ošetrenie vstupov aj na webe. Čím je web rozsiahlejší, tým viac pozornosti vyžaduje kontrola vstupov do aplikácie.

- **Silná politika hesiel**

Požiadavky na heslá by mali byť nastavené minimálne na 8 znakov dlhé heslo obsahujúce malé a veľké písmená, čísla a špeciálne znaky.

6.2.3 Obrana proti spamu

V takmer všetkých falošných e-mailových správach je adresa odosielateľa podvrhnutá. Jeden zo spôsobov ako tomu zabrániť spočíva v zahrnutí SPF (Sender Policy Framework) do DNS záznamov domény. Tento štandard umožňuje určiť, ktoré zariadenia budú autorizované na odosielanie pošty s adresou domény. Takto vložený záznam potom prijímateľ

pošty môže overiť a pokiaľ pochádza z neautorizovaného zdroja, správu odmietne ešte pred tým ako tento spam príjme.

6.2.4 Zabezpečenie otvorených služieb

Je potrebné na internet vystaviť iba služby, pri ktorých to naozaj chceme a potrebujeme. V prípade, že služby nie je potrebné mať dostupné z internetu, je dobré ich dostupnosť obmedziť. Dôležité, je pravidelne vykonávať priebežný audit, aby sa zistilo, ktoré služby v systéme je potrebné zverejňovať.

Ak služba už je dostupná na internete, je dôležité nastaviť dostatočne silné prihlasovacie údaje. Pri slovníkových útokoch či použití brbte forme sú ako prvé prelomiteľné heslá, ktoré administrátori nezmenia z prednastavených nastavení. Nechávať nastavené prihlasovacie údaje ako admin:password alebo admin:1234 je veľmi nebezpečné.

Doležíte je už spomínané šifrovanie. Šifrované protokoly majú opodstatnenie najmä, keď sa prenášajú citlivé údaje, ako prihlasovacie meno a heslo. Použiť sa dá:

- ssh namiesto telnetu,
- FTP/SFTP alebo scp namiesto ftp,
- šifrované verzie poštových protokolov (pop3s, imaps, smtps),
- https namiesto http, v prípade, keď nechceme aby boli prenášané údaje po ceste odchytené.

ZÁVER

V tejto práci som pracovala s tým aký je terorizmus a hlavne kyberterorizmus veľká hrozba. Hlavne v dnešnej dobe plnej techniky sa terorizmus a jeho prostriedky, ale aj dôsledky premiestnili do kybepriestoru. Môžem povedať, že kyberpriestor už nie je miestom slobodnej výmeny informácií, ale priestor plný hrozieb.

V teoretickej časti som sa cez vymedzenie pojmu terorizmus, ďalej cez jeho históriu dostala k opisom jeho foriem a trendom v dnešnej dobe. Opisovala som vývoj terorizmu, ako sa postupom času prispôsoboval a menil podľa doby v ktorej bol páchaný. Keďže doba, v ktorej žijeme je označovaná ako informačný vek, takýmto spôsobom sa vyvíjal aj terorizmus. Jeho účinky, ale tiež prostriedky získavanie k jeho financovaniu sa premiestnili do kybernetického priestoru.

Praktická časť je venovaná štatistikám a následnej analýzy kybeútokov z posledného obdobia vo svete a tiež v Českej a Slovenskej republike. Pre príklad som spomenula aj najznámejšie kybernetické útoky, ktorými boli napadnuté štáty, ako je Amerika, Rusko alebo Čína. Aj keď Česká a Slovenská republika nepatria k popredne napádaným štátom sveta, taktiež sú kyberteroristami napádané, preto sú v práci spomenuté aj kybernetické útoky na české a slovenské servery. V poslednej dobe bola aj Česká republika nútená urobiť určité opatrenia v boji proti kyberterorizmu. Dôvodom je aj zvyšujúci sa počet týchto incidentov, ale vo veľkej miere sa o to zapríčinila Európska únia, ktorá sa obsiahlo tejto téme venuje. Aj napriek tomu je Slovenská republika v problematike počítačovej bezpečnosti pozadu oproti susednej Českej republike.

Záver práce je venovaný mojim návrhom a to tým všeobecným z pohľadu štátu, čoby mal štát, ale aj obyčajný užívateľ zlepšiť, urobiť alebo na čo by mal myslieť v probléme kybernetickej bezpečnosti. Taktiež spomeniem niektoré technické zabezpečenia, vhodné pre bežného užívateľa, ale aj prevádzkara webovej stránky alebo určitej otvorenej služby na internete. Tento boj, z hľadiska užívateľov, je veľmi náročný, lebo útočníci sú experti vo svojom obore, ktorý sú vždy o pár krokov popredu oproti ostatným. Veľmi často sa v práci spomína skupina Anonymous, ktorá je presne takým príkladom, odborníkov, ktorí žijú pre ciele tejto skupiny a bojujú svojim spôsobom za „dobrú vec“.

Či už teoretická ale aj praktická časť, sú vždy opísané s aj z technickej stránky ale aj z pohľadu ekonomického či právneho.

ZOZNAM POUŽITEJ LITERATÚRY

[1] Terorizmus | Slovník. [online]. 2010 [cit. 2015-02-17]. Dostupné z: http://vzdelavanie.nadaciapontis.sk/slovnik/Slovn%C3%ADk-pojmov-1/T/Terorizmus-49/#Top

[2] Encyklopedie Světový terorismus od starověku až po útok na USA: 1. vyd. Praha: Svojtka & Co., 2001. ISBN 80-7237-340-4

[3] HUNTINGTON, S.P. Střet civilizací – Boj kultur a proměna světového řádu. 1 ed. Praha: Rybka Publisher, 2001, s. 83—96. ISBN 80-86182-49-5. 448 s.

