UNIVERZITA KARLOVA V PRAZE

FAKULTA HUMANITNÍCH STUDIÍ

Katedra Elektronické kultury a sémiotiky

Bc. Pavel Latoň

Kyberterorismus - mediální hrozba

Diplomová práce

Vedoucí práce: **PhDr. Zdeněk Zbořil**

Praha 2013

Prohlášení

Prohlašuji, že jsem předkládanou práci zpracoval samostatně a použil jen uvedené prameny a literaturu. Současně dávám svolení k tomu, aby tato práce byla zpřístupněna v příslušné knihovně UK a prostřednictvím elektronické databáze vysokoškolských kvalifikačních prací v repozitáři Univerzity Karlovy a používána ke studijním účelům v souladu s autorským právem.

V Praze dne 28. června 2013 Pavel Latoň

Poděkování

Na tomto místě bych především rád poděkoval svému vedoucímu diplomové práce PhDr. Zdeňku Zbořilovi za velice podnětné vedení práce, vstřícné konzultace a trpělivé komentování jednotlivých fází práce.

Obsah

Abstrakt

Diplomová práce Kyberterorismus jako mediální hrozba se zabývá fenoménem teroristických útoků v rámci kyberprostoru, mediálním diskurzem, v rámci kterého je konstruována realita kyberterorismu v médiích, a jejího vlivu na proces sekuritizace kyberterorismu. Dále se zabývá srovnáním tradičních forem terorismu s těmi, jež se vyvinuly s příchodem nových komunikačních technologií. V práci je nastíněn vývoj pojmu terorismus od jeho vzniku až po současnost. Cílem práce je poukázat na kyberterorismus jako na latentní hrozbu informační společnosti. K interdisciplinárnímu přístupu je použita metoda diskurzivní analýzy. Tvorba sociální a mediální reality je rozebrána na základě teorie Niklase Luhmanna a poukazuje na sebereferenci autopoietických systémů a referenci druhého, jako klíčového pojmu při konstruování reality médií. Další část práce je věnována reakci Evropské unie a Severoatlantické aliance (NATO) na „hrozbu“ kyberterorismu.

Abstract

The subject of my diploma thesis, Cyber terrorism as a medial threat, is a phenomenon of terrorist attacks in cyberspace, media discourse, within the reality is constructed cyber terrorism in the media and its impact on the securitization of cyber terrorism process. It also deals with the comparison of traditional forms of terrorism with those that have evolved with new communication technologies.The thesis outlines the development of the concept of terrorism from its beginning to the present. The aim of the thesis is to show Cyber terrorism as a latent threat to the information society. For the interdisciplinary approach is used the method of discourse analysis. Creating a social and media reality is analyzed based on the theory of Niklas Luhmann and points to the autopoiesis self-reference systems and reference each other, as a key concept in the construction of reality by the media. Another section is devoted to the reaction of the European Union and North Atlantic Treaty Organization (NATO) on the "threat" of cyber terrorism.

Klíčová slova

Terorismus, kyberterorismus, sebereference, autopoiesis, sekuritizace

Keywords

Terrorism, cyber terrorism, self-reference, autopoiesis, securitization

1. Úvod

Nové informační a komunikační technologie (ICT) v čele s Internetem patří bezpochyby k nejzásadnějším technologickým vynálezům dvacátého století. Počítačové technologie, které byly ve svých počátcích dostupné pouze elitním výzkumným ústavům a nejbohatším firmám se díky miniaturizaci a zlevňování staly na konci dvacátého století všudypřítomnou a fakticky nepostradatelnou součástí života nejen západní společnosti. Tyto technologie prostupují všemi oblastmi našeho života od každodenní komunikace, až po řízení procesů v jaderných elektrárnách či přehradách. Vzrůstající závislost na nových technologiích nepřináší však pouze pozitiva, nýbrž je s ní spojen také latentní nárůst rizik a ohrožení, vyplývající ze zneužití těchto technologií. Jednou z latentních hrozeb, která se objevuje s masivním rozšířením uživatelů internetu a ICT, je hrozba kybernetického terorismu.

Kybernetický terorismus a obecně témata spojená s využitím nových informačních a komunikačních technologií, respektive jejich zneužívání vedoucí k ohrožení běžných uživatelů, ekonomických subjektů i států nabírají v poslední době ve všech oblastech společnosti a politiky na aktuálnosti spojené s nárůstem a zvýšenou sofistikovaností útoků provedených v rámci kyberprostoru. Problém kybernetických útoků označil Pentagon jako *„hrozbu katastrofických rozměrů a vážné ohrožení národní bezpečnosti“*[1] již v roce 1996. Je otázkou, do jaké formy a stupně nebezpečí se od té doby kybernetický terorismus dostal, což bude také předmětem zkoumání mé práce. Téma kybernetického terorismu se dostává do zájmu médií a mediálního diskurzu i analýz v rámci bezpečnostních studií na počátku jednadvacátého století spolu s mezinárodním bojem proti terorismu po útocích na WTC z 11. září. Teroristické organizace již nepoužívají pouze tradičních metod vedení boje, ale ke své činnosti stále častěji využívají také informačních technologií a stávají se nedílnou součástí kyberprostoru.

Tato práce se zabývá kybernetickým terorismem v jeho rozličných formách a dává jej do kontextu současného vývoje celého kyberprostoru, společnosti a mediálního diskurzu. Zabývá se mediální konstrukcí pojmu kyberterorismu a dopadu této konstrukce na vytváření sekuritizačního procesu. V práci se věnuji také komparaci klasických forem terorismu a jejich účinků s kybernetickým terorismem a částečně také kybernetickému

[1] San Francisco Chronicle, 23. května 1996. In: BUZAN, B., WAEVER, O., DE WILDE, J.. *Bezpečnost: Nový rámec pro analýzu*. 1. vyd. Brno: Barrister & Principal, 2005. s. 36. ISBN 80-903333-6-2.

warfaru[2], jenž je součástí informační války a byl umožněn implementací nových technologií do armádních strategií vedení boje. Pátá kapitola je věnována rozboru kyberterorismu jako autoreferenčního problému v intencích teorie Niklase Luhmanna. Zkoumaná oblast je vymezena na členské státy NATO a Evropské unie. Danou problematiku budu zkoumat od přelomu dvacátého a jedena dvacátého století po současnost.

[2] Ve své práci budu používat anglické slovo warfare, jelikož jeho překlad je značně problematický a je používáno v řadě českých publikací, které se tímto problémem zabývají. Slovo warfare by se dalo přeložit jako užití určitých prostředků boje ve válce. Například bude-li nějaký stát padělat peníze svého válečného protivníka, aby došlo k devalvaci jeho měny, bude se jednat o ekonomický warfare, jinými slovy užití ekonomických nástrojů ve válce. Kybernetickým warfarem tak budeme rozumět užití kybernetických prostředků ve válce.

2. Hypotéza práce, metodologie a cíl práce

2.1. Hypotéza

Jak jsem zmínil výše, kybernetický terorismus je společně s narůstající závislostí společnosti na ICT technologiích fenoménem posledního desetiletí, ke kterému se čím dál tím častěji uchyluje celá řada skupin, která nesouhlasí se současným společenským systémem západní společnosti a snaží se tak dosáhnout svých cílů za pomocí demonstrace síly v kyberprostoru. Kyberterorismus je latentní hrozbou 21. století. Analýzu tohoto fenoménu budu provádět ve dvou rovinách. Zaprvé v rovině systémové, vycházející z pojetí systémů, jejich vývoje a autopoesis u Niklase Luhmanna. Zadruhé v rovině bezpečnostní, kde je potřeba analyzovat proces sekuritizace kyberterorismu a jeho zařazení do bezpečnostního diskurzu.

Hypotézou práce je, že přestože považujeme kyberterorismus za latentní hrozbu, tak se při zvýšení agresivity útoků v kombinaci s efektivitou a novými prostředky jak napadat infrastrukturu států, může stát reálnou hrozbou 21. století. V důsledku těchto útoků se stává z kyberprostoru nikoliv místo svobodné výměny informací, ale prostor, v němž hrozí permanentní nebezpečí napadení.

2.2. Metoda výzkumu

Jako metoda výzkumu této práce bude použita kritická diskurzivní analýza (CDA) doplněná bezpečnostní analýzou zaměřenou na proces sekuritizace a komparací. Média a specifický typ sociální komunikace, na jejíž realizaci se podílejí, představují stále významnější podobu společenského i kulturního života současných společností. Média v současné době disponují mocí, jež jim umožňuje konstruovat sociální realitu. Tato práce se zaměřuje na přístup médií ke kyberterorismu a teroristickým útokům a způsob, jakým o nich média referují.

Nejprve představím vznik a vývoj CDA a budu se věnovat hlavním výstupům bezpečnostní analýzy a pojmu sekuritizace, který úzce souvisí s mediálním diskurzem a jeho schopností začleňovat témata do samotného bezpečnostního diskurzu.

2.2.1. Kritická analýza diskurzu

„Diskurzivní analýza představuje hodně věcí pro hodně lidí.“[3]

Vznik a vývoj kritické analýzy diskurzu

Vznik kritické analýzy diskurzu *Critical Discourse Analysis* (dále jen „CDA“) se datuje od počátku 90. let 20. století. Je spojen s konáním sympozia v Amsterodamu, na kterém společně diskutovali známí kritičtí analytici. Její počátky však sahají do 70. let 20. století, neboť se v této době začalo pracovat s pojmy diskurz či analýza textu. CDA později vzniká na základech a principech kritické lingvistiky, která vycházela z teze, že jazyk je formou sociální praxe.[4]

Jak zdůrazňuje Roger Fowler ve své stati O kritické lingvistice: *„…kritická lingvistika klade důraz na skutečnost, že všechny reprezentace jsou zprostředkované a formované hodnotovým systémem, který je hluboko zakořeněný v jazyce. Cokoli může být prezentováno mnoha způsoby a pokaždé s jiným významem“*[5].

CDA nepracuje s jedinou metodou, spíše se jedná o sdružení více analytiků vycházejících z podobných postupů a navazujících na stejné zdroje. Existují čtyři základní směry, jež se vytvořily okolo jednotlivých autorů:[6]

- **Kritická lingvistika.** Vzniká ve druhé polovině 70. let ve Velké Británii a Austrálii. Je spojena se jmény Rogera Fowlera, Roberta Hodge či Gunhera Kresse. Kritičtí lingvisté se zaměřovali především na lexiální kategorizace a tranzitivu v jejich proměnách v různých kontextech a napříč různými žánry, především zkoumali média.
- **Socio-kognitivní přístup.** Jeho hlavním představitelem je holandský lingvista Teun van Dijk, který uvádí, že hlavní styčnou plochou mezi diskurzem a společností je individuální a sociální vědomí.[7] Cílem CDA je ukázat vlivy jak historických,

[3] ANTAKI, Ch. *Analysing Talk and Text. A Course for the Universidad Autónoma de Barcelona* [online] [cit. 2013-06-13]. Dostupné na www: <http://www.staff.lboro.ac.uk/~ssca1/tthome.htm>.
[4] Tamtéž
[5] FOWLER, R. On critical linguistics. In CALDAS-COULTHARD, C. R., COULTHARD, M. *Text and Practices: Readings in Critical Discourse Analysis.* London: Routledge, 1996. s. 3 − 14. ISBN 0-415-12143-4.
[6] SEDLÁČKOVÁ, L. *Islám v médiích.* Liberec: Nakladatelství Bor, 2010. s. 13 − 16. ISBN 978-80-86807-65-2.
[7] VAN DIJK, T. Critical Discourse Analysis. In TANNEN, D., SCHIFFRIN, D., HAMILTON, H. *Handbook of Discourse Analysis.* Oxford: Blackwell, 2001. s. 355. ISBN 0-631-20595-0.

kulturních, politických či sociálních kontextů na diskurz, tak vliv diskurzu zpět na tyto kontexty.

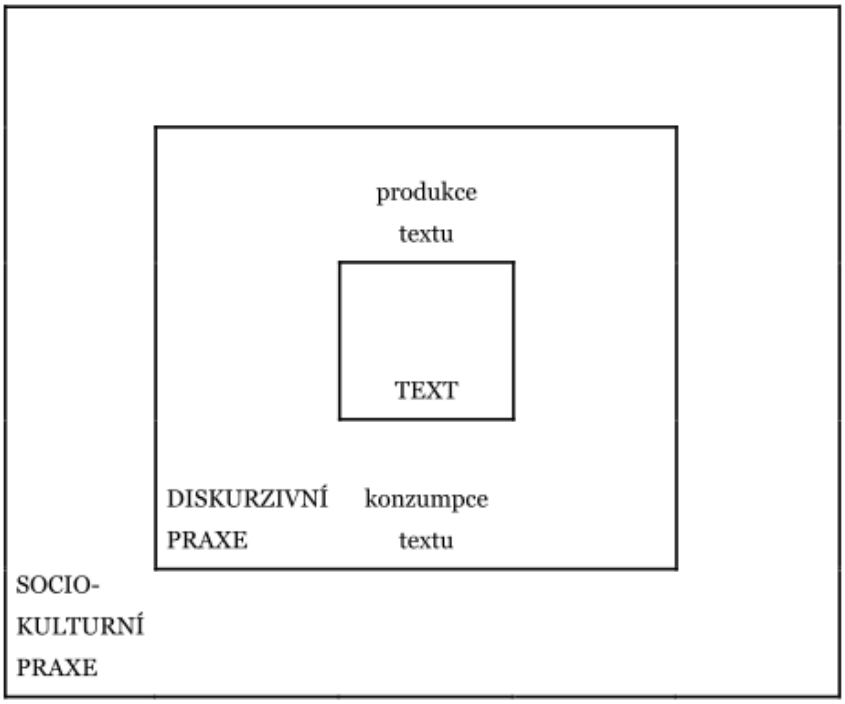
- **Historický směr.** Hlavní představitelkou tohoto směru je Ruth Wodaková. Její nejdůležitější práce se zabývají antisemitismem, rasismem či genderem. Důraz klade na studium historického kontextu diskurzu, soustředí se na zkoumání ideologie, mocenských vztahů, stereotypů a výsledky svých výzkumů se snaží využít v praxi.
- **Společensko-kulturní změny**. Jejich analýzou se zabývá Norman Fairclough. Jedná se o analýzu vztahů mezi proměnami diskurzu, zkoumá úlohu jazyka v procesu sociálních změn, například globalizace či neoliberalismus. Fairclough uvádí, že diskurz je součástí sociální praxe a jeho proměny mají přímou souvislost se společenskými změnami.[8]

Vymezení pojmu – Kritická analýza diskurzu

Nyní se pokusím o načrtnutí možných hranic pojmu Kritická analýza diskurzu (CDA). Pojem diskurz je velmi nejednoznačný a užívá se v mnoha významech. Jednotliví autoři definují tento pojem takto: Wodaková je považuje za soubor jazykových jednání projevujících se napříč sociálními oblastmi jako tematicky spojené psané či mluvené projevy, jež patří k určitému žánru.[9] Podle Faircloughа je tento pojem vymezen jako užití jazyka. Jedná se o nepsaná pravidla, jež kontrolují, co může či nemůže být řečeno a jak. Diskurz tedy v jeho pojetí představuje formu či aspekt sociální praxe.[10] Ve svých pozdějších pracech Fairclough mění pojem diskurz na semiosis, jehož roli vytyčuje ve třech různých sférách: 1) jako část sociální aktivity v rámci praxe, jež konstituuje tzv. žánry, 2) jako způsob bytí, jež konstituuje rozličné styly, například styl celebrity či politika apod., 3) jako reprezentace, jež dává vzniknout tzv. diskurzům.[11] Trojdimenzionální diskurz – viz obrázek níže je v dialektickém vztahu se sociálními strukturami. Diskurz je řízen tzv. pravidly diskurzu, která ovlivňují sociální pravidla (v tomto smyslu jsou pravidla mediátorem mezi textem a společností).

[8] FAIRCLOUGH, N. *Critical Discourse Analysis.* London: Longman, 1995. s. 7. ISBN 0-582-21984-1.
[9] WODAK, R. The discourse-historical approach. In WODAK, R., MEYER, M. *Methods of Critigal Discource Analysis.* London: Sage, 2001. s. 66. ISBN 0-7619-6154-2.
[10] FAIRCLOUGH, N. *Critical Discourse Analysis.* London: Longman, 1995. s. 65. ISBN 0-582-21984-1.
[11] FAIRCLOUGH, N. *Critical discourse analysis. Marges Linquistiques* [online] [cit. 2013-06-13]. Dostupné na www: <http://www.ling.lancs.ac.uk/profiles/236/>.

Obrázek 1: Trojdimenzionální model diskurzu podle Faircloughа



Zdroj: FAIRCLOUGH, N. *Media discourse.* London: Esward Arnold, 1995.

Van Dijk považuje diskurz za specifickou psanou nebo mluvenou komunikační událost. Zahrnuje zde i nonverbální vyjádřování, například obrazy, gesta apod. Odkazuje diskurz k souboru diskurzivních žánrů, které mohou být například politické či rasistické.[12]

Český zástupce diskurzní analýzy Jiří Homoláč hovoří o diskurzu jako o *„... užívání jazyka, event. dalších znakových systémů – členy dané společnosti, resp. jejich jistou skupinou (teoreticky i jednotlivce) a/nebo v určité oblasti společenského života a/nebo v komunikaci o určitém tématu“*[13].

V nejširsím pojetí zahrnuje pojem diskurz sdělení – text, autora, adresáta a situační kontext. Lze ho tedy chápat jako soubor výpovědí, které mají společnou vlastnost, nebo jako jednotlivou výpověď. Zkoumaný diskurz může být buď nonverbální (gesta apod.) nebo verbální (mluvený či psaný).[14]

Pojem kritický je používán v širším pojetí a označuje společenskou angažovanost neboli kritiku stávajícího stavu a snahu jej změnit. Wodaková označuje kritičnost jako zpochyňování toho, co je považováno za samozřejmé, kritiku dichotomického myšlení

[12] VAN DIJK, T. *Discourse and Racism* [online] [cit. 2013-06-13]. Dostupné na www: <http://www.discourses.org//OldArticles/Discourse%20and%20racism.pdf>.
[13] HOMOLÁČ. J. Diskurz o migraci Romů na příkladu internetových diskusí. *Sociologický časopis*, 2006, roč. 42, č. 2, s. 329.
[14] SEDLÁČKOVÁ, L. *Islám v médiích.* Liberec: Nakladatelství Bor, 2010. s. 17. ISBN 978-80-86807-65-2.

a dogmatismu a ozřejmování nejasných struktur mocenských vztahů.[15] Mocenské vztahy jsou považované autory za normální či přirozené. O kritickém myšlení o jazyce mluvíme jako o odcizení nebo odstupu. Jazyk tedy neodráží realitu tak, jak je, ale odráží jednání mluvčího. Příkladem může být označení demonstrantů – militantními muslimy, jak je označila Mladá fronta Dnes na své titulní straně dne 4. 2. 2006 (V indonéské Jakartě vzalo zhruba 300 militantních muslimů útokem dánskou ambasádu), jiné zpravodajství je pojmenovalo jako lid. Jde tedy o pojmenování neboli označení té samé skutečnosti jinými slovy, které dávají zcela jiný význam a tím matou veřejnost.

CDA se se podle Charlese Antakiho, kerý je čelní zástupce konverzační analýzy zaměřuje více na kategorie užívané v rámci diskurzu a klade růraz na teorie a jejich klíčovou úlohu ještě před samotnou analýzou dat.[16] Můžeme odlišit dva významy, které nesou označení CDA, a to dle Normana Faircloughа, který udává, že je to specifická medota, jíž je autorem a nebo jako širší hnutí v rámci diskurzivní analýzy sdružující několik rozdílných přístupů – viz čtyři přístupy kapitole Vznik a vývoj kritické analýzy diskurzu.

Cíle, metody a slabiny CDA

Cílem CDA je osvěta a emancipace, tedy denaturalizace ideologických poselství v různých textech a zpochybňování toho, co je považováno za samozřejmé. Primárním cílem odkrytí ideologických mechanismů je využít je v praxi, neboli snažit se stávající praxi změnit k lepšímu. CDA tedy pouze nekritizuje, ale upozorňuje na to, aby byly její závěry využity v praxi.[17]

CDA je kvalitativní metodou, ale může být zkombinována s metodami kvantitativními. Nemá však jednotný teoretický rámec ani metodologii. Předměty výzkumu se zcela liší, může se jednat o problematiku rasismu, genderu, terorismu, mediálního diskurzu atd. Analyzují se jak rozsáhlá data, tak i malé reprezentativní vzorky textů. Sbírají se různá data, mezi tím se hledají ukazatelé určitých konceptů a utvářejí

[15] WODAK, R. *What Is Critical Discourse Analysis?* [online] [cit. 2013-06-13]. Dostupné na www: <http://www.qualitative-research.net/index.php/fqs/article/view/255/562>.
[16] ANTAKI, Ch. *Analysing Talk and Text. A Course for the Universidad Autónoma de Barcelona* [online] [cit. 2013-06-13]. Dostupné na www: <http://www.staff.lboro.ac.uk/~ssca1/tthome.htm>.
[17] SEDLÁČKOVÁ, L. *Islám v médiích.* Liberec: Nakladatelství Bor, 2010. s. 20. ISBN 978-80-86807-65-2.

kategorie. Charakteristickým znakem CDA je neustálé přecházení mezi textovou analýzou, sběrem dat a teorií.[18]

Fairclough rozděluje CDA do tří samostatných metodologických postupů:[19]

- **Deskripce.** Zabývá se formální stránkou textu zkoumající slovní zásobu, gramatiku, tón, direktivu řeči apod. Fairclough v rámci této analýzy rozšlišuje tři tématické bloky – slovní zásobu, gramatiku a strukturu textu. V každém z těchto bloků se zvláště zaměřuje na zkušenostní hodnoty slov, hodnotu gramatiky, spojení vět, interakční konvence a strukturu textu. Není nutné, aby se analytik zabýval všemi aspekty deskripce najednou, jelikož vše je závislé na konkrétní podobě textu, vzdělanosti analytika v lingvistice a jeho citlivosti.
- **Interpretace.** Znamená co a jak je skrze texty produkováno a co a jak je v textech nacházeno. Analytik se snaží interpetovat různé diskurzivní typy, jež jsou spojeny s určitými typy situací a způsob, jakým ovlivňují ideje, subjekty a vzájemné vztahy. Dle Faircloughа jde o zaměření na to, o co jde, o koho jde a na vztahy mezi subjekty a spojení a to tak, aby bylo možno vypovídat o interpretacích, jež aktéři vztahují k danému situačnímu kontextu, o diskurzivním typu, diferencích a změnách. Analytik hledá spojitost mezi jednotlivými texty a zkoumá, jak jsou různé diskurzy a žánry artikulovány dohromady.
- **Explanace.** Tato se zabývá sociální determinací procesu produkce a interpretace a jeho sociálními efekty: *„Explanace je způsob, jak nahlédnout diskurz jako součást procesu sociálních bojů v rámci mocenských vztahů“*[20]**.** Dle Faircloughа se snažíme najít sociální determinanty, ideologie a efekty, tzn. zda diskurz udržuje nebo transformuje mocenské vztahy.

Kritici se shodují na největší slabině CDA, která je v širším kontextu užívaném k interpretaci textu. Tato kritika je oprávněná, neboť na analytika je kladeno mnoho nároků spočívajících ve znalosti kontextu, jež může zahrnovat mnoho jiných oborů (politologii, sociologii, historii, psychologii aj.). Van Dijk a Wodaková nachází řešení ve spolupráci více odborníků se vzděláním v jiných oborech. Dalším slabým místem je pracnost, neboť analýza velkého množství textů zabere mnoho času a to jak analytikovi, tak čtenáři. Z tohoto důvodu je mediální diskurz ve většině případů realizován na reprezentativních

[18] MEYER, M. Between theory, method, and politics: positioning of the aproaches to CDA. In Wodak, R. MEYER, M. *Methods of Critical Discourse Analysis.* London: Sage, 2001. s. 19. ISBN 0-7619-6154-2.
[19] VAŠÁT, P. *Kritická diskurzivní analýza: sociální konstruktivismus v praxi* [online] [cit. 2013-06-13]. Dostupné na www: <http://www.caat.cz>.
[20] FAIRCLOUGH, N. *Language and Power.* London: Longman Inc., 1989. ISBN 0-582-41483-0.

vzorcích textu. Je vhodné se spíše smířit s analýzou menšího množství textu a vypracovat tak důkladnou analýzu. Mezi další slabiny patří čtenář. Ten může mít o diskurzu znalosti již před samotným čtením textu a tak může měnit významy, jež nejsou ve shodě s ideologií textu.[21]

Analýza by se tedy měla držet několika jednoduchých pravidel, a to spolehlivosti – aby byla postavena na základě více lingvistických znaků, komplexnosti – na důsledném propojení lingvistických znaků s intertextuálními a na transparentnosti výsledků, které by měly být dokládány formou pasáží z textu, jež k výsledkům odkazují. Je potřeba se vyhnout těmto nedostatkům diskurzivních analýz: analýze shrnutí nějakého textu, analýze skrze vyjádření svého stanoviska k textu, analýze založené na identifikaci diskurzů a různých mentálních konstrukcí, analýze skrze nezakotvené citace, analýze provedené skrze špatný výzkum a analýze soustředěné pouze na lingvistické znaky.[22]

2.2.2. Bezpečnostní analýza a sekuritizace

Tradiční bezpečnostní analýza vycházela ze státocentrického pojetí a zaobírala se pouze tématy souvisejícími s činností armád a států. Po rozpadu bipolárního systému se do oblasti bezpečnosti dostává širší pole témat a referenčních objektů. Analýzy zabývající se čistě vojenským ohrožením a ohrožením států se stávají tématem strategických studií, jež jsou podoborem v rámci bezpečnostních studií.

„Bezpečnostní politika je chápána jako širší rámec všech aktivit, jejichž cílem je zabezpečení chráněné hodnoty – referenčního objektu, a to i vůči hrozbám, které mají zcela nevojenský charakter a protiopatření vůči nim spadají do kompetencí nevojenských složek státu či dokonce do oblasti spolupráce s civilním nevládním sektorem.“[23]

Tímto dochází k rozšíření pojmu bezpečnosti také na témata ekonomická, societární, což koresponduje s referenčními objekty ohroženými kybernetickými útoky.

[21] SEDLÁČKOVÁ, L. *Islám v médiích.* Liberec: Nakladatelství Bor, 2010. s. 21 − 23. ISBN 978-80-86807-65-2.
[22] VAŠÁT, P. *Kritická diskurzivní analýza: sociální konstruktivismus v praxi* [online] [cit. 2013-06-13]. Dostupné na: <http://www.caat.cz>.
[23] FRANK, L. *Analýza a predikce bezpečnostních hrozeb a rizik v České republice* [online] 2006 [cit. 2011-01-05]. Dostupné na www: <http://is.muni.cz/th/16735/fss_d/disertace_frank.pdf>.

Jednotky bezpečnostní analýzy

V rámci bezpečnostní analýzy můžeme dle autorů identifikovat tři typy jednotek.

1. **Referenční objekty:** objekty, jež jsou existenčně ohroženy a můžou legitimně nárokovat právo na přežití.
2. **Aktéři sekuritizace:** aktéři, kteří prohlašují něco – referenční objekty – za existenčně ohrožené a jsou tedy hybateli procesu sekuritizace.
3. **Funkcionální aktéři:** tito aktéři působí na dynamiku bezpečnostních vztahů v sektoru. Významně ovlivňují politická rozhodnutí na poli bezpečnosti, aniž by se přímo jednalo o referenční objekty nebo o aktéry poukazující na nutnost bezpečnostních kroků ve vztahu k referenčnímu objektu.

Sekuritizace

Důležitým pojmem v rámci bezpečnostní analýzy je pojem sekuritizace. *„Krokem, jímž se politika dostává mimo zavedená pravidla hry a který rámuje určité téma buď jako zvláštní druh politiky, nebo jako záležitost stojící „nad" standardním politickým jednáním, je právě pojem „bezpečnost". Sekuritizaci (securitization) lze tedy považovat za radikálnější verzi politizace."*[24]

Ze spojení politizace se sekuritizací, však nemůžeme vyvozovat, že sekuritizaci tématu může provádět pouze stát, nýbrž tento proces můžou iniciovat také nestátní subjekty. Zde je důležité poznamenat, že sekuritizace není založena na reálné existenci hrozby, nýbrž na samotném tvrzení, že se o hrozbu jedná, které je akceptováno. Bezpečnostním tématem se daná hrozba stává pokud je možno argumentovat ve prospěch přiřazení priority tomuto tématu. *„"Bezpečnost" tedy představuje autoreferenční druh jednání."*[25] Vytvoření bezpečnostního diskurzu neznamená, že proběhla úspěšná sekuritizace. Dle autorů se jedná pouze o tzv. sekuritizační krok, který vyžaduje akceptaci veřejnosti.

[24] BUZAN, B., WAEVER, O., DE WILDE, J.. *Bezpečnost: Nový rámec pro analýzu*. 1. vyd. Brno: Barrister & Principal, 2005. s. 34. ISBN 80-903333-6-2.
[25] Tamtéž, s. 35.

Klíčovým bodem nového rámce bezpečnostní analýzy je rozlišení mezi objektivním (hrozba existuje) a subjektivním (hrozba je jako taková vnímána) přístupem. *„Jsme přesvědčeni, že sekuritizaci je nutné chápat jako ve své podstatě intersubjektivní proces.“*[26]

Jedná se o to, že ve chvíli, kdy dochází k sekuritizaci jsou legitimizovány prostředky k jejímu zvládnutí, jež se vymykají standartním politickým řešením. Intersubjektivní přístup znamená, že bezpečnostní prostředí je tvořeno samotnými aktéry bezpečnostního prostředí *„… jedná se o součást diskursivního a sociálně konstruovaného světa“*[27]. Vztah mezi těmito aktéry je pochopitelně asymetrický a úspěšná sekuritizace závisí na společenském postavení aktéra.

2.3. Cíl práce

Cílem práce je zjistit, zda skutečně mohou mít teroristické útoky provedené v kyberprostoru stejně zničující dopad na společnost, jako útoky prováděné ve fyzickém prostoru s oběťmi na životech, čímž by se kyberterorismus z latentní hrozby stal nejzávažnějším bezpečnostním tématem dnešní společnosti.

Druhým cílem je dokázat, že mediální diskurz se výrazně podílí na zavedení pojmu kybernetického terorismu do bezpečnostního diskurzu a tvorbou vlastních verzí reality.

[26] BUZAN, B., WAEVER, O., DE WILDE, J.. *Bezpečnost: Nový rámec pro analýzu*. 1. vyd. Brno: Barrister & Principal, 2005. s. 41. ISBN 80-903333-6-2.
[27] Tamtéž, s. 43

3. Terorismus

Již od pradávna doprovází lidské společenství násilí. Pokud se jedna strana domnívala, že k povolení druhé strany je potřeba strachu, neváhala jej využít. Násilí má nekonečně mnoho podob a variant, ale tou nejnebezpečnější formou je terorismus.

3.1. Vymezení pojmu

Slovo teror je odvozeno z latinského slova *terrere*, v českém překladu znamenající hrozný, strašný nebo vyděsit, postrašit. Pojem teror se od pojmu terorismus odlišuje absencí politických cílů a zaměřením proti konkrétním osobám. Samotné definování pojmu terorismus je velmi obtížné. Obecně hovoříme o jakémkoliv použití organizovaného násilí zaměřeného proti nezúčastněným osobám k dosažení politických, kriminálních nebo jiných cílů. Do moderních slovníků se dostal až díky francouzskému jazyku během 14. století. V angličtině byl poprvé zaznamenán v roce 1528. Čínský filosof a vojevůdce Sun Tsu vidí základ teroru ve starém čínském přísloví: *„Zabij jednoho a postrašíš deset tisíc.“*[28]

Definic terorismu existuje skutečně nepřeberné množství, například Alex P. Schmid zjistil, že od roku 1936 do roku 1981 se jich v literatuře objevilo celkem 109. Nyní bych chtěl uvést některé ze soudobých definic:[29]

- *„Terorismus je propočítané použití násilí nebo hrozby násilím, obykle zaměřené proti nezúčastněným osobám, s cílem vyvolat strach, jehož prostřednictvím jsou dosahovány politické, náboženské nebo ideologické cíle. Terorismus zahrnuje i kriminální zločiny, jež jsou ve své podstatě symbolické a jsou cestou k dosažení jiných cílů, než na které je kriminální čin zaměřen.“* (USA, 1980)
- *„Terorismus je úmyslným užitím nebo hrozbou užití násilí proti civilistům nebo civilním cílům, za účelem dosažení politických záměrů“* [30]. Dle B. Ganora obsahuje systematizace terorismu tři prvky, a to *„násilný aktivismus, s politickým záměrem a zacílený na civilní cíle (tj. osoby či objekty)“* [31].

---

[28] *Encyklopedie Světový terorismus od starověku až po útok na USA.* 1. vyd. Praha: Svojtka & Co., 2001. s. 10. ISBN 80-7237-340-4.
[29] MIKA, O. *Současný terorismus.* Praha: Nakladatelství Triton, 2003. s. 10−13. ISBN: 80-7254-409-8.
[30] GANOR, B. Defining Terrorism: Is One Man´s Terrorist Another Man´s Freedom Fighter?, ICT − *International Institute for Counter-Terrorism* [online] 1998. Dostupné z www: <http://www.ict.org.il/ResearchPublications/tabid/64/Articlsid/432/Default.aspx>.
[31] Tamtéž

- *„Terorismus je politicky motivované násilí, páchané jednotlivci, skupinami nebo státy, s úmyslem roznítit v populaci pocity strachu a bezmoci za účelem ovlivnit procesy rozhodování a změnit chování.“* [32]
- *„Souhrn antihumánních metod hrubého zastrašování politických odpůrců hrozbou síly a užití různých forem násilí. Vedle individuálního terorismu existuje terorismus skupin, některé koordinují svoji činnost na mezinárodní úrovni (mezinárodní terorismus).”* (Český encyklopedický slovník, 1993)
- *„Terorismus – v politice používání teroristických prostředků k zastrašování politických odpůrců a ovlivňování veřejného mínění. Cílem terorismu je obvykle vyvíjení extrémního psychického nátlaku na jednotlivce nebo častěji na celé skupiny obyvatelstva...”* (Encyklopedie politiky, 1999)
- *„Terorismus, politické násilí zaměřené na vládu, ale často ohrožující i řadové občany. Jeho cílem je vytvořit atmosféru strachu, v níž by vláda splnila požadavky teroristů...”* (Blackwellova encyklopedie politického myšlení, 2000)
- *„V současnosti se za terorismus označují takové akty teroru, které vycházejí od vládních protivníků. Rozsah činností, jež tento termín zahrnuje, je velmi široký, můžeme však vyjmenovat čtyři hlavní formy: úkladné vraždy a atentáty, bombové útoky, držení jednotlivců jako rukojmí a v nedávné době také únosy letadel...”* (Oxfordský slovník světové politiky, 2000)
- *„Terorismus je ekvivalentem válečných zločinů v období míru.”* (Encyklopedie světového terorismu, 2001).
- *„Společně s organizovaným zločinem a šířením zbraní hromadného ničení patří terorismus – zejména jeho mezinárodní forma – k nejzávažnějším rizikům ohrožujícím celou lidskou civilizaci. Globálnost tohoto nebezpečí potvrzuje fakt, že podstatná část světa byla zasažena nebo je ohrožena terorismem politického a náboženského charakteru, akcemi regionálních či nadnárodních teroristických a extremistických organizací a skupin. Bez ohledu na mimořádné úsilí bezpečnostních složek všech demokratických států mezinárodní terorismus eliminovat se s jeho aktivitami každoročně setkává kolem padesáti až šedesáti zemí. Téměř nic neřeší zpřísnění tresů. Mezinárodní teroristé – k jejichž požadavkům patří změna vnitřní a zahraniční politiky, změna právního systému, propuštění vězněných teroristů či zaplacení výkupného a umožnění bezpečného úniku – jsou*

[32] MOGHADDAM, F. The Staircase to Terrorism: A Psychological Exploration, In *American Psychologist*, 2005, roč. 60, č. 2, s. 161 – 169. ISSN 0003-066X.

odhodláni ke všemu, nedají se zastrašit, častou jsou připraveni zemřít při sebevražedném útoku. Zastavení připravené akce je proto nesmírně obtížné a stejně obtížná je i jakákoliv prevence." (Bezpečnostní informační služba České republiky, www.bis.cz)

Jednotlivé definice pojmu terorismus se různí a vyvíjí v čase, například na počátku byly za teroristické činy označovány i činy kriminální, které neměly za úkol žádný politický cíl ani zastrašení protivníků. V každém případě můžeme ve všech současných definicích nalézt shodu v tom, že se jedná o útok vedený proti civilistům, jinými slovy, nebojovým cílům za účelem dosažení politického cíle. Značně rozdílný výklad se u řady autorů vyskytuje i u pojmu terorista. Jednou je nazýván teroristou příslušník bojového hnutí, v dalším případě je označen za bojovníka za svobodu. Zákonná definice terorismu Alexe P. Schmida *„Terorismus je ekvivalentem válečných zločinů v období míru."*[33] se jeví jako tou nejvhodnější z hlediska ujednocení postupů při zacházení s teroristy a to také z toho důvodu, že vylučuje některé formy násilí, které v současnosti vlády některých států označují slovem terorismus. Pokud by se stalo, že mezinárodní společenství takovouto definici přijme, nemůže již nikdo moci vydávat teroristy za bojovníky za svobodu.

Světová encyklopedie terorismu uvádí, že je nezaujatost rozhovorů na toto téma poskvrněna vztahem zúčastněných k teroristickým útokům. Existují tak čtyři skupiny, které se liší svými názory a chápáním:[34]

- **Vědečtí odborníci** – hledají obecný pojem, debatují, aniž by se obávali bezprostředního útoku na své osoby.
- **Vládní autority** – hrozby a útoky se jich přímo dotýkají a poznamenávají je.
- **Veřejnost** – často mění své postoje, jejich názor je ve velké míře ovlivňován médii.
- **Názory teroristů a jejich sympatizantů** – věří a jsou přesvědčeni, že žijí pod špatnou nadvládou, a tak svými činy toto jednání ospravedlňují. Cílem teroristů je dle Eichlera[35] přilákat pozornost, vyvolat atmosféru strachu, destabilizovat stát a vyprovokovat jej k tvrdé odvetě či vynutit si změnu vnitřní nebo zahraniční politiky. Z hlediska této práce je, dle mého názoru, nejdůležitější cílená snaha o vynucení změny vnitřní nebo zahraniční politiky.

[33] *Encyklopedie Světový terorismus od starověku až po útok na USA.* 1. vyd. Praha: Svojtka & Co., 2001. s. 12. ISBN 80-7237-340-4.
[34] Tamtéž, s. 10 − 20.
[35] EICHLER, J. *Terorismus a války na počátku 21. století.* Praha: Karolinum, 2007. s. 147. ISBN 978-80-246-1317-8.

Každý jedinec má tedy k pojmu terorismus jiný vztah. I z tohoto důvodu jsou odborníci skeptičtí k vytvoření univerzální poučky. Aby bylo možné lépe pochopit původ slova teror či terorismus, je třeba nahlédnout do historie.

3.2. Historické kořeny

Pokud se podíváme do historie, tak zcela jasný politický význam získal pojem terorismus již za francouzské buržoazní revoluce. Teror, který byl původně zamýšlen jako nástroj na potlačení aristokracie a monarchie, se nakonec obrátil i proti příznivcům revoluce a republiky. Kořeny terorismu však sahají ještě dále do starého Řecka a Říma.

3.2.1. Teror ve středověku do roku 1789[36]

Historické prameny včetně Bible uvádějí mnoho příkladů, kdy bylo použito násilí pro dosažení určitého cíle. Již ve středověku bylo učiněno několik politických vražd, které by se daly svým způsobem zařadit mezi jisté formy teroru. Ve starém Řecku byl tyranem nazýván vládce, který se chopil násilím vlády, aniž by mě plnou podporu obyvatelstva, například případ bratří Hipparcha a Hippiase.

Vznik Římské republiky předznamenávaly konflikty mezi aristokraty, její ustanovení tak mělo zabránit krveprolití mezi nevyšší vrstvou společnosti. Římané vedli války z důvodu rozšíření své země. Poté, co daná území získali, dali obyvatelům na výběr – buď se za určitých podmínek podřídí, nebo v zemi vypukne teror. Většinou však vyvraždili veškeré obyvatelstvo, jako například roku 70 n. l. v Jeruzalémě. Teror taktéž prosazovali za účelem udržení kázně ve své armádě či proti revoltám v samotném Římě. Když například vojenská jednotka neprokázala dost statečnosti, byl popraven každý 10 muž v armádě. Modernímu terorismu se nejvíce přibližují vražedné atentáty v římském císařství. Dá se říci, že Římané bezesporu častokrát využili teroru k zastašení či prosazení svého záměru.

Výňatky ze středověké literatury poukazují na to, že při vedení válek se teror běžně používal k zastrašování poražených. Jejich domy byly vždy vydrancovány, zajatci prodáni do otroctví a vůdcové poražené strany mohli v tom lepším případě očekávat rychlou smrt. Ve druhé polovině středověku, od 11. do 16. století, začalo docházet ke změně názorů

[36] *Encyklopedie Světový terorismus od starověku až po útok na USA.* 1. vyd. Praha: Svojtka & Co., 2001. s. 27 − 43. ISBN 80-7237-340-4.

na vedení války. Středověké nájezdy tak směřovaly spíše ke drancování, než k teroru na obyvatelstvu. Stále však platilo, že stupeň uplatňovaného teroru závisel na tom, z jaké sociální vrstvy jedinec pocházel. Takže teror i nadále zůstával nástrojem k udržení sociálního pořádku ve středověkém světě, ale z hlediska našeho pohledu bychom toto jednání zařadili pod pojem warfare.

Od 11. do 13. století se v Perském zálivu vyvinula fanatická vražedná sekta muslimů zvaná Assasíni. Pouhá hrozba vyvražděním vždy přiměla jejich odpůrce k podrobení se. Sami sebe považovali za boží vyslance a aktem božím ospravedlňovali jakokouliv vraždu. Vrahům slibovali, že po návratu z akce jim bude povolen vstup do rajské zahrady a pokud zahynou při plnění úkolu, půjdou do rajské zahrady okamžitě. O této sektě se traduje, že fanatická odvaha vrahů byla zapříčiněna vlivem drog.

O největším a nemilosrdném teroru ve středověku se hovoří ve spojitosti s nájezdy mongolských hord pod vedením Čingischána, které si vyžádaly tisíce lidských životů. Vojenské úspěchy Čingischána, který chtěl dobýt celý svět, jsou připisovány dokonalé organizaci, taktice a strategii. Mongolové při svých nájezdech dávali lidem možnost výběru, buď budou kapitulovat nebo jim hrozí smrt. Velmi často však padlo veškeré obyvatelstvo, například po dobytí Herátu (dnes západní Afghánistán) vyvraždili celkem 2,4 miliou lidí, což se blíží počtu Židů povražděných nacisty v době holocaustu. Pokud obránci pevnosti odmítli nabídku na kapitulaci, museli počítat s tím, že si vítěz vezme nejen všechnen jejich majetek, ale i jejich životy.

Přesuneme-li se do Severní Ameriky, zde byly vztahy mezi domorodými indiány a osadníky vždy provázeny násilím. Zpočátku měly indiánské kmeny z kolonizátorů prospěch, neboť od nich získaly koně, ovce a další zboží. Poté však následoval teror, například v průběh koniálních válek v letech 1689−1760 používali Britové a Francouzi indiánské spojence k terorizování civilního obyvatelstva. Přeživší osadníci vykonali na indidánech neméně hrůznou odvetu, pobili indiány, zničili úrodu a vesnice. Bitvy nekončily normální porážkou, ale masakrem. Vzájemné terorizování bylo brutální a neslavné a trvalo do roku 1875, kdy vláda Spojených států donutila indiány žít ve vyhrazených rezervacích.