[4] EICHLER J. Asymetrické války. Vojenské rozhledy, Praha, 2004, roč. 14 (46), č. 2. s 17—26. ISSN 1210-3292.

[5] Globální terorismus, blíže viz. EICHLER, J. Mezinárodní bezpečnost na počátku 21. století. 1. vyd. HISTORICKÝ VÝVOJ TERORISMU Praha: AVIS, 2006, s. 159—161. ISBN 80-7278-326-2. 303.

[6] JANOUŠEK, M. Obrana a stratetgie: Kyberterorismus: Terorismus informační společnosti [online] [cit. 2013-06-13]. Dostupné na www: <www.defenceandstrategy.eu/cs/archiv/rocnik-2006/2-20>.

[7] Globální terorismus, blíže viz. EICHLER, J. Mezinárodní bezpečnost na počátku 21. století. 1. vyd. HISTORICKÝ VÝVOJ TERORISMU Praha: AVIS, 2006, s. 159—161. ISBN 80-7278-326-2. 303.

[8] List25. *25 biggest cyber attacks in history* [online]. 2011 [cit. 2015-04-11]. Dostupné z: http://list25.com/25-biggest-cyber-attacks-in-history/

[9] Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. *Council of the European Union*[online]. 2013 [cit. 2015-04-11]. Dostupné z: http://eeas.europa.eu/background/origins-of-the-european-external-action-service/index_en.htm

[10] EUR-Lex. *Přístup k právu Evropské unie* [online]. 2010 [cit. 2015-04-11]. Dostupné z:http://eur-lex.europa.eu/homepage.html?locale=cs

[11] FOLTIN, Pavel. Mezinárodní spolupráce v boji proti terorismu. *Obrana a strategie* [online]. 2007, 1/2007 [cit. 2015-04-11]. Dostupné z: http://www.obranaastrategie.cz/cs/aktualni-cislo-1-2007/clanky/mezinarodni-spoluprace-v-boji-proti-terorismu.html#.VSlCC_msUuc

[12] CARR, C. Dějiny terorismu : dějiny války proti civilistům. Praha: Práh, 2002. 184 s. ISBN80-7252-063-6

[13] EICHLER, J. Terorismus a války na počátku 21. století. Praha: Karolinium, 2007. 354 s. ISBN 978-80-246-1317-8

[14] JIROVSKÝ, Václav. Kybernetická kriminalita -- nejen o hackingu, crackingu, virech a trojských koních bez tajemství.

[15] *CSIRT: Statistiky řešených incidentů* [online]. 2011 [cit. 2015-04-26]. Dostupné z: https://www.csirt.cz/page/2635/statistiky-resenych-incidentu/

[16] *Cyber espionage* [online]. 2011 [cit. 2015-04-26]. Dostupné z:http://hackmageddon.com/tag/cyber-espionage/

[17] Národní strategie kybernetické bezpečnosti České republiky na období let 2015 až 2020. [online]. 2015, č. 1 [cit. 2015-05-01]. Dostupné z: https://www.govcert.cz/cs/informacni-servis/strategie-a-akcni-plan/

[18] *Encyklopedický slovník češtiny*. Editor Petr Karlík, Marek Nekula, Jana Pleskalová. Praha: Nakladatelství Lidové noviny, 2002, 604 s. ISBN 80-7106484-x.

[19] ŽALOUDEK, Karel. *Encyklopedie politiky*. 2., přeprac. a aktualiz. vyd. Praha: Libri, 1999, 559 s. ISBN 80-85983-75-3.

[20] *Blackwellova encyklopedie politického myšlení*. Vyd. 2. Editor William E Connolly, David Miller, Alan Ryan, Janet Coleman. Brno: Barrister & Principal, 2000, xiii, 581 s. Studium (Barrister & Principal). ISBN 80-85947-56-0.

[21] KRIEGER, Joel. *Oxfordský slovník světové politiky*. České vyd. 1. Praha: Ottovo nakladatelství, 2000, xxx, 1090 s. ISBN 80-7181-463-6.

[22] JÍROVSKÝ, V. Kyberterorismus. ICTfórum/PERSONALIS 2006. [předneseno 27.9.2006]. Praha.

[23] Denial of service dos attacks. *Hacker´s Choise* [online]. [cit. 2015-05-08]. Dostupné z: http://hacksguide.blogspot.cz/2009/06/denial-of-service-dos-attacks.html

[24] CSIRT. 2014. *CSIRT - Základní princípy DoS útoku* [online]. [cit. 2015-05-08]. Dostupné z: https://www.csirt.cz/page/2790/zakladni-principy-dos-utoku/

ZOZNAM POUŽITÝCH SYMBOLOV A SKRATIEK

ACK	Potvrdzovací znak pri prenose dát.
a pod.	a podobne.
CIA	Central Intelligence Agency
ICT	Informačné a komunikačné technológie.
IP	Internetový protokol.
napr.	napríklad.
NCKB	Národné centrum kybernetickej bezpečnosti.
p.n.l.	pred naším letopočtom
RST	Odpoveď na službu.
SYN	Synchronizovať.
TCP	Transmission Control Protocol.
tj.	to je.
tzv.	takzvaný.
ZHN	Zbrane hromadného ničenia.

ZOZNAM OBRÁZKOV

ZOZNAM TABULIEK