3.2.2. Teror v období od Velké francouzské revoluce do 2. světové války[37]

Teror ve formě zastrašování obyvatelstva je spojen s obdobím Velké francouzské revoluce. Pojem vešel v povědomí ve spojitosti s vládou teroru (1793−1794) uskutečňovanou Výbory pro veřejné blaho a obecnou společnost v čele s diktátorem Maximilienem Robespierrem, který plnil příkazy národního Konventu. Metody teroru, používané za vlády teroru, zahrnovaly sledování lidí a jejich názorů, žalář nebo vyhnanství, a to jak proti rebelům, tak proti vlastním revolucionářům. Výbor však nebyl jediným, kdo ve Francii vládl terorem. Byla jím Státní bezpečnost, politická policie a kontrašpionáž v rukou Výboru všeobecné bezpečnosti. Revoluční tribunál nechal jen v Paříži popravit na 3000 osob, po celé zemi v žalářích umíralo 12 tisíc lidí. Celkové číslo politických vězňů dosáhlo půl milionu lidí. V oblastech, kde zuřila občanská válka se odhadují oběti na 30 − 40 tisíc.

Po svržení Robespierra a jeho přívrženců 27. července 1794 omezil národní Konvent pracovmoci Výboru veřejného blaha, odvolal komisaře Konventu z provincií, osvobodil stovky politických vězňů, rozpustil lidové spolky, atd. O rok později nahradil národní Konvent direktoriát. V této době se spustila vlna bílého teroru – oběti začaly napadat a vraždit bývalé vykonavatele revolučního teroru. Po nástupu Napoleona k moci roku 1799 se rozšířila další metoda teroru, a to státem organizované vraždy politických protivníků.

Téměř po 80 letech od Robespierrovy vlády teroru se v Paříži rozšířily násilnosti. Po porážce s Pruskem v roce 1871 se pracující třída vzbouřila proti nové francouzské vládě, která uprchla do Versailles. Dne 28. března bylo před pařížským davem ustanovena Pařížská komuna. O pět dní později však vypukla občanská válka. V zemi opět panovalo násilií a teror. Vláda byla odtržena od reality v Paříži a občané vládu ignorovali. Nikdo vlastně nevěděl, kdo vládne. Při zpětném dobývání Paříže se dopouštěly teroru i vládní jednotky, které postřílely až 25 tisíc obyvatel z dělnických čtvrtí. Pařížští radikálové vedli v období let 1789−1871 čtyři revoluce. Po dozdrcení Komuny nedošlo v Paříži k nepokojům až do roku 1968.

Pojem anarchismus si ve zmatku po francouzské revoluci vysloužil synonymum pro chaos, revoluční teror a politické vraždění. Anarchisté hlásali, že se jedná o svobodnou společnost svobodných lidí obsahující revoluční dobrovolné aktivity. Ty byly založeny na existenci dřímající revoluční energie lidu. Tuto energii bylo nutno probudit, a to buď

[37] *Encyklopedie Světový terorismus od starověku až po útok na USA.* 1. vyd. Praha: Svojtka & Co., 2001. s. 44 − 73. ISBN 80-7237-340-4.

propagandou nebo terorem. Ruští anarchisté čítali cca 500 osob a zahájili svou činnost v polovině 19. století. Jejich vůdčí osobností byl Michail Bakunin. Podle jeho učení každá forma autority zotročovala velkou většinu lidu, hlásal proto, že pro osvobození je nutné osovobození existující společnosti. Venkovské masy však zůstaly vůči nespravedllnostem carského režimu netečné. Anarchistům nezbylo nic než pokračovat a doufat, že masy rolníků se k nim časem připojí. Na podzim roku 1879 přijala zbylá menšina narchistů název Vůle lidu. Jejím hlavním úkolem byla vražda vládních činitelů a také cara. Skupina ve svém úkolu třikrát uspěla a i přes uvěznení svých vůdčích osobnosti se jí povedlo uskutečnit atentát na cara Alexandra II. Rolníci se však k protestům přesto nepřidali, střední vrstvy byly naplněny hrůzou a radikálové ztratili podporu. Anarchismus se v této podobě minul účinkem.

Zřejmě nejvýznamnějším teroristickým činem počátku 20. stol. byl atentát na arcivévodu Františka Ferdinanda d´Este, který se stal terčem extremistických nacionalistických organizací na Balkáně. Měl tak dalekosáhlé následky, jejichž výsledkem se stalo vypuknutí 1. světové války (1914−1918). Útok provedla skupina Černá ruka, která podporovala řadu teroristických skupin v Makedonii a Bosně. Pod vedením Dragutina Dimitrijeviče, který měl také vedoucí úlohu v atentátu na cara Alexandra, zintenzivnila Černá ruka své teroristické akce, které se soustředily na vládní budovy v Bosně. Pro Srby byl den atentátu – 28. června 1941 dnem národního smutku, jelikož si připomínali 525. výročí prohrané bitvy u Kosova, která přivodila pád středověké srbské říše. Rakouská odveta přišla velmi brzy. Všichni spiklenci byli uvězněni, ale k odhalení spojitosti s Černou rukou a Dimitrijevičem došlo až v roce 1918. První světová válka vypukla přesně pět týdnů po teroristickém útoku.

Počátek první světové války byl poznamenán uplatňováním politiky teroru, tedy udržováním protivníka v děsu, tzv. Schrecklichkeit. Německá armáda brala jako rukojmí místní obyvatelstvo ve Francii a Belgii, které popravovala jako odpověď na aktivity partyzánů. Chtěla tímto přinutit vystrašené obyvatelstvo k poslušnosti. Další vlnou teroru proti civilistům bylo vyhlášení totální ponorkové války. Po rozkaze útočit na všechny lodě, které vplují do nepřátelských vod, zahynulo v květnu 1915 až 1400 lidí z osobní lodi Lusitania.

V době, kdy v Evropě zuřila 1. světová válka, nacionalistické hnutí v Irsku roku 1916 vyvolalo velikonoční nepokoje za účelem vyhlášení Irské republiky. Britové vyslali na Irsko vojsko a povstání potlačili s takovou brutalitou, že se z popravených rebelů stali mečedníci a z velikončního povstání legenda. Propast mezi Iry a Brity se ještě více

prohloubila. Hnutí odporu tak dostalo novou podobu ve formě zrození Irské republikánské armády (IRA). V roce 1920 dosáhl konflikt svého vrcholu, když IRA denně vraždila policisty a prováděla pumové atentáty na veřejné budovy. IRA předznamenala prvky moderního terorismu, a to mučednictví, špionáž, pašování zbraní, směs politiky, teroru a propagandy, vojenské taktiky a metody atd.

Občanské války v Rusku a Finsku se také nevyhly vlně teroru. Rudý teror v letech 1917−1921 využíval k potlačení svých protivníků koncentračních táborů, braní rukojmí či poprav bez soudů a připravil o život od 50 do 250 tisíc lidí. Jeho kořeny vycházely z třídní nenávisti bolševiků, kteří by bez používání metod teroru nikdy nedokázali udržet svůj menšinový režim. Socialističtí revolucionáři toužili po odstranění Lenina a tak upřednostňovali akty individuálního teroru tzv. Bílého teroru. Finská občanská válka, v níž proti sobě bojovaly bílé a rudé gardy, trvala pouhé 4 měsíce, ale byla velmi krvavá. Ze 3 milionů obyvatel zahynulo 30 tisíc obyvatel.

Nástrojů státního terorismu hojně využíval v Sovětském svazu i Josef Stalin. Po nástupu bolševiků k moci převychovával Lenin třídní nepřátele nucenými pracemi. Od Leninovy smrti se stal diktátorem Stalin. Na následky nucených prací, poprav a hladomoru skonalo za komunistické vlády v Rusku na 20 milionů lidí.

3.2.3. Teror v období 2. světové války do roku 1945[38]

Velmi mnoho teroristických činů se odehrálo za 2. světové války, ale také v jiných zemích, například v Rumunsku, Norsku či Jugoslávii. Druhá světová válka se stala největším válečným konfliktem, který se odehrál v histori lidstva. V průběhu války docházelo na okupovaných územích k velkým ukrutnostem, intenzifikaci a systematizaci teroristických metod. Nejen, že zahynulo velké množství nevinných civilistů zvláště v bojích s partyzány, ale vojáci zacházeli špatně i s válečnými zajatci. V německém zajetí zahynulo více než 3,3 milionu ruských vojáků z celkového počtu 5,7 milionu válečných zajatců.

V rámci holocaustu využívali Nacisté metod teroru také ke korumpování lidí, kteří jej vykonávali, a to podněcováním sadistických metod a násilí. Rovněž vyhrožovali popravami a zařazením do transportu lidem, kteří Židům pomáhali.

[38] *Encyklopedie Světový terorismus od starověku až po útok na USA.* 1. vyd. Praha: Svojtka & Co., 2001. str.74 – 119. ISBN 80-7237-340-4.

Není možné se ovšem nezmínit o odvětě, která byla učiněna za atentát na říšského protektora Heydricha. Při ní byla zcela zničena česká vesnice Lidice, muži byli zavražděni na místě, ženy poslány do koncentračních táborů a děti poslány na převýchovu do Německa. Zemřelo tak 1300 lidí. Následně došlo i k vypálení obce Ležáky. Válka, která dala základy modernímu terorismu, skončila po vyčerpání a vysokých ztrátách na všech stranách 8. května 1945 kapitulací Německa.

Po skončení 2. světové války chtěli Spojenci potrestat válečné zločince za používání teroru jako nástroje státní politiky. Stalo se tak v norimberském a tokijském procesu, který byl vedený mezinárodním tribunálem pro válečné zločiny při OSN. Norimberský soud obvinil 22 německých vojenských vůdců, z nichž 12 bylo oběšeno, 7 dostalo trest odnětí svobody až po doživotí a 3 byli viny zproštěni. Mezinárodní vojenský tribunál pro Dálný východ obvinil 28 válečných zločinců z 55 zločinů proti lidskosti. Tři osoby zemřely v průběhu procesu, 16 jich bylo odsouzeno na doživotí, 7 bylo oběšeno a dva obdrželi krátký trest odnětí svobody.

3.2.4. Soudobý terorismus

„Soudobý terorismus je probíhající násilnou fází evoluce, jejíž počátky sahají stejně daleko jako lidské konflikty samotné." (Caleb Carr, Dějiny terorismu)

Moderní historie terorismu se začala psát v polovině minulého století. Od 2. světové války se začal terorismus rozvíjet ve větším měřítku, což úzce souvisí s regionálními i globálními problémy. Taktika, strategie a prostředky se přitom den ode dne stále více zdokonalují. Významnou roli zvláště v posledních letech hrají všechny druhy médií, které věnují zprávám o teroristických útocích mimořádnou pozornost, čímž vlastně nepřímo teroristický program či požadavky zveřejňují.

V 60. letech se k tradičním metodám, jež byly bombové útoky, úkladné vraždy, vydírání či braní rukojmí, přidaly také únosy letadel. O deset let později začala operovat řada teroristických organizací či skupin zvláště na území jiných států, než na kterých vznikly. Některé z nejznámějších nyní uvádím.[39]

Již v roce 1919 vznikla teroristická organizace IRA (Irská republikánská armáda), která se snažila bojovat proti přítomnosti Angličanů v Severním Irsku – viz předchozí

[39] MIKA, O. *Současný terorismus.* Praha: Nakladatelství Triton, 2003, 2003. s. 23 − 24. ISBN: 80-7254-409-8.

kapitola. V současné době je organizace rozdělena na dvě části – první z nich se snaží o dohodu politickou cestou, druhá pokračuje v extremistických útocích.

V roce 1958 vznikla v období krize tradičního baskického nacionalismu organizace ETA (Euskadi ta Askatasuna, což znamená Baskicko a jeho svoboda). Jejím cílem bylo vytvoření nezávislého baskického státu na severu Španělska. Organizace se však názorově rozdělila na dvě části – ETA-militar a ETA-político-militar. Členové první z nich dávali přednost ozbrojeným akcím, zatímco v té druhé usilovali o vytvoření politické shody. Počty teroristických útoků během posledních let klesají spolu s počty členů této organizace.

Libanonská šíitská militantní a politická skupina Hizballáh (Boží strana) působí od roku 1982. Hlavní myšlenkou skupiny je vytvořit v Libanonu teokratickou vládu jako v Iránu a poté ji rozšířit po celém arabském světě. Teroristické útoky skupina převážně vede proti Izraeli a jeho spojencům.

Další teroristickou organizací je palestinská islamistická militantní skupina Hamas (Hnutí islámského odboru), která vznikla v roce 1987. I tato organizace se rozdělila na militantní, která provádí teroristické útoky a na politickou, jejíž hlavním cílem je přijímání nových členů a finanční stránka.

Nejvíce známou teroristickou organizací, která je spojována zejména s útoky na USA, je Al-Káida. Vznikla přibližně v 80. letech minulého století, v době, kdy její vůdce Usáma bin Ládin začal formovat svou organizaci k odboji proti sovětské armádě. V roce 1979 Al-Káida vstoupila na území Afghánistánu s pomocí upadající komunistické menšině. Zde setrvala přes 9 let. Fakt, že SSSR v této válce neuspěl, jen posílil sebevědomí Al-Káidy a upevnil stabilitu válečníků ve jméno džihádu.

Teroristických útoků bylo do současnosti podniknuto velmi mnoho. Konají se převážně na veřejných místech, na nichž dochází k vysoké koncentraci osob, například ve stanicích metra, na letištích, autobusových a vlakových nádražích, sportovních stadionech, divadlech, marketech atd. Zmíním se však pouze o některých z nich, které znamenaly významný předěl v historii terorismu.

Otakar Míka ve své knize Současný terorismus uvádí: *„… chemický útok sarinem v tokijském metru, který si vyžádal 12 obětí na lidských životech, zranil více než 1000 osob, z čehož 17 bylo v kritickém stavu, 37 osob bylo vážně zdravotně postiženo a 984 bylo*

poškozeno lehce. Celkový počet oběží byl však podle japonské policejní zprávy 4460 osob"[40].

Další dva ničivé teroristickými útoky se staly v Moskvě a na Bali. V říjnu roku 2002 bylo zadržováno 50členným čečenským komandem asi 1000 diváků, kteří byli v té době v moskevském divadle. Celá teroristická skupina byla následně zlikvidována, ale za oběti padlo 130 diváků a zachranářů. Na podzim roku 2002 byl proveden výbuch v luxusním hotelu na Bali. Zemřelo 180 turistů, zejména z Austrálie.[41]

O dva roky později se dočkala i Evropa. V Madridu byly umístěny do vlakových souprav čtyři nálože a odpáleny byly v době ranní špičky. Obětí bylo 200, zraněných přes dva tisíce. V roce 2005 provedli teroristé sérii koordinovaných sebevražedných útoků v soupravách metra a v autobuse v Londýně. Zraněných osob bylo přes 700, útok si však vyžádal 52 mrtvých. V ruském Beslanu napadli čečenci budovu školy, ve které zahynulo přes 334 osob, z toho bylo 186 dětí.[42]

Tím nejzávažnějším však byl teroristický útok na budovy World Trade Center a Pentagonu v USA 11. září 2001. Únosci se zmocnili čtyř letadel. Dvě narazila do WTC, další letadlo do budovy Pentagonu a poslední, které mělo údajně za cíl Bílý dům, se zřítilo do polí v Pensylvánii. O život přišlo 3047 nevinných obětí[43]. Katastrofa, která neměla v té době ve světě většího rozsahu, iniciovala celosvětovou kampaň proti terorismu, do níž se zapojila i naše republika.

V současné době se za hlavní ohnisko teroristického nebezpečí považuje Pentagon, oblast Středního a Blízkého východu. Dalším centrem je Rusko, ve kterém velkou rychlostí narůstají teroristické aktivity a organizovaný zločin. Například v období od ledna do června 1995 zde bylo zaznamenáno více než 600 teroristických útoků. V České republice je situace v porovnání se sousedními státy klidná. Terorismus je u nás prezentován pouze v médiích. To však neznamená, že tento problém neexistuje a v budoucnu se nás nemůže týkat, například v podobě domácích extremistických organizací. I přes zkvalitnění bezpečnostní situace přijetím naší země do NATO bychom

[40] MIKA, O. *Současný terorismus.* Praha: Nakladatelství Triton, 2003, 2003. s. 17. ISBN: 80-7254-409-8.
[41] Tamtéž,. s. 18 − 19.
[42] FOLTIN, P., ŘEHÁK, D. *Důvody realizace a formy terorismu. Strategie a obrana* [online] 2005, č. 1 [cit. 2013-05-13]. Dostupné na www: <http://www.defenceandstrategy.eu/cs/archiv/rocnik-2005/1-2005/duvodyrealizace-a-formy-terorismu.html>.
[43] Údaje vychází z amerických zdrojů.

měli včas přijímat preventivní opatření a nezlehčovat nebezpečí terorismu. Velmi důležitá je osvěta a informovanost široké veřejnosti.[44]

Ministerstvo obrany USA vypracovalou v roce 1999 novou studii s názvem Teror 2000, která se zabývá současným stavem terorismu a předpovídá další vývoj. Závěry této studie jsou alarmující, neboť předpokládá, že rozvinuté technologie, pomocí kterých lze vyvinout či vyrobit zbraně hromadného ničení, jsou již nyní teroristům přístupné. Je tedy velmi pravděpodobné, že mohou být jednou použity. Státy jako Libye, Súdán, Irán, KLDR, Sýrie či Kuba disponují chemickými zbraněmi, některé z nich se snaží tajně vyrobit jaderné zbraně, známy jsou jaderné zkoušky KLDR, jiné provozují biologické programy. V budoucnu se tedy bude stále více měnit motivace násilí a jeho ideologie. Jedinou možností obrany se jeví spolupráce všech států světa. Je zcela jisté, že většinu států budoucí vývoj přímo či nepřímo donutí, aby se na spolupráci v boji proti terorismu podílely.[45]

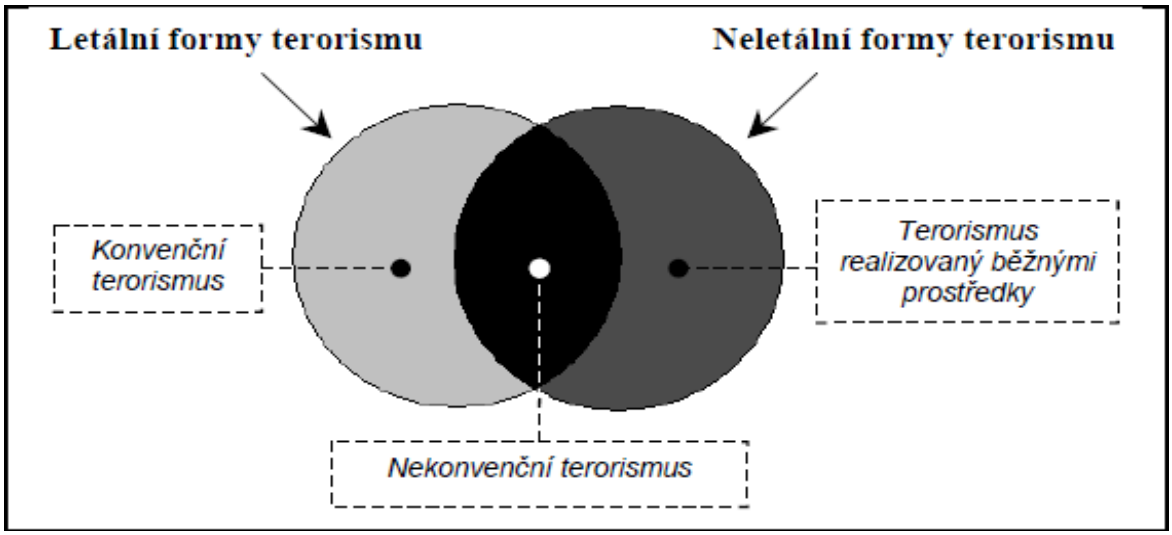
3.3. Formy terorismu

V současné době zaznamenáváme menší počet teroristckých útoků, avšak rozsah materiálních škod a počet obětí neustále roste. Tento nárůst je spojován s nárůstem počtu využívaných forem, které členíme do dvou skupin, a to na:[46]

- letální formy,
- neletální formy.

[44] BRZYBOHATÝ, M. *Terorismus I.* 2. vyd. Praha: Vydavatelství Police history, 1999. s. 138 − 139. ISBN: 80-902670-1-7.
[45] Tamtéž, s. 138 − 139.
[46] FOLTIN, P, ŘEHÁK, D. *Důvody realizace a formy terorismu. Strategie a obrana* [online] 2005, č. 1 [cit. 2013-05-13]. Dostupný na www: <http://www.defenceandstrategy.eu/cs/archiv/rocnik-2005/1-2005/duvodyrealizace-a-formy-terorismu.html>.

Obrázek 2: Vzájemný vztah mezi letálními a neletálními formami terorismu



Zdroj: FOLTIN, P, ŘEHÁK, D. *Důvody realizace a formy terorismu. Strategie a obrana* [online] 2005, č. 1 [cit. 2013-05-13]. Dostupné na www: <http://www.defenceandstrategy.eu/cs/archiv/rocnik-2005/1-2005/duvodyrealizace-a-formy-terorismu.html>.

3.3.1. Letální formy terorismu

Letální formy terorismu obsahují základní prostředky realizace násilí a liší se pouze použitými prostředky. Z tohoto důvodu je rozdělujeme na dvě podskupiny, a to konvenční a nekonvenční terorismus.

Do **konvenčního terorismu** můžeme zařadit tyto útoky:[47]

- bombové útoky,
- ozbrojené útoky, žhářství, sabotáže,
- únosy osob,
- únosy letadel,
- držení rukojmí.

Do **nekonvenčního terorismu** řadíme:[48]

- **informační operace (Infop),**
  - ⇒ kyberterorismus,
  - ⇒ psychologické operace (Psyop),
  - ⇒ ekonomická válka,

[47] FOLTIN, P, ŘEHÁK, D. *Důvody realizace a formy terorismu. Strategie a obrana* [online] 2005, č. 1 [cit. 2013-05-13]. Dostupný z www: <http://www.defenceandstrategy.eu/cs/archiv/rocnik-2005/1-2005/duvodyrealizace-a-formy-terorismu.html>.
[48] Tamtéž

- **prostředky hromadného ničení**

  ⇒ chemické zbraně,

  ⇒ jaderné zbraně,

  ⇒ radiologické zbraně,

  ⇒ zbraně založené na biologickém účinku,

  ⇒ termické zbraně.

3.3.2. Neletální formy terorismu

Neletární formy terorismu taktéž nazýváme moderním či sofistikovaným terorismem, jelikož jsou při útocích využívány moderní nástroje, respektive staré, ale novým způsobem v kombinci s letálními prostředky. Opět dle používaných prostředků při teroristickém útoku dělíme tyto formy do dvou podskupin, a to na: terorismus realizovaný běžnými prostředky a nekonvenční terorismus.[49]

Terorismus realizovaný běžnými prostředky:

- pomocí výpočetní techniky a internetu – tzv. kyberterorismus,
- pomocí dopravních prostředků – např. automobil, letadlo, vlak, loď,
- mediální terorismus – psychologický terorismus.

Nekonveční terorismus:

- zbraně využívající optiky
- zbraně využívající akustiky
- zbraně využívající elektromagnetického pulsu.

[49] FOLTIN, P, ŘEHÁK, D. *Důvody realizace a formy terorismu. Strategie a obrana* [online] 2005, č. 1 [cit. 2013-05-13]. Dostupný z www: <http://www.defenceandstrategy.eu/cs/archiv/rocnik-2005/1-2005/duvodyrealizace-a-formy-terorismu.html>.

4. Kyberterorismus

„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."[50]

Teroristé v současné době využívají stále nové metody, techniky a prostředky. Kybernetický terorismus se tak stal novou formou terorismu. Může mít podobu tradičního teroristického útoku, například fyzickou likvidací budovy, jejíž každodenní provoz je závislý na počítačích, ale také samozřejmě i virtuální prostřednictvím internetu. Čím vyspělejší stát, tím je možná větší zranitelnost prostřednictvím datových sítí.

4.1. Vymezení pojmů

Vznik internetu sebou nese existenci tzv. **informační společnosti**. Pojmem informační společnost se rozumí: *„... společnost, kde kvalita života i perspektiva sociálních změn a ekonomického rozvoje závisí na informacích a schopnosti jejich využití, tj. informace se stává klíčovým faktorem takovéto společnosti"*[51].

Jedná se tedy o společnost založenou na intenzivním využívání komunikačních a informačních technologií.

Pojem „kyberterorismus" pochází z anglického výrazu „cyberterrorism". Jedná se o složeninu dvou slov – slova „cyber" označujícího něco virtuálního a slova „terrorism" znamenající „terorismus". Kyberterorismus neboli kybernetický terorismus lze chápat jako projekci klasického, již zmiňovaného, terorismu do tzv. kyberprostoru (anglicky „cyberspace").

Informační společnost se pohybuje v tzv. **kyberprostoru**, který již definoval v roce 1984 William Gibson: *„Konsensuální halucinace každý den zakoušená miliardami*

[50] 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>.
[51] DYTRT, Z., MIKULECKÝ, P., NEJEZCHLEBA, M., PRILLWITZ, G., ROUDNÝ, R. (editoři). *Etika podnikání a veřejné správy: Informační společnost – etická výzva pro 21. století.* Sborník z 2. mezinárodní konference, Hradec Králové, 18. – 20. 5. 1999. Praha: VUSTE ENVIS, 1999. ISBN 80-902356-5-4.

oprávněných operátorů všech národů, dětmi, které se učí základy matematiky. Grafická reprezentace dat abstrahovaných z bank všech počítačů lidského systému. Neodmyslitelná komplexnost. Linie světla seřazené v ne-prostoru mysli, shluky a souhvězdí dat." [52]

Kyberprostor lze také definovat jako *„…nehmotný svět informací, který vzniká vzájemným propojením informačních a komunikačních systémů. Toto prostředí umožňuje vytvářet, uchovávat, využívat a vzájemně si vyměňovat informace. Zahrnuje počítače a databáze propojené komunikačními systémy, jako například celosvětovou síť internet. Kyberprostor využívá nové možnosti komunikace, jako jsou například emaily, webové stránky, počítačové sítě, telefony, faxy a videokonference. Nicméně je imaginárním místem, na které se nevztahují omezení fyzického světa. To mimo jiné umožňuje vznik nových identit - uživatel „opouští" své fyzické tělo a pobývá v tomto (virtuálním) prostředí bez něj"*[53].

S. McQuade III definuje kyberprostor jako *„…metaforu vyjádření virtuálního (nefyzického) prostředí vytvořeného propojením počítačových systémů v síti"*[54]. Jedná se tedy o prostor, který je primárně závislý na kybernetické infrastruktuře (anglicky *„cyberinfrastructure"*) zahrnující příslušný hardware a software.

Prostřednictvím kyberprostoru lze teoreticky ochromit infrastrukturu celého státu například shozením serverů důležitých institucí. Pojmem kyberprostor je označován jako svět virtuální reality, v němž se odehrávají každodenní úkony, například emailová či telefonická komunikace nebo právě používání internetu. Stal se tedy neoddělitelnou součástí každodenního života lidské společnosti. První počítače, které tvořily internet, počítaly s úplně jiným využitím a to spíše jako komunikační kanál. Postupem času se síť stala otevřenou společnosti a předmětem ekonomických, marketingových či politických zájmů. Proto bylo nutné se zamýšlet nad bezpečností dat. Existuje několik různých negativních dopadům, jako je například závislost na kyberprostoru, zneužívání informací v kyberprostoru, kybernetická kriminalita či kybertetorismus a kybernetické války. Kyberprostor je tedy velmi zranitelný, například je známo velmi mnoho incidentů, jako jsou špionáže, činy počítačové kriminality či protesty proti něčemu.

Mezi základní vlastnosti kyberprostoru se řadí:[55]

⇒ je decentralizovaný,

⇒ je globální,

---

[52] Wikipedia – the Free Encyclopedia. *Kyberprostor [*online] [cit. 2013-05-14]. Dostupné na www: <http://en.wikipedia.org/wiki/Cyberspace>.
[53] KUŽEL, S. Kybernetická kriminalita I: Co se děje v kyberprostoru, *BusinessIT.cz* [online], 2012.
[54] MCQUADE III, S. *Encyclopedia of Cybercrime*, 2008, s. 115.
[55] JIROVSKÝ, V. *Společnost ve virtuálním světě*. Konference CYTER [online] 2010, č. 01 [cit. 2013-05-14]. Dostupný na www: <https://cythres.fd.cvut.cz/cyter2010/cs/presentation.php>.

⇒ je otevřený,

⇒ je interaktivní,

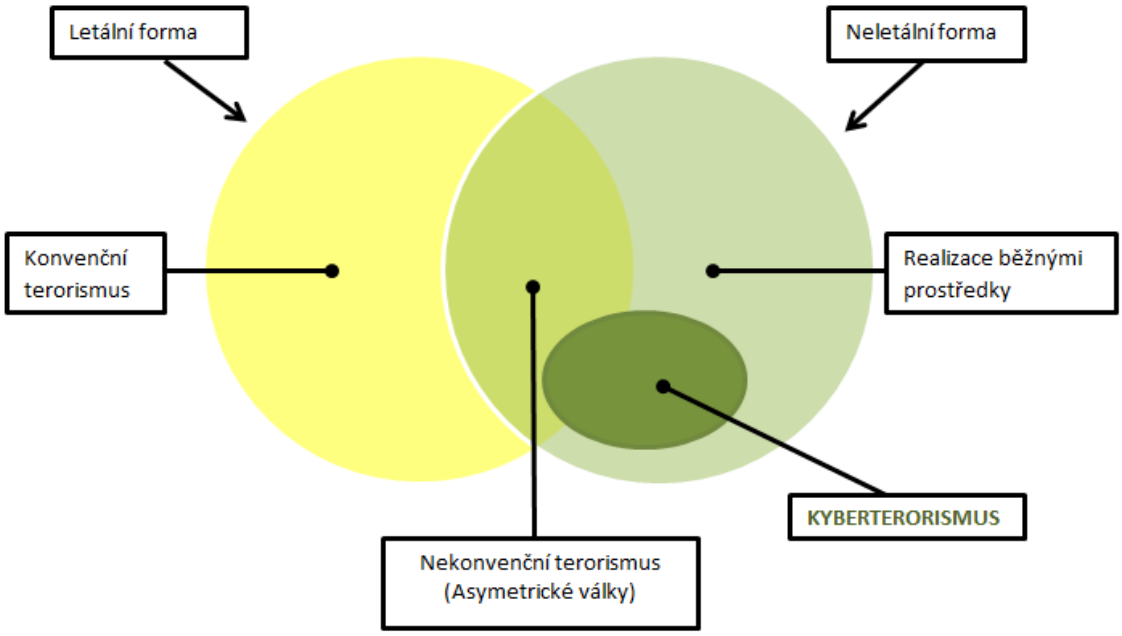
⇒ obsahuje velké množství dat a informací,

⇒ je řízen pouze uživateli,

⇒ je závislý na infrastruktuře.

Jednou z hrozeb, kterým může kyberprostor čelit je kybertetorismus. Jedná se o neletální formu teroristické činnosti realizovanou skrze služby, které podporuje a sdílí daná informační či komunikační síť. Fyzická likvidace instituce či systému vedoucí až k lidským ztrátám může být sekundárním důsledkem tohoto útoku. Ale zde se většinou nejedná o primární cíl útoku. Proto lze neletální formu považovat pouze za vnější skořápku.

Obrázek 3: Postavení kyberterorismu v rámci jednotlivých forem terorismu



Zdroj: JIROVSKÝ, V. Kyberterorismus. *Personalis* [online] 2006 [cit. 2013-05-14]. Dostupné na www: <www.as4u.cz/filemanager/files/file.php?file=3990>.

Pod pojmem kyberterorismus jsou obecně řečeno myšleny teroristické aktivity, jejichž cílem, přenašečem či použitým prostředkem je kyberprostor a fyzické či virtuální objekty, které se v něm nacházejí.

Oficiální definice kyberterorismu byla formulována Dorothy E. Denningovou: *„Kyberterorismus je konvergencí terorismu a kyberprostoru obecně chápaný jako*

nezákonný útok nebo nebezpečí útoku proti počítačům, počítačovým sítím a informacím v nich skladovaných v případě, že útok je konán za účelem zastrašit nebo donutit vládu, nebo obyvatele k podporování sociálních nebo politických cílů."[56]

Americká analytička D. E. Denningová však chápe akty kyberterorismu jako útoky směřované proti kritické infrastruktuře, které mají za cíl získání informační nadvlády. Podle Denningové mají kyberútoky jen málokdy za cíl fyzické zničení objektu. Ovšem v realitě, však většinou dochází k narušení funkcí určité služby nebo její součásti a útok tedy není veden proti vládě za určitým konkrétním účelem. Definice tedy nepostihuje nejčastější formy útoků.

V případě dalších definic kyberterorismu se ale nejedná o snadné a zcela jednoznačné vymezení tohoto pojmu, neboť je potřeba využít velkého množství přístupů. Přehled dalších nejčastěji publikovaných definic kyberterorismu je například:

- **definice kyberterorismu dle A. Colarika a L. Janczewskiho:**

„Kybernetický terorismus lze definovat jako představitele aktivit vedených nebo koordinovaných státem s cílem získat informační převahu nebo vyřadit technologickou infrastrukturu protivníka." [57]

- **definice kyberterorismu dle Severoatlantického paktu publikovaná P. Everardem:**

„Kybernetický terorismus je kybernetický útok užívající či zneužívající počítač nebo komunikační sítě za účelem způsobení dostatečné škody s cílem zastrašit společnost a mající ideologický podtext." [58]

- **definice kyberterorismu dle Ministerstva vnitra Spojených států amerických (United States Department of the Interior – DOI) publikovaná P. Everardem:**

„Kybernetický terorismus je kriminální akt vedený za pomocí počítače nebo telekomunikačních prostředků. Cílem je pak způsobit zmatek a nejistotu za účelem ovlivnit vládu či populaci k přijetí určitých politických, ideologických či sociálních témat." [59]

---

[56] DENNING, D. E. *Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy* [online] [cit. 14. 5. 2013]. Dostupné na www: <http://www.nautilus.org/infopolicy/workshop/papers/deinning.html>.
[57] JANCZEWSKI, L, COLARIK, A. *Managerial Guide For Handling Cyber-Terrorism And Information Warfare*, 2005, s. 229.
[58] EVERARD, P., NATO and Cyber Terrorism, In *Responses to Cyber Terrorism*, 2008, s. 118 – 119.
[59] Tamtéž, s. 119.

- **další definice kyberterorismu dle D. Denningové:**

„Kybernetický terorismus představuje společný střet reálných subjektů ve virtuální realitě v tzv. kyberprostoru (cyberspace).“ [60]

„Kyberterorismus je konvergencí terorismu a kyberprostoru obecně chápaný jako nezákonný útok nebo nebezpečí útoku proti počítačům, počítačovým sítím a informacím v nich skladovaným v případě, že útok je konán za účelem zastrašit nebo donutit vládu, nebo obyvatele k podporování sociálních nebo politických cílů.“ [61]

- **definice kyberterorismu dle časopisu Rexter registrovaným Ministerstvem kultury České republiky:**

„Kyberterorismus je politicky motivovaný útok na nástroje a/anebo proces získávání a/anebo zpracovávání elektronických dat, který ve svém důsledku znamená násilí nebo hrozbu násilím proti nevojenským cílům a jehož účelem je určitým způsobem ovlivnit širší okruh recipientů, než jsou přímé oběti takového útoku.“ [62]

Zde je tedy vidět, že stejně jako u pojmu terorismus neexistuje konsensus na jedné obecně platné definici, také výkladů kybernetického terorismu je celá řada.

Lech Janczewki a Andrew Colarik ještě dále vysvětlují kybernetický terorismus jako: *„…promyšlený, politicky motivovaný útok sub-státních skupin, tajných agentů nebo jednotlivců proti informačním a počítačovým systémům, počítačovým programům a datům, jehož výsledkem je násilí proti civilním osobám (nebojovým cílům)“*[63].

Takto prezentovaný pojem kybernetického terorismu má nespornou výhodu ve vyloučení aktů, které bychom zařadili spíše do kategorie kybernetických zločinů díky začlenění politické motivace útočníka. Přesto pro potřeby této práce, bude potřeba definici ještě rozšířit, tak aby se opírala o etymologický základ slova terorismus.

Za útok spadající do oblasti kybernetického terorismu budeme v této práci považovat promyšlený, politicky motivovaný útok sub-státních skupin, tajných agentů nebo jednotlivců proti informačním a počítačovým systémům, počítačovým programům

[60] DENNING, D. Cyberterrorism, *Georgetown University* [online], 2000.
[61] DENNING, D. Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy, In *ARQUILLA, John, RONFELDT, David, Networks and Netwars: The Future of Terror, Crime, and Militancy*, 2001, s. 239.
[62] Koncept politického kyber-terorismu, *Rexter* [online], 2012.
[63] JANCZEWSKI, L., COLARIK, A. *Managerial guide for handling cyber-terrorism and information warfare*. London: IGP, 2005, s. 43. ISBN 1-59140-583-1.

a datům, jehož výsledkem je násilí proti civilním osobám, nebo způsobení alespoň takové škody, jež vyvolá strach.[64]

Toto rozšíření nám přináší do kybernetického terorismu další aspekt, který úzce souvisí s různými typy útoků. Řada autorů podmiňuje zařazení útoku do kybernetického terorismu vyústěním ve fyzické násilí vůči osobám. Typů útoků, však existuje celá řada. Ačkoliv je možné napadnout kritickou infrastrukturu jako elektrárny, letový provoz atd. použitím kybernetických prostředků a dosáhnout tak ztrát na lidských životech, mnohem častějšími bývají neletální formy útoků.

Myriam Cavelty ilustruje nebezpečnost útoků na pomyslném žebříku, kdy na nejnižším stupni stojí kybernetický vandalismus (jedná se především o napadení internetových stránek), následují kybernetické zločiny a kybernetická špionáž, které dle autorky zasahují především subjekty v ekonomickém sektoru. Poslední dva stupně tvoří kybernetický terorismus a na samotném vrcholu najdeme kybernetickou válku.[65] Toto rozčlenění věrně kopíruje současný stav útoků spáchaných v kyberprostoru, přesto se v této práci vymezím vůči vyřazení například DDoS útoků z kybernetického terorismu, jelikož mohou zaprvé způsobit škody postačující k vyvolání strachu a za druhé jimi může být argumentováno ve prospěch sekuritizace.

Možnými důsledky kyberterorismu jsou:[66]

⇒ krádež dat

⇒ zničení dat

⇒ destabilizace systému

⇒ nedostupnost služby

⇒ blokování systémových prostředků atd.

4.2. Metody, technologie a nástroje kyberterorismu

Kyberterorismus může vůči informačním technologiím působit třemi níže uvedenými způsoby:

[64] Pro celou řadu definic kybernetického terorismu doporučuji: ÖZEREN, Süleyman. *Response to Cyber Terrorism*. Amsterdam: IOS Press, 2008. Cyberterrorism and International Cooperation: General Overview of the Available Mechanisms to Facilitate an Overwhelming Task, s. 161. ISBN 9781607503118.
[65] CSS Analysis in Security Policy. *Cyberwar: Concept, status quo, and limitations.* 2010. No 71. s. 1 – 3.
[66] Inflow. *Kyberterorismus v informační společnosti* [online] [cit. 2013-05-14]. Dostupné na www: <http://www.inflow.cz>.

- **přímým teroristickým útokem na lokální technologii** – specifický druh kybernetického teroristického útoku závisí na umístění a významu konkrétní technologie,
- **souběžným teroristickým útokem** – jedná se o nejnebezpečnější teroristický útok, neboť dochází k množství souběžných teroristických útoků na konkrétní zóny různých úrovní, ve většině případů se jedná o pouhou přípravu pro útok nebo podporu pro jeho dezorientaci a následné zničení,
- **zničením technologie k řízení teroristické organizace** – jedná se o soulad teroristických skupin a jejich činností globálního charakteru (tedy po celém světě), příkladem může být využití steganografie, která umožňuje skrytí textu do obrázků. [67]

Metody kyberterorismu jsou založeny především na zneužití důvěrnosti, integrity a dostupnosti počítačových systémů. Postupem času se tyto metody stále vyvíjí a zdokonalují. Prostředky kyberútoků spočívají zejména ve využití tzv. **malwaru** neboli škodlivého softwaru, k němuž patří:

- **adware** – jedná se o zvláštní softwarový prostředek, který slouží k získávání dat, údajů a informací či odposlouchávání na koncových bodech počítačových sítí,
- **spyware** – představuje mimořádný programový prostředek, pomocí něhož dochází k utajenému zasílání osobních dat uživatele,
- **trojští koně** – jedná se o druh počítačových virům skrývajících skutečnou identitu, ve většině případů se jedná o tzv. programy zadních vrátek se schopností spuštění určité činnosti v daném čase, a to zcela bez vědomí uživatele,
- **počítačové viry** – jedná se o zvláštní softwarové prostředky, které znemožňují funkce některých služeb nebo procesů počítačových sítí.

Ze skupiny malware lze dále jmenovat např. *„červy, rootkity, keyloggery, hijackery či dialery“* [68].

K dalším metodám kyberterorismu patří zejména:

- *„**hacking** – jedná se o neoprávněné získání přístupu k datům, tzv. průnik do systému jinou než standardní cestou,*
- ***technika sociálního inženýrství neboli tzv. sociotechnika** – využívá nátlakové metody v podobě časového limitu či hrozícího nebezpečí, další záminkou k získání*

[67] JIROVSKÝ, V. *Kybernetická kriminalita: Nejen o hackingu, crackingu, virech a trojských koních bez tajemství*, 2007, s. 284.
[68] PAUKERTOVÁ, V. Úvod do problematiky elektronické informační kriminality. *Ikaros: Elektronický časopis o informační společnosti* [online], 2006.

důvěry uživatelů je fakt, že například u e-mailu je odesílatelem subjekt s vyšší autoritou, obsah slibuje nevídané slevy či nabízí něco zdarma atd.,

- ***phreaking*** *– představuje činnost, která vede k bezplatnému využívání telefonních linek (napichování služby, hovory na účet někoho jiného nebo telekomunikační firmy),*
- ***phishing neboli „brand spoofing" či „carding"*** *– jedná se o běžnou metodu krádeže identity, spočívá v krádeži obecnějších privátních citlivých informací týkajících se jedince, těmito údaji mohou být především údaje o platební kartě nebo krádež přístupového jména a hesla k různým internetovým službám, s jejichž pomocí lze na dálku manipulovat s bankovním kontem, tyto nelegálně získané údaje jsou pak zneužity například při převodu peněz, internetových nákupech, aukcích a jiných internetových podvodech,*
- ***pharming*** *– spočívá v překládání URL adresy do formátu IP adresy prostřednictvím DNS serverů, útočníci se pokoušejí najít špatně zabezpečený server, v němž následně přepíší IP adresu určenou například pro URL banky IP adresou falešné stránky"* [69]**.**

Velmi známou metodou kyberterorismu je tzv. **defacement** (tj. přetvoření, modifikování či nahrazení) internetových stránek serveru jiným obsahem. Jedná se o tzv. skupinu psychologického infoware. Podstata této metody spočívá ve změně či přesměrování primární internetové stránky, což vede k dezorientaci uživatelů. Další metodou je tzv. **spam**. Spamem se rozumí nevyžádaná e-mailová pošta. Lze zmínit také tzv. **hoax**, což je falešná poplašná zpráva varující uživatele před případným nebezpečím. Hoax může mít například formu e-mailových zpráv, které uživatele vybízí k jejich dalšímu rozesílání mezi přátele a známé (jedná se o tzv. řetězové e-maily).

K charakteristickým znakům hoaxingu patří kupříkladu:

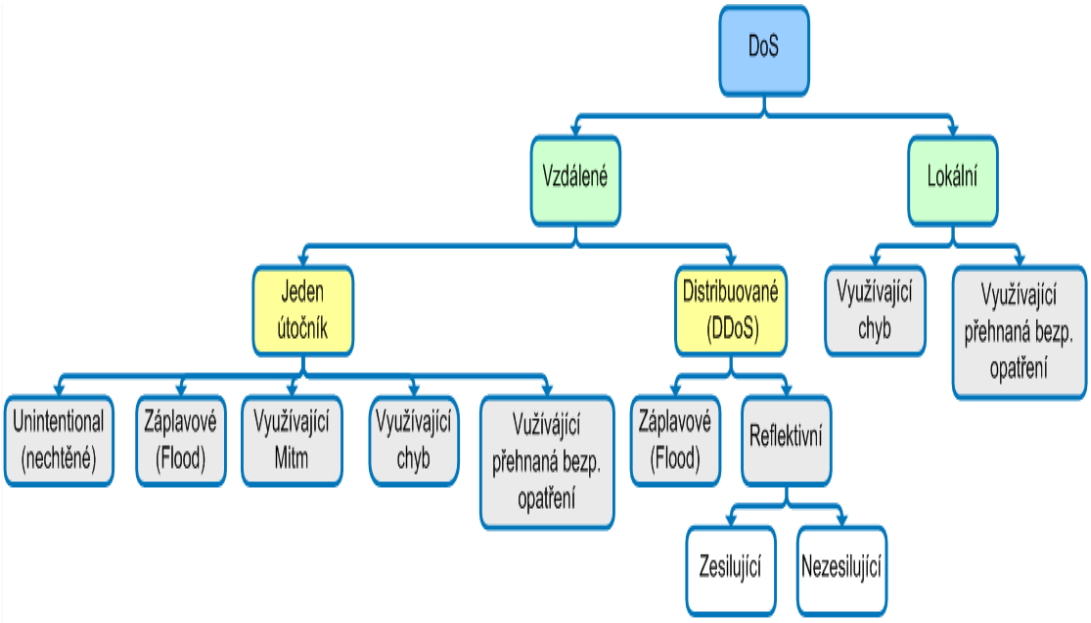
- *„obtěžování příjemců,*
- *nebezpečné rady,*
- *nadbytečné zatěžování linek a serverů,*
- *ztráta důvěryhodnosti šiřitele,*
- *prozrazení důvěrných informací,*
- *přetěžování konkrétní cílové e-mailové schránky,*

[69] PAUKERTOVÁ, V. Úvod do problematiky elektronické informační kriminality. *Ikaros: Elektronický časopis o informační společnosti* [online], 2006.

- *poškození konkrétní instituce“* [70].

Snad největší kybernetickou hrozbu (metodu kyberterorismu) v současné době představuje tzv. **odepření služby** (anglicky „**Denial of Service**“ – označovaný zkratkou „**DoS**“), neboť se jedná o nejpoužívanější a také nejnebezpečnější formy kyberútoků. Rozdělení DoS útoků je uvedeno na obrázku 4 níže.

Obrázek 4: Rozdělení DoS útoků



Zdroj: HALLER, M. Denial of Service útoky: reflektivní a zesilující typy. *Lupa.cz* [online] 2006 [cit. 2013-06-20]. Dostupné na www: <www.lupa.cz/clanky/denial-of-service-utoky-reflektivni-a-zesilujici-typy/>.

DoS představuje *„ …přehlcování cílové stanice požadavky, které vedou ke zpomalení či k odstavení systémů, na něž je útok veden“* [71]. Takové přehlcování serveru má ve většině případů za následek jeho zhroucení, případně zahlcení a restartování vzdáleného počítače.[72]

Skupina CERT (Computer Emergency Response Team) charakterizuje DoS útoky jako *„ …explicitními pokusy útočníků směřované k legitimním uživatelům služeb k zabránění jejich používání“* [73]. Jednoduše lze říci, že se jedná o zabránění v přístupu

[70] Nebezpečné komunikační praktiky: Co je hoax. *E-bezpečí* [online], 2008.
[71] JANCZEWSKI, L., COLARIK, A. *Managerial Guide For Handling Cyber-Terrorism And Information Warfare*, 2005, s. 85 – 95.
[72] PAUKERTOVÁ, V. Úvod do problematiky elektronické informační kriminality. *Ikaros: Elektronický časopis o informační společnosti* [online], 2006.
[73] Denial of Service Attacks, *CERT* [online], 2013.

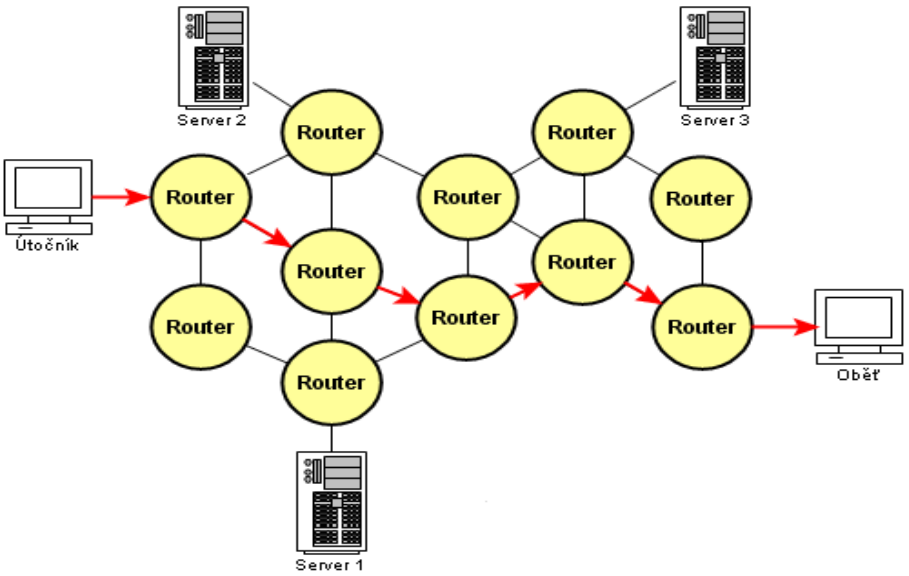
k informacím nebo služby zákonným uživatelům (například zabránění v přístupu k e-mailu, webovým stránkám, on-line účtům – kupříkladu elektronického bankovnictví atd.). [74]

K DoS útokům dle skupiny CERT patří:

- *„pokusy o zahlcení sítě, které mají zabránit legitimnímu provozu sítě,*
- *pokusy o narušení spojení mezi dvěma zařízeními, které mají zabránit přístupu ke službě,*
- *pokusy zabránit konkrétní osobě v přístupu ke službě,*
- *pokusy o narušení služby pro určitý systém nebo osobu“* [75].

Identifikace některého z výše uvedených pokusů (odmítnutí služby) nemusí vždy znamenat skutečný DoS útok. V některých případech se může jednat o tzv. asymetrické útoky, kdy k uskutečňování DoS útoků dochází pouze s omezenými zdroji. Ty však mohou napadnout velké sofistikované sítě – kupříkladu *„útočník se starým počítačem a pomalým modemem může zakázat mnohem rychlejší a sofistikovanější stroje nebo sítě“* [76]. Obecné schéma běžného DoS útoku je uvedeno na obrázku 5 níže.

Obrázek 5: Schéma běžného DoS útoku



Zdroj: HALLER, M. Denial of Service útoky: reflektivní a zesilující typy. *Lupa.cz* [online]. 2006. [Cit. 2013-06-20]. Dostupné na www: <www.lupa.cz/clanky/denial-of-service-utoky-reflektivni-a-zesilujici-typy/>.

[74] Understanding Denial-of-Service Attacks, *US-CERT: United States Computer Emergency Readiness Team* [online], 2013.
[75] Denial of Service Attacks, *CERT* [online], 2013.
[76] Tamtéž

DoS útoky jsou realizovány v různých formách a jsou zaměřeny na celou řadu služeb. Lze rozpoznávat následující **druhy DoS útoků:**

- *„spotřebu vzácných, omezených nebo neobnovitelných zdrojů,*
- *zničení nebo změnu informací o konfiguraci,*
- *fyzické zničení nebo změnu síťových komponent“* [77].

Pro realizaci DoS útoků v podobě spotřeby vzácných, omezených či neobnovitelných zdrojů jsou nutné jisté předpoklady počítače nebo sítě – například *„šířka pásma, paměť a místo na disku, čas procesoru, datové struktury, přístup k ostatním počítačům a sítím, popř. některé ekologické zdroje (tj. energie, chladný vzduch či voda)“*[78].

Základním předpokladem je však připojení k síti. Tento druh DoS útoků začíná navazováním spojení útočníka s počítačem oběti, přičemž nedochází k dokončení tohoto spojení. Zatímco oběť vyčkává na dokončení falešného a částečně otevřeného spojení, legitimní spojení jsou odmítnuta[79]. Dalším způsobem DoS útoků v podobě spotřeby vzácných, omezených či neobnovitelných zdrojů je použití vlastních prostředků ze strany útočníka – tyto DoS útoky jsou nazývány jako tzv. zaplavování (anglicky flood attacks). Ve většině případů se jedná o velmi nečekané útoky.

Tyto útoky spočívají v *„…obesílání cílové stanice vysokým objemem datových paketů prostřednictvím internetového protokolu UDP (User Datagram Protocol), který nevyžaduje spolehlivý příjem zaslaných dat. Pakety vytěžují kapacitu komunikační linky a pracovní výkon cílové stanice, což může mít za následek zpomalení či úplnou nedostupnost stanice a služeb na ní fungujících“*[80].

Dalším typem DoS útoku jsou nároky útočníka na šířku pásma. Útočníci si tak mohou nárokovat všechny dostupné šířky pásma na síti. Dochází ke generaci velkého množství paketů (obvykle ICMP paketů), které směřují k síti. Útočník ve většině případů koordinuje i několik strojů v různých sítích.[81] Kromě šířky pásma mohou útočníky využívat také jiných zdrojů – například počty datových struktur. Útočník spotřebovává datové struktury za pomocí jednoduchého programu či skriptu, který opakovaně vytváří kopie sebe sama.

[77] Denial of Service Attacks, *CERT* [online], 2013.
[78] Tamtéž
[79] Tamtéž
[80] DISTERER, G., ALLES, A., HERVATIN, A.. Denial-of-Service (DoS) Attacks: Prevention, Intrusion Detection, and Mitigation, *In JANCZEWSKI, Lech, COLARIK, Andrew, Cyber Warfare and Cyber Terrorism*, 2008, s. 265.
[81] Denial of Service Attacks, *CERT* [online], 2013.

Útočník může využívat také:

- *„generování nadměrného množství e-mailových zpráv,*
- *záměrného generování chyb, pro které je třeba se přihlásit,*
- *umístění souborů na FTP protokoly (File Transfer Protocol), sloužící pro přenos souborů mezi počítači pomocí počítačové sítě nebo na sdílené síťové složky pro informace o správné konfiguraci pro anonymní FTP protokoly“* [82].

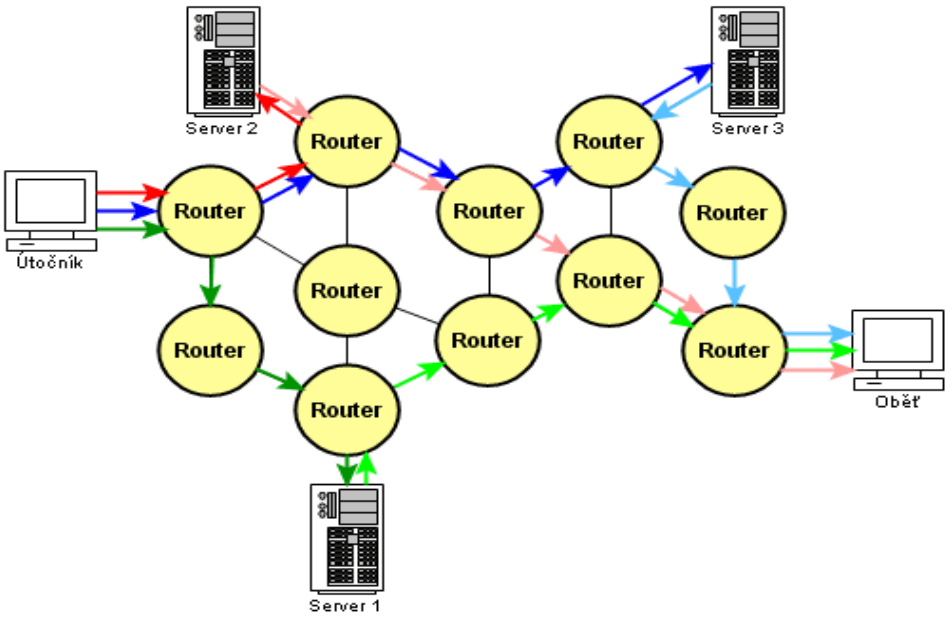
V současné době již existuje mnoho způsobů, kterými lze po určitém počtu neúspěšných pokusů o přihlášení uzamknout jakékoliv účty. Pro útočníky však toto není žádnou překážkou, neboť mohou legitimním uživatelům zabránit v přihlášení, a to v některých případech také na privilegované účty. Útočníci mohou způsobit také selhání systému pomocí nestabilního zasílání neočekávaných dat po síti. [83] K DoS útokům lze zařadit také napadení dalších zdrojů ze strany útočníků – například tiskáren, páskových připojení apod. DoS útoky v podobě zničení nebo pozměnění informací o konfiguraci spočívají v likvidaci nebo změnách konfiguračních dat, což má za následek zabránění používání počítače nebo sítě.

DoS útoky v podobě fyzického zničení nebo změny síťových komponent spočívají *„…v neoprávněném přístupu k počítačům, routerům, síťovým skříním elektroinstalace, segmentům páteřních sítí, napájení a chlazení stanic, popř. dalších důležitých součástí“* [84].

Variantou DoS útoků je tzv. **distribuovaný DoS** (anglicky *„**Distributed Denial of Service**“* označovaný zkratkou *„**DDoS**“*) neboli také tzv. reflektivní útoky (viz obrázek 6 níže). Tyto DDoS útoky jsou prováděny souběžně z velkého množství počítačů spadajících do tzv. sítě internetových robotů (botnet). Jedná se o velmi efektivní útoky uskutečňované právě prostřednictvím těchto počítačových stanic, kterých mohou být „jen“ desítky nebo také milióny, neboť útočníci velmi koordinovaně napadají vybranou oblast.

[82] Denial of Service Attacks, *CERT* [online], 2013.
[83] Tamtéž
[84] Tamtéž

Obrázek 6: Schéma reflektivního DoS útoku



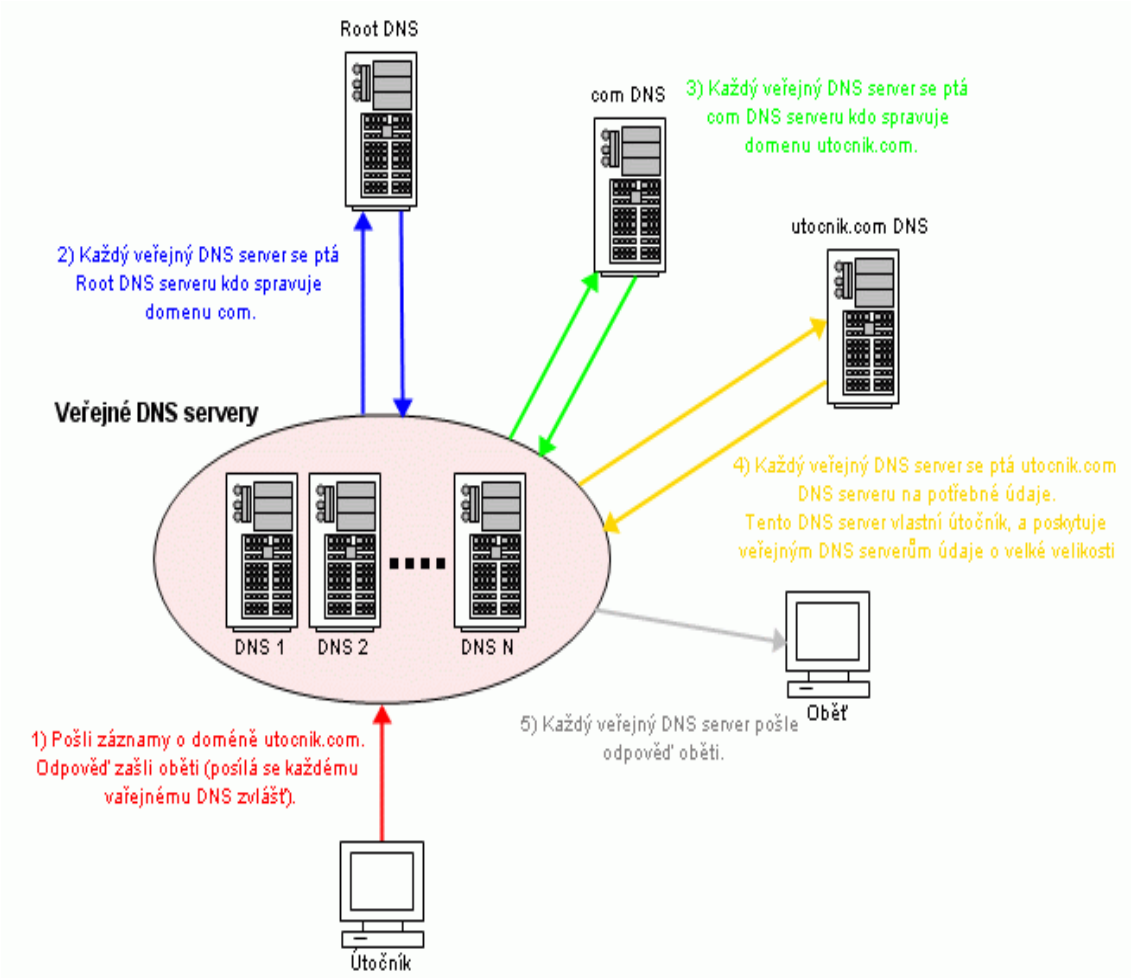
Zdroj: HALLER, M. Denial of Service útoky: reflektivní a zesilující typy. *Lupa.cz* [online] 2006 [cit. 2013-06-20]. Dostupné na www: <www.lupa.cz/clanky/denial-of-service-utoky-reflektivni-a-zesilujici-typy/>.

DDoS útoky dle způsobů jejich uskutečňování (tedy jejich účelu) lze klasifikovat následujícím způsobem:

- již zmiňované zaplavování (flood attacks) – viz výše,
- zesilující útoky (anglicky *DNS amplification attacks*) – jedná se o kyberútoky využívající chyb v počítačových sítích, prostřednictvím nichž dochází k přeměně vstupních požadavků o malé velikosti na požadavky o větší velikosti, Tyto útoky jsou obvykle zaměřeny na celou síť, odpověď je nastavena na IP adresu oběti, schéma DNS zesilujícího DNS útoku je znázorněno na obrázku 7 níže,
- SYN záplavy (anglicky *SYN flood*) – tyto kyberútoky využívají seznamu počítačů, které útočník využije k falešnému navázání spojení, *„útočník začne posílat TCP pakety s nastaveným příznakem SYN a zdrojovou IP adresou nastavenou na IP adresu oběti, tyto servery si myslí, že se s nimi oběť snaží navázat komunikaci a pošlou jí zpět TCP paket s příznaky SYN a ACK, oběť ovšem nic takového nečeká a normálně by poslala TCP paket s příznakem RST, ovšem v dnešní době toto pravidlo není dodržováno, nebo je filtrováno, takže oběť nic takového neodešle,*

server (použitý jako prostředník) si myslí, že jeho TCP paket s příznaky SYN a ACK se asi někde ztratil, tak jej pošle znovu, a tak to jde dál“ [85].

Obrázek 7: Schéma DNS zesilujícího útoku



Zdroj: HALLER, M. Denial of Service útoky: reflektivní a zesilující typy. *Lupa.cz* [online] 2006 [cit. 2013-06-20]. Dostupné na www: <www.lupa.cz/clanky/denial-of-service-utoky-reflektivni-a-zesilujici-typy/>.

4.3. Příklady realizovaných kyberútoků z minulosti

Národní CSIRT České republiky (Computer Security Incident Response Team – bezpečnostní tým pro koordinaci řešení bezpečnostních incidentů v počítačových sítích provozovaných v České republice) prostřednictvím svých internetových stránek CSIRT.CZ uvádí statistiky kyberútoků za období od 1. 4. 2008 do 16. 6. 2013 – viz tabulka 1 níže.

[85] HALLER, M. Denial of Service útoky: reflektivní a zesilující typy, *Lupa.cz* [online] 2006.

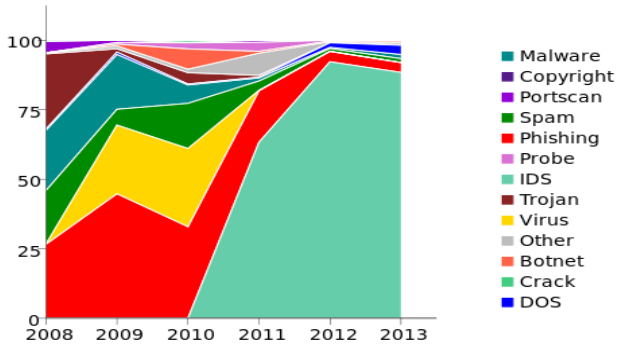
Tabulka 1: Počty otevřených a uzavřených incidentů kyberútoků dle typu v období 2008 – 2013 [86]

Typ kyberútoku	Rok						Celkem
	2008	2009	2010	2011	2012	2013	
IDS	-	-	-	491	3 924	1541	**5 956**
Phishing	65	220	209	144	159	62	**859**
Virus	-	121	178	1	1	-	**301**
Spam	47	28	103	26	43	24	**271**
Malware	53	97	42	9	19	27	**247**
DOS	1	4	2	2	68	57	**134**
Trojan	66	6	26	5	5	5	**113**
Ostatní	1	5	8	62	13	14	**103**
Botnet	-	3	46	5	8	8	**70**
Probe	-	3	14	25	12	5	**59**
Portscan	10	4	1	6	1	-	**22**
Crack	1	-	4	-	-	-	**5**
Copyright	-	-	1	-	1	-	**2**
Celkem	**244**	**491**	**634**	**776**	**4 254**	**1 743**	**8 142**

Zdroj: upraveno dle CSIRT.CZ: Incident handling statistics. *CSIRT.CZ* [online] 2013 [cit. 2013-06-21]. Dostupné na www: <http://csirt.cz/files/csirt/statistics/stats.html>.

Z tabulky 1 výše je patrné, že kyberútoků v České republice od roku 2008 stále přibývá. K extrémnímu nárůstu počtu kyberútoků došlo v roce 2012, kdy se počet napadení počítačových sítí oproti předešlému roku 2011 zvýšil o 3 478 kyberútoků. Největší počet kyberútoků je od roku 2001 zaznamenán Systémem detekce průniku (Intrusion Detection System – IDS). K tabulce 1 se vztahuje obrázek 8 níže znázorňující počty otevřených a uzavřených incidentů kyberútoků dle typu v období 2008 – 2013 a dále obrázek 9 níže, který zobrazuje celkový počet otevřených a uzavřených incidentů kyberútoků.

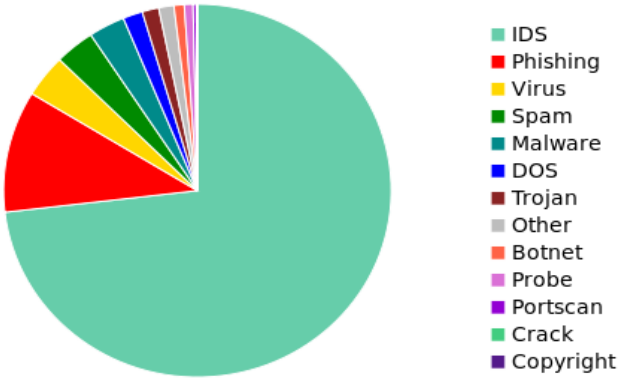
Obrázek 8: Počty otevřených a uzavřených incidentů kyberútoků dle typu v období 2008 – 2013



Zdroj: CSIRT.CZ: Incident handling statistics. *CSIRT.CZ [*online] 2013 [cit. 2013-06-21]. Dostupné na www: <http://csirt.cz/files/csirt/statistics/stats.html>.

[86] CSIRT.CZ: Incident handling statistics, *CSIRT.CZ* [online], 2013.

Obrázek 9: Celkový počet otevřených a uzavřených incidentů kyberútoků



Zdroj: CSIRT.CZ: Incident handling statistics. *CSIRT.CZ* [online] 2013 [cit. 2013-06-21]. Dostupné na www: <http://csirt.cz/files/csirt/statistics/stats.html>.

Největší kyberútoky na české servery v historii uvádí internetový portál Patria Online, a. s.:

- *„30. září 2008 – DDoS útok na zpravodajské weby Blesk.cz a DenikSport.cz,*
- *29. května 2011 – napadení internetových stránek Cermat,*
- *leden a únor 2012 – napadení internetových stránek autorských organizací – například Ochranného svazu autorského, Mezinárodní federace hudebního průmyslu IFPI, Intergramu, webu ODS nebo stránky Poslanecké sněmovny a vlády,*
- *14. října 2012 – napadení internetových stránek brněnských komunistů,*
- *16. listopadu 2012 – získání databáze z webu exekutorské komory a umístění dat na internetu,*
- *březen 2013 – DDoS útoky na velké české zpravodajské weby, portál Seznam.cz, stránky českých bank včetně internetového bankovnictví“* [87].

1 – DDoS útok, při kterém byly servery zahlceny velkým množstvím dotazů a nefungovaly, postihl zpravodajské weby Blesk.cz a DenikSport.cz, které patří vydavatelství Ringier.

2 – Hacker napadl den před zahájením písemné části státních maturit internetové stránky s ukázkovými testy a informacemi o zkoušce, nefungovaly ani stránky organizace Cermat, která maturity zajišťuje, útočníci nahráli na web vlastní obsah.

[87] Patria online, a.s. Zpravodajství [online] 2013 [cit. 2013-06-21]. Dostupné na www: <http://www.patria.cz/zpravodajstvi/zpravy.html>.

3 – Během schvalování kontroverzní dohody proti padělatelství ACTA napadli lidé, hlásící se k hnutí Anonymous, celou řadu českých webů. Terčem útoku byly internetové stránky autorských organizací (Ochranného svazu autorského, Mezinárodní federace hudebního průmyslu IFPI či Intergramu), ale i web ODS nebo stránky Poslanecké sněmovny a vlády. Intenzita a druh útoků byly různé, vedle zahlcení serverů se hackerů podařilo například získat osobní data tisíců členů ODS.

4 – Internetovou stránku brněnských komunistů napadli hackeři z hnutí Anonymous. Téměř na den na ně umístili nápis, podle něhož jsou voliči KSČM "omezení idioti". Web pozměnili po krajských volbách, a to v reakci na úspěch komunistů, jehož v nich dosáhli.

5 – Hackeři získali databázi z webu exekutorské komory a data umístili na internetu. Skupina Czechurity na svém webu uvedla, že zabavili databázi, neboť exekutoři zabavují majetek občanům. Web komory byl na krátkou dobu po oznámení útoku mimo provoz.

6 – Od 4. března napadli neznámí útočníci pomocí DDoS útoku, kdy zahltili servery obrovským množstvím požadavků, nejprve velké české zpravodajské weby. V úterý byl terčem útoku také portál Seznam.cz i další stránky. Dnes čelí napadení stránky českých bank včetně internetového bankovnictví.

5. Konstrukce reality a terorismus

V této kapitole se budu zabývat dvěma klíčovými pojmy v rámci jistých odlišných konstrukcí realit, které představují sociální konstrukce reality jako symbolického světa v pojetí Bergera a Luckmanna a konstrukce reality médií v pojetí Niklase Luhmanna, a jejich dopadů a vlivů na terorismus jako „hrozbu" dnešní společnosti. Cílem kapitoly je ukázat konstrukci reality „kyberterorismu" v médiích.

Je zcela zřejmé, že teroristické akty, ať již jsou uskutečňovány v rámci fyzického světa či kyberprostoru, jsou aktivitami lidí, kteří se radikálně vymezují vůči současnému uspořádání společnosti a jejich hodnot. Jinými slovy, terorismus můžeme považovat za jistou formu anarchie, jehož cílem je změna společenského řádu, případně klíčových rozhodnutí ve sféře politické či ekonomické. Celá reflexe terorismu a kyberterorismu v médiích či společnosti je založena na hodnotové diferenci, případně určité nekompatibilitě teroristů.

Na začátku je důležité zdůraznit, že sociální konstrukce reality a konstrukce reality v mediálním diskurzu jsou značně diferencované. Základní diference spočívá, jak ukážu v této kapitole, v rozdílném pojímání času a prostoru při modelování skutečnosti. Konstrukce terorismu v médiích je vyústěním konfliktu mezi dvěma odlišnými systémy, přičemž v rámci kyberprostoru se stále ještě jedná o konflikt latentní.

5.1. Sociální konstrukce reality

Klíčovým aspektem, se kterým pracuje sociální konstrukce reality při vývoji a tvorbě společenských systémů a řádů, je forma vědění, skrze kterou lze danou verzi reality vymezit. Dané verze reality však nejsou založeny na empirickém zkoumání, ale převážně na symbolickém řádu. Tento řád plní dvě role, je zároveň základním a výkladovým systémem pro tvorbu univerza. Hegemonii tohoto řádu může narušit objevení se alternativního symbolického řádu.

„Objevení se alternativního symbolického světa představuje velké ohrožení, protože samotná existence takového světa empiricky dokazuje, že náš vlastní svět není až

tak nevyhnutelně samozřejmý…. Tato šokující skutečnost musí být, když už nic jiného, alespoň teoreticky vysvětlena.“[88]

Terorismus se tak nachází v opozici vůči pohledu Evropy a Západu, který vytváří diferující konstrukci, aby tak legitimizoval své postavení a vymezil se vůči veškerému „jinému“, které nezapadá do jeho verze reality.

Nabízí se samozřejmě otázka, jak je možné tuto sociální konstrukci reality legitimizovat a obhajovat? Nutností je podpora všech mechanismů úzce spjatých s mocenskými strukturami:

„Pojmové aparáty sloužící k udržování symbolického světa jsou rovněž produkty společenské činnosti, stejně jako všechny formy legitimizace, a nemohou být pochopeny bez porozumění ostatním činnostem daného společenství.“[89]

Lze to přirovnat k téměř totalitárním prostředků, uvážíme-li, že propojení sociální konstrukcí reality s vytvářením pojmových aparátů sjednocených s konkrétním sociálním řádem, dokážou institucionalizovat formy vědění a tím dlouhodobě udržovat v chodu konkrétní symbolický svět.

„Pojmové aparáty pro udržování symbolických světů v sobě vždy zahrnují systematizaci kognitivních a normativních legitimizací, které už byly ve společnosti přítomny v mnohem jednodušší formě a vykrystalizovaly v daný symbolický svět.“[90]

Legitimizace tohoto symbolického světa jsou tak v zásadě evolucí integrace legitimizme jednotlivých institucí. Můžeme říci, že se jedná o komplexnější symbolický svět.

Institucionalizované vědění západní společnosti a rozličný hodnotový systém teroristů a jejich pohled na „svobodu“ v rámci kyberprostoru činí základní vymezení odlišných symbolických světů při výzkumu diference v produkci médií, hlavně z pohledu jejich popisu reality, které se odehrávají v již institucionalizovaném mediálním prostředí.

Dalším důležitým prvkem v našem výkladu, který nesmíme opomenout, je samotná teorie vědění. Vycházíme z toho, že žádné vědění není odtrženo od reality společnosti, jejích tradic a kulturního vývoje. Jinými slovy, vědění nelze posuzovat z exteritoriálního pole a oprostit jej ze základů společnosti, jež jej vytvořilo a to včetně jazykových prostředků a struktur, které mu dávají význam a zakotvují jej uvnitř institucionálních forem. To znamená, že vědění získává svou platnost v tomto kontextu a v dané epistémé.

[88] BERGER, P. L./LUCKMANN, N. *Sociální konstrukce reality,* 1. vyd. Brno: CDK, 2001. s. 108. ISBN 80-85959-46-1.
[89] Tamtéž, s. 109
[90] Tamtéž, s. 109

Sociální konstrukci reality lze proto považovat za konstrukce možných forem reálného na základě historických, sociálních a kulturních souvislostí, které umožnily vznik a začlenění této instituce vědění.

Již z vymezení teroristů, jako osob, jež v zásadě stojí proti současnému uspořádání společenského systému, či proti pravidlům stanoveným v rámci kyberprostoru, je zřejmé, že dochází k produkci rozlišné verze reality. V případě islámských teroristů je tato produkce spjata s historickým a kulturním vývojem. Co se týče kyberterorismu, určitá skupina hackerů se vyvíjela již od počátku kyberprostoru, i když původně se jednalo o spřátelené hackery, kteří se podíleli na pozitivním vývoji kyberprostoru a až následně došlo k vytvoření lidí, kteří úmyslně ničili a narušovali prostor původně svobodné výměny informací a znalostí.

Musíme ještě vzít v úvahu, že vědění nereprezentuje samu realitu a samo o sobě není ani žádným řádem. V současné době, a to také díky struktuře internetu vědění, nabývá síťové podoby, z čehož vyplývá, že informace se nacházejí pouze na místech, kde je dopředu zajistíme určitou operací. Tento princip dává velký vliv celé řadě ideologií a politické moci a umožňuje jim šíření a vytváření rozličných typů realit.

5.2. Média a konstrukce reality

To, co víme o naší společnosti, tedy o světě, ve kterém žijeme, a co tvoří z převážné části naši „realitu“ se dozvídáme z velké části prostřednictvím masmédií. Platí to celkově o vědomostech z téměř všech oblastí našeho života – o společnosti, dějinách, vědě, přírodě atd. Proto je nyní důležité vysvětlit diferenci mezi sociální konstrukcí reality tak, jak byla popsána v předchozí kapitole a konstrukcí reality, jež vytvářejí média, případně masmédia.

Pod pojmem masmédia rozumíme všechny společenské instituce, které rozšiřují komunikaci pomocí jakýchkoliv technických prostředků. K nejzásadnějším masmédiím řadíme knihy, časopisy a noviny z tiskových prostředků. A vzhledem k zaměření práce jsou jimi samozřejmě také veškeré materiály a kopie elektronické povahy. Podmínkou masmédií je jejich šíření ve velkém množství s neurčitým adresátem.

Sociální konstrukce je založena na předpokladu určitých organizovaných jednání, která vycházejí z uspořádání předpisů a norem pro vlastní fungování. Systém sociální konstrukce pracuje s předdefinovanou symbolickou interakcí. Činitelé se utvářejí v konkrétních interakcích a na jejich základě jsou situována na jednotlivé režimy jednání.

Řád je zde pojímán symbolicky. Média konstruují realitu na základě jiných principů. Na tomto místě uveďme pro začátek rozdílné uspořádání časového rámce. N. Luhmann popisuje základní diferenci mezi sociální a mediální konstrukcí takto:

„Jeden důležitý, totiž časový aspekt vztahu společnosti a interakce lze uchopit pojmem epizoda. Interakce jsou epizody společenského procesu. Jsou možné pouze na základě jistoty, že společenská komunikace proběhla již před začátkem epizody, takže lze předpokládat akumulace předchozí komunikace: a jsou možné pouze proto, že se ví, že společenská komunikace je možná i po ukončení epizody. Začátek a konec epizody jsou pouze cézurami v autopoésis společnosti… Interakce tak realizuje společnost tím, že je oproštěna od nutnosti být společností."[91]

Vidíme, že časová dimenze je zde zcela neslučitelná. Navíc celková sociální interakce je rozdělena na rozdílných principech. Při sociální konstrukci je organizovaná, spojitost mezi ději a vztahy je předem očekávaná. Média konstruují realitu kontingentně, vytváří nepravděpodobná spojení událostí. Můžeme říci: Mediální konstrukce má vyšší komplexitu, která vede k nepravděpodobnosti plné předpokladů.

„Jednoduché společnosti se nedají dekomponovat, aniž by byla ztracena sociální kvalita života zúčastněných. Komplexní společnosti sestávají sice z jednoduchých společností, ale jsou, protože jsou složené, také rozložitelné, a proto modifikované na vyšším stupni."[92]

Dalo by se říci, že realita je v mediální konstrukci smyšlená. Protože nemá přímého referenta, čímž chybí odpovídající zpětná vazba. Mediální konstruování reality je oproti sociální spíše celou řadou kontingenčních vazeb. S vývojem technologií a doby se radikálně proměňuje status médií, čímž dochází ke změně reference k reálnému a ke konstrukcím reality. Mediální realitu, tak lze definovat jako vyprázdnění reality, založené na relacích.

Z toho vyplývá, že chceme-li se zabývat konstrukcemi reality v médiích, je potřeba brát v potaz, že mediální realita se ustavuje toliko jako realita relační. Pojímáme ji tedy jako určité operativní prostředí, založené z větší části na režimu technologického zprostředkování se zvláštním typem „komunikace" a procesování. Zásadním bodem analýzy mediální reality, jak blíže ukážu v následující kapitole, je zdvojení reality v mediálním diskurzu, doprovázené procesy sebe-reference a reference někoho jiného.

---

[91] LUHMANN, N. *Sociální systémy – nárys obecné teorie,* 1. vyd. Brno: CDK, 2006. s. 461. ISBN 80-7325-100-0.
[92] Tamtéž, s. 462

Cílem analýzy je pak pochopení samotných operací sebe-reference a reference jiného. To znamená, že výstupem by mělo být samotné sebe-referování o reflexi zprostředkování a pojímání mediální reality jako autopoietického systému. Jinými slovy, nejdříve musíme být schopni uchopit, jaké operace v komunikaci přenášejí informace, abychom s nimi mohli pracovat jako vlastní sebe-referencí a nemuseli si pomáhat dalšími systémy porozumění.

Toto porozumění je důležité pro samotné pochopení sekuritizace jako auto-referenčního problému. Pokud média vytvářejí konstrukci reality, ve které je dané téma řazeno do bezpečnostního diskurzu a nemá konkrétního referenta, dojde nakonec k odkazům na své vlastní popisy událostí, čímž vytvoří logiku auto-referenční simulace.

5.3. Masmédia, konstrukce reality a reference druhého

V předchozí kapitole jsem definoval pojem masmédií, který nyní rozšířím o další aspekty. Masmédia jsou tedy všechny společenské instituce rozšiřující komunikaci skrze technické prostředky.

K masmédiím počítáme také veřejné vysílání. Na druhou stranu nesplňují vymezení tohoto pojmu produkce odehrávající se ve veřejném sektoru jako divadelní představení, koncerty, přednášky atd., ovšem jejich diseminace prostřednictvím různých přenosových prostředků ano. Vycházíme z toho, že až masová mechanická výroba umožnila vznik systému masmédií. Jde o to, že technologie pouze vytváří médium, které je schopno vytvářet formy a provádět komunikační operace.

Důležitým aspektem je: *„…že nemůže probíhat žádná interakce mezi přítomnými emitenty a recipienty. Interakce je vyloučena vložením techniky, a to má dalekosáhlé důsledky, které nám definují pojem „masmédia.“*[93]

To, že recipientům je díky použití aparátů znemožněna interakce, má dva důsledky. Zaprvé je umožněna relativně velká svoboda komunikace, čímž vzniká redundantní počet komunikačních možností. Tento přebytek možností lze kontrolovat pouze uvnitř systému a to prostřednictvím sebe-organizace a vytvářením vlastních konstrukcí reality. Zadruhé, organizace produkující komunikace musí počítat s tím, že nedokážou cílit na jedince. Masmediální produkce se tak standardizuje a částečně diferencuje, aby měl recipient

[93] LUHMANN, N., *The Reality of the Mass Media.* 2. vyd. Stanford: Polity Press, s. 4. ISBN 0-8047-4076-3.

na výběr. Nyní jsem zmínil určité strukturální podmínky omezující tvorbu reality masmédií.

Je nutno podotknout, že o realitě masových médií můžeme hovořit ve dvojím smyslu. Prvním je „fyzická“, jinými slovy skutečná realita. Je založena na operacích, jež jsou masovým médiím vlastní. Dochází k tisku, vysílání, a ze strany recipientů k četbě a sledování vysílání. Proces takového šíření komunikace je zcela závislý na technologiích, které tak vytvářejí struktury a limity masové komunikace. V rámci mé práce není nutné studovat operace těchto strojů.

„…má smysl nahlížet na skutečnou realitu masmédií jako na komunikace, které v nich plynou a probíhají. Nepochybujeme o tom, že takové komunikace fakticky probíhají. Vyloučením technické aparatury, „materializace komunikace“, včetně jejich významu, z operací toho, co je komunikováo, a to proto, že nejsou tím, co je sdělováno, zahrnujeme do tohoto procesu recepci.“[94]

Ke komunikaci dochází pouze tehdy, pokud se jedná o jednotu tří selekcí. K úspěšné či neúspěšné komunikaci dochází, pokud dojdou jednoty informace, sdělení a porozumění. Faktor porozumění je zde zcela klíčový. Samotné sdělování tedy komunikaci nekonstituuje.

„Komunikace je tedy nadále pojímána jako triadická jednota. Vycházíme z toho, že musí být syntetizovány tři selekce, aby byla komunikace uskutečněna jako emergentní dění. Dle Bühlera má lidský jazyk tři „kapacity“ či „funkce“: znázorňovací, vyjadřovací a apelové. První pojem míní selektivitu informace samotnou, druhý selekci jejího sdělení a třetí očekávání výsledku, očekávání příjmové selekce.“[95]

Bavíme-li se o masových médiích, je velice obtížné určit cílovou skupinu, a zda došlo k porozumění. Proto je nutné nahradit nepochybnou přítomnou pochybnostmi a to v případě, že je potřeba v rámci další komunikace uvnitř nebo vně systému masmédií pracovat se srozumitelností případně nesrozumitelností.

Toto vymezení se vztahuje na reálně plynoucí operace, týkající se reprodukce samotného systému a jeho diferenci vůči prostředí. Druhým smyslem, jakým můžeme pojímat realitu masových médií, je smysl toho, co se pro ni nebo skrze ni pro druhé jeví jako realita. Nyní je potřeba nahlížet na činnost masmédií jako na sekvence pozorování, přesněji: pozorujících operací.

---

[94] LUHMANN, N., *The Reality of the Mass Media.* 2. vyd. Stanford: Polity Press, s. 4. ISBN 0-8047-4076-3.
[95] LUHMANN, N. *Sociální systémy – nárys obecné teorie,* 1. vyd. Brno: CDK, 2006. s. 163. ISBN 80-7325-100-0.

„Abychom dospěli k pochopení masmédií, musíme pozorovat jejich pozorování. Pro smysl, který jsme nejprve představili, stačí pozorování prvního stupně, jako by se jednalo o fakta. Pro druhou možnost pochopení je potřeba zaujmout postoj pozorovatele druhého stupně, pozorovatel pozorovatelů.“[96]

Právě nyní nám dochází ke zdvojení reality v systému masových médií. Probíhá skutečná komunikace a zároveň komunikace prostřednictví něčeho jiného, případně prostřednictví samo sebe. Ustanovuje se nám zde rozlišení sebereference a reference druhého v systému.

„Masmédia jsou jakožto pozorující systémy nucené rozlišovat mezi sebereferencí a referencí jiného. Nemohou jinak. Nelze, aby jednoduše považovali sebe sama za pravdu. Musí konstruovat – na rozdíl od vlastní reality – ještě jinou realitu.“[97]

Výše zmíněné je důležité pro teorii poznání a konstruktivismus. V případě, že je veškeré poznání dosažitelné na základě diference sebereference a reference druhého, musí být veškeré poznání a realita konstrukcí. Tato diference se musí vždy nacházet v systému samém. Toto nás vede k příklonu k operativnímu konstruktivismu a jeho teorii poznání. V této teorii jde o to, že v rámci kognitivních systémů nelze rozlišit mezi podmínkami existence reálných objektů a podmínkami jejich poznání, protože nemáme přístup nezávislý na poznání k reálným objektům. Tento problém lze zredukovat na úrovni pozorování druhého stupně, tj. pozorování poznávacích procesů jiných systémů.

„Primární realita, ať ji poznání reflektuje, jak chce, se nenachází někde „venku ve světě“, nýbrž v samotných kognitivních operacích, protože ty jsou možné pouze na základě dvou podmínek, totiž jednak tak, že tvoří systém reprodukující sebe sama, a dále tak, že tento systém může pozorovat pouze tehdy, když rozlišuje mezi sebereferencí a referencí druhého.“[98]

Vzhledem k tomu, že operativní konstruktivismus sice nepopírá existenci vnějšího prostředí, ale považuje svět za nedosažitelný, existuje pouze jediná alternativa. Konstrukce reality, nebo pozorovat pozorovatele a to, jak konstruují realitu.

Toto má samozřejmě dopad i na problém terorismu, jako jisté formy anarchie. Terorismus můžeme zkoumat nikoliv z pohledu sebereference systému masových médií, ale vždy z pohledu druhého a toho, jak teroristé sami konstruují realitu a snaží se překročit hranice systému, opustit jej a vytvořit vlastní konstrukci reality a vlastní systém.

---

[96] LUHMANN, N., *The Reality of the Mass Media.* 2. vyd. Stanford: Polity Press, s. 9. ISBN 0-8047-4076-3.
[97] Tamtéž, s. 10
[98] Tamtéž, s. 11

„To, co je míněno „realitou“, může být proto jen vnitřním korelátem operací systému, která přísluší i objektům poznání a slouží k označování podle individuality nebo druhu. Realita tak není ničím jiným než indikátorem pro úspěšné ověřování konzistence v systému. Realita se utváří uvnitř systému na základě formování smyslu.“[99]

Produkce reality ve dvojím smyslu skutečně probíhá: pozorovatelné operace a těmito operacemi vytvářená realita společnosti můžou spolupůsobit společně s konstrukcí zvenčí. Sledovat to můžeme na vytváření reality o terorismu a kyberterorismu. V případě teroristických útoků jsou vždy zdůrazňovány počty obětí a nezapomíná se připomenout, že teroristy jsou islamisti, v převážné většině propojení s Al-Káidou. V rámci masmediální konstrukce reality kyberterorismu se nejčastěji referuje o ohrožení ekonomických statků, případně osobních dat, což může vést k „ukradení identity“ a velkému zásahu do našeho života.

Když se vrátím na začátek kapitoly, musím na závěr kapitoly uvést následující: Kyberterorismus má se sociální konstrukcí reality jednu společnou a jednu rozdílnou věc. Odvolává se na stejné výchozí podmínky sociální konstrukce, tzn. je programově konstruován. Druhou věcí je jeho odlišnost. Kyberterorismus pracuje především s tím, co A. Giddens nazývá reflexivní monitorování. Vyhodnocuje už interpretované události, a to zcela specifickým způsobem. Zatímco u Giddense jde o „praxi“ společenských disciplín, u kyberterorismu jde o latentní hrozbu, která se musí stát součástí obecného diskurzu. Je tedy ze své povahy čistě militárně invazivní, a to sociální konstrukce reality nepředpokládala.

[99] LUHMANN, N., *The Reality of the Mass Media.* 2. vyd. Stanford: Polity Press, s. 12. ISBN 0-8047-4076-3.

6. Přístupy a spolupráce mezinárodních organizací Evropské unie a NATO v oblasti boje proti kyberterorismu

Tato kapitola diplomové práce je zaměřena na problematiku mezinárodní spolupráce v oblasti boje proti kyberterorismu prostřednictvím vybraných nejvýznamnějších internacionálních organizací. Kyberterorismus lze obecně považovat za trestný čin, jehož definice se v právních systémech jednotlivých států mnohdy i zásadně liší. Významný problém představuje zejména odlišné definování základních terminologických pojmů. Bariérou jsou také jazykové odlišnosti, které napomáhají různorodým pojetím týkajících se kyberterorismu. Tato skutečnost může mít negativní vliv na přístupy a vzájemnou spolupráci organizací, které se snaží bojovat proti teroristickým hrozbám moderní doby – kyberterorismu. Obecně lze říci, že v důsledku závažnosti problematiky hrozícího kyberterorismu se jednotlivé organizace Evropské unie a Severoatlantické aliance snaží o uzavírání mezinárodních dohod s cílem podpory harmonizace a legislativy a aplikace standardizovaných postupů v boji proti kyberterorismu. [100] Do jaké míry je však tento soulad efektivně zajištěn, zůstává velmi diskutabilní tematikou.

6.1. Evropská unie

V rámci **Evropské unie** byla vypracována „**Strategie kybernetické bezpečnosti Evropské unie: Otevřený, bezpečný a chráněný kyberprostor**".

Tato *„ …strategie představuje vizi Evropské unie v oblasti kybernetické bezpečnosti, objasňuje úlohy a povinnosti a představuje opatření, jež jsou na základě silné a účinné ochrany a podpory práv občanů nutná k tomu, aby se online prostředí Evropské unie stalo nejbezpečnějším na světě"* [101]. Dle této strategie by se měla řídit politika kybernetické bezpečnosti v nejen v Evropské unii, ale také na mezinárodní úrovni.

Strategie kybernetické bezpečnosti Evropské unie *„ …se opírá o základní práva a svobody zakotvené v Listině základních práv Evropské unie a o základní hodnoty Evropské unie, včetně harmonizace s právními předpisy Evropské unie o ochraně údajů"*[102].

[100] PERL, R. Terrorist Use of the Internet: Threat, Issues, and Options for International Co-operation, *OSCE: Organization for Security and Co-operation in Europe* [online], 2008.
[101] Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, *Council of the European Union* [online], 2013.
[102] Tamtéž

K základním vizím této strategie patří následující priority:

- *„dosažení kybernetické odolnosti,*
- *výrazné omezení kyberkriminality,*
- *rozvoj politiky a kapacit kybernetické obrany v souvislosti se společnou bezpečnostní a obrannou politikou (SBOP),*
- *rozvoj průmyslových a technologických zdrojů pro kybernetickou bezpečnost,*
- *zavedení soudržné mezinárodní politiky Evropské unie týkající se kyberprostoru a podpora základních hodnot Evropské unie“* [103].

Pro dosažení výše uvedených vizí Strategie kybernetické bezpečnosti Evropské unie je definována řada opatření krátkodobého i dlouhodobého charakteru zahrnující množství politických nástrojů a různých subjektů v podobě orgánů Evropské unie, členských států nebo odvětví. V souladu s touto strategií byla vytvořena **politika bezpečnosti sítí a informací** (Síťový informační systém – anglicky Network Information system – NIS).

V roce 2004 byla zřízena **Evropská agentura pro bezpečnost sítí a informací** (**European Network and Information Security Agency – ENISA**), jejímž posláním je *„…dosažení vysoké a účinné úrovně bezpečnosti sítí a informací v rámci Evropské unie. Spolu s orgány Evropské unie a členských států usiluje o vytvoření kultury bezpečnosti sítí a informací ve prospěch občanů, spotřebitelů, podniků a organizací veřejného sektoru v Evropské unii“*[104].

Z dalších významných institucí zmiňovaných ve výše uvedené strategii lze jmenovat například **Computer Emergency Response Team** (**CERT-EU**). Jedná se o tým tvořený z *„…IT bezpečnostních odborníků z hlavních institucí Evropské unie (např. Evropské komise, generálního sekretariátu Rady, Evropského parlamentu, Výboru regionů, Hospodářského a sociálního výboru), který úzce spolupracuje s ostatními skupinami CERT v členských státech a s dalšími specializovanými IT bezpečnostními společnostmi“*[105].

Od ledna roku 2013 funguje také **Evropské centrum pro boj proti kyberkriminalitě** (**EC3**), jehož sídlem je Evropský policejní úřad (tedy ústředí Europolu) v nizozemském Haagu. Cílem tohoto centra je *„…chránit občany a podniky v Evropské unii před trestnou činností páchanou prostřednictvím internetu“*[106].

---

[103] Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, *Council of the European Union* [online], 2013.
[104] *European Network and information Security Agency (ENISA)* [online], 2013.
[105] *CERT-EU* [online], 2013.
[106] Evropské centrum pro boj proti kyberkriminalitě zahajuje činnost, *Evropská komise: Zastoupení v České republice* [online], 2013.

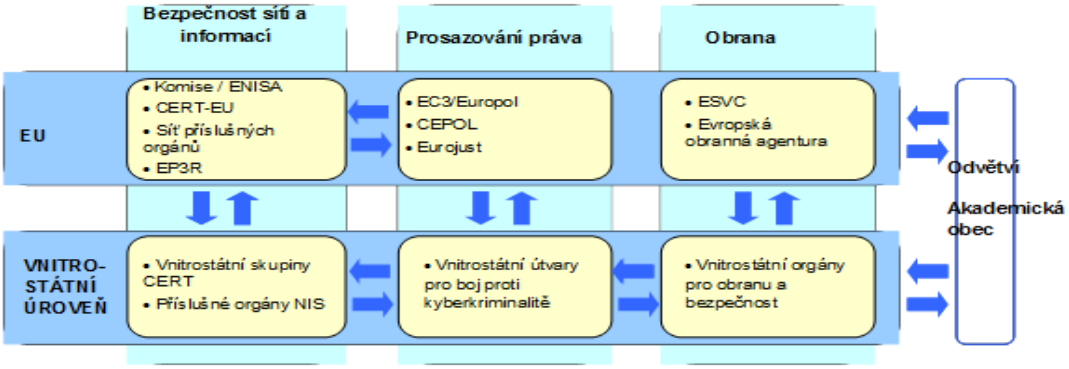
Důležitou úlohu v boji proti kyberterorismu v rámci Evropské unie zastává **Evropská policejní akademie** (**European Police College – CEPOL**). Tato instituce *„sdružuje vyšší policejní důstojníky evropských policejních sil, podporuje rozvoj sítě a přeshraniční spolupráci v boji proti trestné činnosti, udržuje veřejnou bezpečnost a veřejný pořádek v organizování vzdělávacích aktivit a výzkumných zjištění“*[107].

V souvislosti s kyberterorismem je úkolem Evropské policejní akademie *„…koordinace podoby a plánování kurzů, jež by měly pracovníky donucovacích orgánů vybavit znalostmi a odbornými poznatky pro účinný boj proti kyberkriminalitě“*[108].

V soudní oblasti spadá v rámci Evropské unie *„…vyšetřování kyberkriminality, koordinace mezi členskými státy a se třetími zeměmi, včetně podpory vyšetřování a stíhání kyberkriminality na operační i strategické úrovni, jakož i vzdělávací činnost v této oblasti“*[109] do kompetence **Jednotky Evropské unie pro justiční spolupráci** (**The European Union's Judicial Cooperation Unit – Eurojust**).

Lze uvést také činnosti **Evropské obranné agentury** (**European Defence Agency – EDA**), která posuzuje operační požadavky kybernetické ochrany Evropské unie a podporuje rozvoj odborníků a technologií Evropské unie týkající se kybernetické obrany (například v oblasti řízení, organizace, odborné přípravy, infrastruktury, dopravy apod.).[110] Komplexní řešení kybernetické bezpečnosti je dle Strategie kybernetické bezpečnosti Evropské unie uvedeno na obrázku 10 níže.

Obrázek 10: Zajištění komplexního řešení kybernetické bezpečnosti dle Strategie kybernetické bezpečnosti Evropské unie



Zdroj: Cybersecurity Strategy of the European Union: *An Open, Safe and Secure Cyberspace. Council of the European Union* [online] 2013 [cit. 2013-06-23]. Dostupné na www: <http://www.psp.cz/sqw/text/orig2.sqw?idd=175262>.

[107] *European Police College (CEPOL)* [online], 2013.
[108] Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, *Council of the European Union* [online], 2013.
[109] Tamtéž
[110] Tamtéž

Zjednodušeně lze tedy říci, že **spolupráce Evropské unie** je v oblasti kyberkriminality / kyberterorismu řešena na třech základních úrovních – na vnitrostátní úrovni, na úrovni Evropské unie a na úrovni mezinárodní. **Na vnitrostátní úrovni** se jedná o zajištění kybernetické odolnosti, kyberkriminality a obrany z hlediska členských států a jejich vnitrostátních subjektů. Velmi důležitá je však i vzájemná spolupráce a předávání informací mezi vnitrostátními subjekty jednotlivých členských států a soukromým sektorem. **Na úrovni Evropské unie** se jedná o spolupráci již zmiňované Evropské agentury pro bezpečnost sítí a informací (ENISA), Evropského centra pro boj proti kyberkriminalitě (EC3), Evropské obranné agentury, skupiny CERT-EU, Evropské policejní akademie a Eurojust.[111]

Mezinárodní úroveň v boji proti kyberkriminalitě / kyberterorismu je založena na vzájemné spolupráci níže uvedených organizací:

- Rada Evropy – Council of Europe – CE,
- Organizace pro hospodářskou spolupráci a rozvoj – Organisation for Economic Co-operation and Development – OECD,
- Organizace spojených národů – United Nations – OSN,
- Organizace pro bezpečnost a spolupráci v Evropě – Organization for Security and Cooperation in Europe – OBCE,
- Severoatlantická aliance – North Atlantic Treaty Organization – NATO.[112]

Evropská unie v oblasti boje proti kyberkriminalitě a kyberterorismu spolupracuje také se Sdružením národů jihovýchodní Asie (Association of South East Asian Nations – ASEAN), Organizací amerických států (Organization of American States – OAS) či s pracovní skupinou pro kybernetickou bezpečnost a kyberkriminalitu EU-USA. V souvislosti s bojem proti kyberkriminalitě / kyberterorismu lze zmínit také návrh směrnice Evropského parlamentu a Rady o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informací v Unii, který byl předložen společně s již uvedenou Strategií kybernetické bezpečnosti Evropské unie. Dle této směrnice musí být v členských státech Evropské unie zřízena skupina CERT. V souvislosti s obecným poskytováním informací a ochranou údajů, které také souvisí s tematikou kyberkriminality / kyberterorismu, lze uvést také **přehled stěžejních právních ustanovení, směrnic, nařízení, rozhodnutí**

[111] Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, *Council of the European Union* [online], 2013.
[112] Tamtéž

a dalších dokumentů Evropské unie upravujících tuto problematiku. K velmi důležitým **směrnicím Evropského parlamentu a Rady** patří:

- 98/48/ES, kterou se mění směrnice 98/34/ES o postupu při poskytování informací v oblasti norem a technických předpisů,
- 1999/5/ES o rádiových zařízeních a telekomunikačních koncových zařízeních a vzájemném uznávání jejich shody,
- 2000/31/ES o některých právních aspektech služeb informační společnosti, zejména elektronického obchodu, na vnitřním trhu („směrnice o elektronickém obchodu“),
- 2009/140/ES, kterou se mění směrnice 2002/21/ES o společném předpisovém rámci pro sítě a služby elektronických komunikací, směrnice 2002/19/ES o přístupu k sítím elektronických komunikací a přiřazeným zařízením a o jejich vzájemném propojení a směrnice 2002/20/ES o oprávnění pro sítě a služby elektronických komunikací,
- 2002/58/ES o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (Směrnice o soukromí a elektronických komunikacích),
- 2006/24/ES o uchovávání údajů vytvářených nebo zpracovávaných v souvislosti s poskytováním veřejně dostupných služeb elektronických komunikací nebo veřejných komunikačních sítí a o změně směrnice 2002/58/ES,
- 2008/114/ES o určování a označování evropských kritických infrastruktur a o posouzení potřeby zvýšit jejich ochranu. [113]

Z významných **nařízení Evropského parlamentu a Rady** lze jmenovat například nařízení č. 1007/2008, kterým se mění nařízení (ES) č. 460/2004 o zřízení Evropské agentury pro bezpečnost sítí a informací, pokud jde o období její činnosti nebo nařízení č. 1077/2011, kterým se zřizuje Evropská agentura pro provozní řízení rozsáhlých informačních systémů v prostoru svobody, bezpečnosti a práva.[114] Z **rozhodnutí Rady** lze uvést rozhodnutí č. 92/242/EHS o bezpečnosti informačních systémů či rozhodnutí č. 2011/292/EU o bezpečnostních pravidlech na ochranu utajovaných informací EU.[115]

Specifičtějšími předpisy Evropské unie vztahujícími se k problematice kyberkriminality / kyberterorismu jsou **dokumenty Komise Evropských společenství**:

- KOM/2006/251 Strategie pro bezpečnou informační společnost – „Dialog, partnerství a posílení účasti“,

[113] *EUR-Lex: Přístup k právu Evropské unie* [online], 2013.
[114] Tamtéž
[115] Tamtéž

- KOM/2006/688 Boj proti spamu a špionážnímu („spyware“) a škodlivému softwaru („malicious software“),
- KOM/2007/267 k obecné politice v boji proti počítačové kriminalitě,
- KOM/2009/149 o ochraně kritické informační infrastruktury - „Ochrana Evropy před rozsáhlými počítačovými útoky a narušením: zvyšujeme připravenost, bezpečnost a odolnost“,
- KOM/2011/163 o ochraně kritické informační infrastruktury - „Dosažené výsledky a další kroky: směrem ke globální kybernetické bezpečnosti“,
- KOM/2010/245 Digitální agenda pro Evropu,
- KOM/2010/673 Strategie vnitřní bezpečnosti Evropské unie: pět kroků směrem k bezpečnější Evropě,
- 2002/465/JHA o společných vyšetřovacích týmech,
- Usnesení rady 2002/C 43/02 o společném přístupu a zvláštních opatřeních v oblasti bezpečnosti sítí a informací,
- Usnesení Rady 2003/C 48/01 o evropském přístupu ke kultuře bezpečnosti sítí a informací,
- Rámcové rozhodnutí Rady 2005/222/SVV o útocích proti informačním systémům,
- 2009/C 62/05 o společné pracovní strategii a konkrétních opatřeních v oblasti boje proti počítačové trestné činnosti,
- Usnesení Rady 2009/C321/01 o společném evropském přístupu k bezpečnosti sítí a informací. [116]

V souvislosti s kyberkriminalitou / kyberterorismem lze uvést některé **dokumenty Rady Evropy**: Úmluva Rady Evropy č. 185 o kybernetické kriminalitě, Úmluva Rady Evropy č. 196 o prevenci terorismu, Doporučení Parlamentního shromáždění č. 1706 (2005) o médiích a terorismu a mnoho dalších.

6.2. Organizace Severoatlantické smlouvy

Organizace Severoatlantické smlouvy (**North Atlantic Treaty Organization – NATO**) vznikla na základě Severoatlantické smlouvy 4. 4. 1949 ve městě Washington. Smlouva byla podepsána celkem 12 nezávislými státy, kterým zaručovala vzájemnou pomoc v případě jejich napadení. Postupem času se k této smlouvě připojovaly další státy Evropy. V roce 1999 se k Severoatlantické smlouvě připojila také Česká republika.

[116] *EUR-Lex: Přístup k právu Evropské unie* [online], 2013.

V současnosti je členy této smlouvy celkem 26 států na evropském a severoevropském světadílu. Severoatlantická smlouva je dokumentem, který vychází z Charty Organizace spojených národů.

Cílem organizace NATO je zajištění bezpečnost všem členským státům při ozbrojených útocích, kterými se rozumí *„…ozbrojený zásah proti území členského státu a proti ostrovům nebo lodím či letadlům kterékoli smluvní strany v Atlantickém oceánu na sever od obratníku Raka“*[117].

S rozvojem dalších teroristických hrozeb rozšířila organizace NATO svou působnost. Na základě realizovaných masivních kyberútoků na Estonskou národní internetovo infrastrukturu, ke kterým došlo v roce 2007, byl roku 2008 v Bukurešti uskutečněn Summit NATO, kde byla přijata „**Politika v oblasti kybernetické obrany**“.[118]

O dva roky později se konal Summit v Lisabonu, kde byla přijata „**Lisabonská deklarace**“ týkající se rovněž kybernetické obrany.

Jedná se o *„…strategickou koncepci založenou na pružnější, schopnější a efektivnější schopnosti Severoatlantické aliance bránit své členské státy před celou řadou hrozeb, řídit i ty nejnáročnější krize a lépe spolupracovat s dalšími organizacemi a národy na podporu mezinárodní stability“*[119].

Cílem je také posílení kybernetické obranné schopnosti. V této deklaraci je v souvislosti s kyber hrozbami uvedeno: *„Kybernetické hrozby se neustále velmi rychle vyvíjí a zdokonalují. V zájmu NATO je zajištění stálého a neomezeného přístupu ke kyberprostoru a integrity svých kritických systémů, přičemž je nutno brát v úvahu kybernetické dimenze moderních konfliktů a zlepšit schopnosti detekce, hodnocení, prevence k obraně a následné obnově v případech, kdy mají kybernetické útoky na systémy zásadní význam pro Alianci. Snahou je také urychlení* ***Programu kyberobrany či vytvoření schopností k odvracení kyberútoků proti komunikačním a informačním systémům NATO (Computer Incident Response Capability – NCIRC****) do plné provozní způsobilosti. Pozornost je zaměřena obranným procesům plánování s cílem podpory rozvoje počítačových spojeneckých obranných schopností, pomoci jednotlivým spojencům na požádání, optimalizace sdílení informací, spolupráce a interoperability. Pro řešení bezpečnostních rizik vycházejících z kyberprostoru je nutno spolupracovat s dalšími aktéry*

[117] FOLTIN, P., ŘEHÁK, D. Mezinárodní spolupráce v boji proti terorismu, In *Obrana a strategie*, 2007, s. 60.
[118] HUGHES, Rex, *NATO and Cyber Defence: Mission Accomplished?* [online], 2009.
[119] Lisbon Summit Declaration, *NATO: North Atlantic Treaty Organization* [online], 2010.

– jako jsou Organizace spojených národů a Evropská unie. Sestavena je také Rada pro vývoj, jejímž úkolem je vypracování akčního plánu kybernetické obranné politiky"[120].

V červnu roku 2011 byl přijat **akční plán**, který je založen na koordinovaném přístupu k počítačové obraně celé aliance. Zaměřuje se na prevenci kybernetických útoků a zvyšování odolnosti. Všechny struktury NATO jsou začleněny do centralizované ochrany. V rámci této revidované kybernetické obranné politiky jsou rovněž stanoveny zásady NATO pro kybernetickou obrannou spolupráci s partnerskými zeměmi, mezinárodními organizacemi, soukromým sektorem a akademickou obcí. Kybernetická obrana je tak začleněna do **Národního procesu obranného plánování** (**NATO Defence Planning Process – NDPP**). V oblasti kybernetické obrany jsou v rámci Severoatlantické aliance zřízeny následující instituce:

- *„Poradní skupina NATO pro průmysl – NATO Industrial 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"* [121].

Obecně lze konstatovat, že spolupráce organizací Evropské unie a organizací Severoatlantické smlouvy je rozmanitá, avšak stále se hledají nové způsoby zefektivnění jejich vzájemné kooperace, aby kybernetická obrana byla co možná nejúčinnější.

6.3. Kybernetická bezpečnost ve vybraných zemích

Předchozí podkapitoly této diplomové práce byly zaměřeny na mezinárodní spolupráci významných organizací Evropské unie a Severoatlantické smlouvy v oblasti kybernetické bezpečnosti a v boji proti kyberkriminalitě / kyberterorismu. Tato podkapitola předkládané diplomové práce se zabývá vlivem zmiňovaných organizací na bezpečností politiky nejen jednotlivých členských států Evropské unie, ale také ostatních zemí v oblasti kybernetické bezpečnosti. Kybernetická bezpečnost je ve vybraných zemích zabezpečena zejména **skupinami CERT** (**Computer Emergency Response Team**):

[120] Lisbon Summit Declaration, *NATO: North Atlantic Treaty Organization* [online], 2010.
[121] Tamtéž

- **Belgie:**

Kybernetickou bezpečnost v Belgii zajišťuje skupina CERT.be[122], která je provozována belgickou sítí národního výzkumu BELNET[123]. V minulosti byla kybernetická bezpečnost zajišťována Federální veřejnou službou pro informační a komunikační technologie ve spolupráci s Belgickým institutem pro poštovní služby a telekomunikace (Belgian Institute for Postal Services and Telecommunications – BIPT).[124]

- **Dánsko:**

V Dánsku je kybernetická bezpečnost zabezpečována skupinou DK.CERT (Danish Computer Emergency Response Team)[125], která byla založena v roce 1991 dánským Centrem informačních technologií pro vývoj a výzkum. Toto centrum je národní organizací, která spadá pod Ministerstvo školství Dánska. V Dánsku působí také Danish GovCERT[126], který je řízen Ministerstvem obrany.

- **Estonsko:**

Kybernetická bezpečnost je v Estonsku zajištěna skupinou CERT-EE[127] spadající do gesce Ministerstva hospodářství a komunikací.

- **Litva:**

V Litvě působí skupina CERT-LT (Lithuanian National Computer Emergency Response Team)[128], která je provozována The Communications Regulatory Authority of the Republic of Lithuania[129].

- **Maďarsko:**

Maďarsko zajišťuje kybernetickou bezpečnost pomocí skupiny CERT-Hungary[130], která od roku 2010 funguje jako Centrum kybernetické bezpečnosti Maďarska.

- **Německo:**

Kybernetická bezpečnost v Německu je zajištěna skupinou CERT-BUND[131], která plní funkce vládního týmu.

---

[122] *CERT.be: The Federal Cyber Emergency Team* [online], 2013.
[123] *Belnet: Dedicated Connectivity* [online], 2013.
[124] *BIPT* [online], 2013.
[125] *DKCERT: Computer Security Incident Response Team* [online], 2013.
[126] *GovCERT: Center for Cybersikkerhed* [online], 2013.
[127] *CERT-EE* [online], 2013.
[128] Tamtéž
[129] *Communications Regulatory Authority of the Republic of Lithuania* [online], 2013.
[130] *CERT-Hungary* [online], 2013.
[131] *CERT-BUND* [online], 2013.

- **Norsko:**

V Norsku byl roku 2006 zřízen NorCERT[132], který je operačním oddělením Národního bezpečnostního úřadu Norska skládajícího se z Norského systému pro upozornění a brzké varování systémů digitální infrastruktury a Sekce pro Incident Handling.

- **Polsko:**

V Polsku pro zajištění kybernetické bezpečnosti funguje tým CERT.GOV.PL[133].

- **Rakousko:**

V Rakousku působí v rámci zajištění kybernetické bezpečnosti skupina CERT.at (Computer Emergency Response Team Austria**)[134].**

- **Spojené království:**

Kybernetická bezpečnost je ve Velké Británii řešena skupinou GovCertUK (Computer Emergency Response Team (CERT) for United Kingdom Government)[135].

- **Spojené státy americké:**

Ve Spojených státech amerických funguje US-CERT (US Computer Emergency Readiness Team)[136].

- **Španělsko:**

Ve Španělsku existuje několik skupin zajišťujících kybernetickou bezpečnost – například IRIS-CERT, CCN-CERT, INTECO-CERT, CESICAT, CSIRT-GV či ANDALUCIA-CERT.

Kybernetická bezpečnost je v některých vybraných zemích zajištěna také **prostřednictvím dalších institucí či organizací**:

- **Estonsko:**

V Estonsku bylo kromě skupiny CERT-EE v roce 2008 zřízeno NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) se statutem mezinárodní vojenské organizace, které je akreditováno, jako NATO Centre of Excellence.

- **Litva:**

Kybernetickou bezpečnost v Litvě dále zajišťuje Ministerstvo vnitra.

---

[132] *NorCERT* [online], 2013.
[133] *CERT.GOV.PL* [online], 2013.
[134] *CERT.at: Computer Emergency Response Team Austria* [online], 2013.
[135] GovCertUK, *CESG* [online], 2013.
[136] *US-CERT: United States Computer Emergency Readiness Team* [online], 2013.

- **Nizozemsko:**

V Nizozemí působí tým NCSC-NL (Nationaal Cyber Security Centrum)[137], který je pod záštitou Ministerstva bezpečnosti a spravedlnosti.

- **Slovensko:**

Slovenská republika zřídila v roce 2009 skupinu CSIRT.SK[138], která je harmonizovaná s její Národní strategií pro informační bezpečnost.

- **Spojené království:**

Jedná se o Ministerstvo obrany s Operační skupinou pro kybernetickou obranu spolupracující s Vládním velitelstvím pro komunikace, dále Středisko globálních operací a bezpečnostní kontroly, Centrum pro ochranu národní infrastruktury a Centrum sdílení informací (pro ochranu internetu).

- **Spojené státy americké:**

Existuje separátní jednotné kybernetické velitelství (US Cyber Command), které je podřízené hlavnímu US velitelství (US Strategic Command), jež sdílí řadu pravomocí s Ministerstvem pro národní bezpečnost (Department of Homeland Security – DHS). Dále se jedná o National Security Agency (NSA), která je součástí Ministerstva obrany.

- **Španělsko:**

Ve Španělsku je kromě výše uvedených CERT skupin také Národní kryptologické centrum (CCN) spadající pod Ministerstvo obrany. Toto centrum je součástí Národního zpravodajského centra, členem Vysoké rady pro elektronickou správu a Národního centra pro ochranu kritické infrastruktury.

Výše uvedené instituce a organizace zajišťující ve vybraných státech kybernetickou bezpečnost zpracovávají **celou řadu dokumentů** týkajících se boje proti kyberkriminalitě / kyberterorismu. Jedná se zejména o níže uvedené dokumenty:

- **Litva:**

Jedná se o dokument „Program rozvoje bezpečnosti elektronické informace (kybernetické bezpečnosti) na období 2011 – 2019“.

- **Německo:**

Německo má vypracovanou „Strategii pro kybernetickou bezpečnost“, jejímž základem je činnost Centra pro kybernetickou obranu, které podléhá Spolkovému úřadu pro informační bezpečnost a Rady kybernetické bezpečnosti.

[137] *NCSC: Nationaal Cyber Security Centrum* [online], 2013.
[138] *CSIRT.SK* [online], 2013.

- **Polsko:**

Jedná se o „Vládní program ochrany kyberprostoru Polské republiky v letech 2011 až 2016“.

- **Spojené království:**

Velká Británie schválila národní „Strategii kybernetické bezpečnosti do roku 2015“. Dále je na období 4 let vypracován „Národní program kybernetické bezpečnosti“ s rozpočtem 650 000 000 GBP.

- **Spojené státy americké:**

Ve Spojených státech amerických byl v roce 2009 zpracován strategický dokument „Cyberspace Policy Review“, v roce 2010 pak „Národně bezpečnostní strategie (NSS) a Obranná doktrína (QDR). V roce 2011 byly přijaty dokumenty: „National Strategy for Trusted Identities in Cyberspace (NSTIC)“, „International Strategy for Cyberspace“, „Defense Strategy for Cyberspace“ a „Quadrennial Homeland Security Review“.

7. Analýza dvou největších evropských konfliktů

7.1. Rusko-estonský konflikt

Z hlediska geografického prostoru, jak jsem jej vymezil na úvodu práce, je nejvýznamnějším konflikt, který se odehrál v dubnu roku 2007, při kterém Estonsko čelilo tři týdny trvajícím kybernetickým útokům. Událostí, jež vyvolala napětí mezi Estonskem a Ruskem, bylo rozhodnutí o přemístění sochy „rudoarmějce" připomínajícího porážku nacistů sovětskými vojsky během druhé světové války. Po odstranění sochy z centra Tallinnu, které se odehrálo 27. dubna, došlo k hromadným protestům etnických rusů žijících v Estonsku.[139] Vztahy mezi rusky mluvícími obyvateli a Estonci jsou značně problematické a jsou negativně ovlivněny historickými událostmi, které provázely připojení Estonska k Sovětskému svazu.

První vlna kybernetických útoků se odehrával mezi 28. – 30. dubnem. Jednalo se o nekoordinované útoky mající původ v Rusku. Estonská vláda obvinila z těchto útoků přímo Ruskou Federaci, ale zapojení ruských ozbrojených složek či oficiálních míst se nepotvrdilo. Jako útočníci byli nakonec označeni ruští hackeři.

Cílem kyberútoků byla kritická infrastruktura Estonska. Jednalo se o kybernetické útoky typu DoS[140]. Estonsku jako zemi se podařilo problematiku kyberútoků zveličit, neboť požádalo Severoatlantickou alianci, ve které je členem, o pomoc. Dle Severoatlantické smlouvy však kybernetické útoky nejsou považovány za ohrožení státu válečného charakteru. NATO na žádost Estonska o pomoc reagovala pozitivně. Do Tallinnu byl vyslán tým odborníků zaměřených na kyberterorismus, který měl prošetřit kyberútoky probíhající v Estonsku již po dobu 3 týdnů. Tallinnský vládní úřad z kyberútoků obvinil ruský Kreml, neboť bylo zjištěno, že napadení pocházejí z ruských IP adres (například moskevských bezpečnostních služeb).[141]

Motivacemi ke kyberútokům na estonskou infrastrukturu disponovala ruská vláda a další vládní agentury. Internetové stránky státních institucí v Estonsku byly přechodně nepřístupné. Přístup na tyto státní webové stránky byl možný pouze ze strany estonských poskytovatelů. Dle odborníků museli hackeři, kteří měli na svědomí probíhající

[139] Etničtí Rusové tvoří zhruba čtvrtinu všech obyvatel Estonska.
[140] Cyber Conflict Studies Association, Proceedings of the Annual Symposium, In *Implication for an Estonia-Like Cyber Conflict for the Government and the Private Sector*, 2008, s. 17 – 19.
[141] Tamtéž, s. 13 – 15.

kybernetické útoky, spolupracovat se státními institucemi, aby se jim podařilo ovládnout důležitou infrastrukturu Estonska.[142]

Tyto předpoklady o iniciativě ruské vlády o ochromení estonské infrastruktury se však nepotvrdily. K tomuto zjištění se dospělo na základě provedení analýzy probíhajících kyberútoků, které proběhly například ve Spojených státech amerických, v Brazílii, Kanadě či Vietnamu. Rovněž se dospělo ke skutečnosti, že realizace takto masivních kybernetických útoků na estonskou infrastrukturu by ze strany vládních agentur nebyla možná. Věcné důkazy však pro toto neexistují. Odborníci dále spekulovali, že takto intenzivní kybernetické útoky typu DoS by mohly být provedeny prostřednictvím několika separovanými hackery, bez pomoci státních institucí. Za kybernetické útoky na Estonsko byli zodpovědní hackeři z Ruska, kteří pro odstavení estonských státních a vládních internetových stránek využili botnetu.

Rusko-Estonský konflikt vyprovokovaný řadou kyberútoků znamenal množství důsledků. V Estonsku bylo v roce 2008 založeno Centrum pro výzkum kybernetických hrozeb a počítačovou obranu – Cooperative Cyber Defence Centre of Excellence (CCD COE). Jeho sídlem je město Tallinn. Jedná se o mezinárodní organizaci, která je zaměřena na boj proti kybernetickým hrozbám. Toto kybercentrum koordinuje počítačovou obranu v rámci členských zemí Severoatlantické aliance. Jeho úkolem je zlepšování spolupráce a posílení pozice NATO v boji proti kyberterorismu, včetně ustanovení právních hledisek obrany počítačů.[143] Další vizí kybercentra je zlepšení a zefektivnění vzájemné spolupráce mezi členskými zeměmi Severoatlantické aliance, včetně výměny informací mezi těmito státy, a to prostřednictvím vzdělání, výzkumu, vývoje či sdílení zkušeností v oblasti kyberútoků.

7.2. Rusko-gruzínský konflikt

Rusko-gruzínská válka o Jižní Osetii[144] je dalším příkladem využití kybernetických útoků. Přestože se daná oblast vymyká zkoumanému geografickému prostoru této práce, je rusko-gruzínský konflikt přínosný pro zkoumání kybernetického terorismu a využiji jej při komparaci s incidentem v Estonsku. V tomto regionu docházelo k narůstání napětí, které vyústilo 7. srpna 2008 v útok gruzínských ozbrojených sil proti separatistům. O den

[142] ASHMORE, William, *Impact of Alleged Russian Cyber Attacks* [online], 2009.
[143] Estonsko v přední linii boje proti kyberterorismu, *EU-Media, s. r. o.* [online], 2009.
[144] Jižní Osetie byla od roku 1991 autonomní oblastí ležící na hranicích s Ruskem, která však byla mezinárodně uznávána jako součást Gruzie.

později, tedy 8. srpna došlo k reakci Ruska, které vyslalo do Jižní Osetie své vojenské složky. Ještě před vpádem ruských vojsk byly spuštěny kybernetické útoky proti mnoha internetovým stránkám v Gruzii. V této případové studii se budu zabývat identifikací útočníků, technikami, které k útokům využili a důsledky těchto útoků na průběh konfliktu a život v Gruzii.

Ze zprávy, kterou vydala U.S. Cyber Consequences Unit (US-CCU) vyplývá, že: *„Kybernetické útoky proti gruzínským cílům byly podnikány civilisty s malou nebo žádnou účastí ze strany ruské vlády nebo armády.“* (US-CCU: 2009: 2)

Ruská armáda se sice prokazatelně nepodílela na samotných útocích, ale vzhledem k rychlosti, s jakou byly tyto útoky spuštěny a s přesností jejich zacílení dochází zpráva k závěru, že docházelo k jisté kooperaci mezi organizátory útoků a ruskými vojenskými silami. *„Kybernetické útoky začaly ve velkém měřítku těsně před začátkem operací ruských vojenských jednotek a skončily přesně s koncem těchto operací.“* (US-CCU: 2009: 6)

Vzhledem k situaci v regionu a k napětí v rusko-gruzínských vztazích, které se vyskytovalo již v minulosti, se nabízí domněnka, že scénář útoku byl připraven již v dřívějších letech. Útoky byly také podporovány ruským organizovaným zločinem. Jednou ze stránek, skrze kterou byly útoky organizovány a kde se také daly stáhnout programy k jejich provedení, byla stránka stopgeorgia.eu.

„Podle studie provedené Švédskou Univerzitou Národní Obrany, je stopgeorgia.ru spojena s různými kriminálními aktivitami, jako padělání pasů či krádeže kreditních karet.“ (Eneken Tikk a další: 2008: 13)

Mezi metody, které byly v tomto konfliktu použity, patří úprava internetových stránek a DDoS útoky. *„K útokům odmítnutí služby byly využity botnetové sítě a systémy comand and control, které náležely ruskému organizovanému zločinu. Botnetové sítě byly po celý průběh konfliktu používány k útokům na stejné stránky a nikdy nepřekročily počet jedenácti cílů.“* (US-CCU: 2009:4)

Naprostá většina těchto útoků byla provedena metodou SYN záplavy, která je značně sofistikovaná. Ze zprávy Arbor Networks vyplývá, že útoky byly vedeny s velkou intenzitou.

„Průměrné hodnoty provozu na komunikačních linkách v době útoku dosahovaly 211,66 Mbps a při nejsilnějším útoku bylo zaznamenáno dokonce 814,33 Mbps. Průměrná doba útoku se pohybovala okolo dvou hodin a nejdelší zaznamenaný útok trval šest hodin. Z těchto statistik můžeme usuzovat, že jakákoliv běžná internetová stránka by vůči nim byla zranitelná.“ (Azario: 2008)

„Cílem DDoS útoků byly nejen oficiální stránky gruzínské administrativy, ze kterých můžeme jmenovat stránky gruzínského prezidenta Michaila Saakashviliho, stránky gruzínského parlamentu a oficiální stránky Autonomní republiky Abcházie, která sousedí s Ruskem, ale také novinové internetové portály a stránky největšího bankovního ústavu v Gruzii.“ (Eneken Tikk a další: 2008: 8)

Napadeno bylo také největší hackerské fórum v Gruzii, což jednoznačně implikuje strach z kybernetické odpovědi ze strany gruzínských hackerů.

Defacementem, tedy úpravou internetových stránek byly postiženy stránky prezidenta Saakashviliho a stránky ministerstva zahraničí, na nichž byly shodně vyobrazena koláž prezidenta Saakasviliho a Adolfa Hitlera.[145] Domněnku, že se jednalo o pečlivě připravený útok, se kterým ruská strana počítala již dávno před vpádem svých vojsk do Jižní Osetie, potvrzuje analýza jedné upravené stránky.

US-CCU dochází k závěru, že: *„Nejméně jedna úprava stránek použitá v rusko-gruzínském konfliktu byla připravena nejméně dva roky před uskutečněním útoků. Technická analýza prokázala, že úprava stránky byla vytvořena již v březnu roku 2006, tedy v době, kdy vztahy mezi Gruzií a Ruskem byly napjaté.“* (US-CCU: 2009: 5)

Z výběru napadených cílů při kybernetických útocích vyplývá, že hlavní snahou útočníků bylo podpořit útočící ruské jednotky a znemožnit rychlou reakci gruzínské vlády proti vpádu ruské armády a znemožnit přísun informací o probíhajícím konfliktu na jedné straně gruzínským občanům, na straně druhé světovým médiím. Útoky měly také dopad na veřejné služby. Národní banka Gruzie vydala devátého září příkaz všem bankám zastavit poskytování elektronických služeb, které byly nepřístupné celých deset dní. Je pravdou, že kromě bankovního sektoru nebyla cílem útoků žádná složka kritické infrastruktury země, přestože dle US-CCU byla některá tato zařízení připojena na internet.

Z výše uvedeného vyplývá, že se jedná o jednoznačný případ kybernetického terorismu. Dle mého názoru je průkazné, že útoky byly vedeny s ideologickými cíli. Prvním cílem bylo podpořit akce ruské armády, které směřovaly k dosažení větší autonomie regionu Jižní Osetie. Úpravu prezidentských stránek v jejich rozsahu a konotacím, které vyplývají z přirovnávání Michaila Saakashviliho k Adolfu Hitlerovi, můžeme chápat jako snahu ovlivnit gruzínské veřejné mínění v jeho postoji k tomuto

[145] Koláž k vidění v DANCHEV, Dancho. *Coordinated Russia vs Georgia cyber attack in progress [online]* 11. srpna 2008 [cit. 2011-09-04]. Dostupné na www: <http://www.zdnet.com/blog/security/coordinated-russia-vs-georgia-cyber-attack-in-progress/1670>.

prezidentovi. Vzhledem k nezapojení ruské armády do těchto útoků můžeme vyloučit jejich zařazení do oblasti kybernetického warfaru.

8. Závěr

V této práci jsem pracoval s hypotézami, že kyberterorismus ač je latentní hrozbou, může se při zvýšení agresivity útoků stát reálnou hrozbou 21. století. Provedená analýza nám ukázala, že nebezpečí kyberterorismu spočívá v jeho latentní formě, na což nedokážou sociálně konstruované systémy reagovat. Můžeme tak říci, že kyberprostor, již nelze nadále považovat za místo svobodné výměny informací, ale prostor plný hrozeb, které jsou o to nebezpečnější právě proto, že jsou latentní a militantně invazivní.

Dále je nutno odpovědět na otázku, zda úspěšně proběhl proces sekuritizace v souvislosti s pojmem kyberterorismu. Výzkum ukázal, že sekuritizace proběhla na úrovni tajných služeb států a bezpečnostních složek, které jako takové nemůžeme pojímat za referenční objekty.

Cílem práce bylo dokázat, že masmédia záměrně konstruují realitu, která prezentuje kyberterorismus jako závažnou hrozbu. V práci jsem jednoznačně ukázal, že tomu tak je a skrze zdvojení reality dochází k definování kyberterorismu jako velmi nebezpečného jevu.

Seznam použité literatury

Publikace

1. BERGER, P. L./LUCKMANN, N. *Sociální konstrukce reality,* 1. vyd. Brno: CDK, 2001. 216 s. ISBN 80-85959-46-1.

2. BRZYBOHATÝ, M. *Terorismus I.* 2. vyd. Praha: Vydavatelství Police history, 1999. 141 s. ISBN: 80-902670-1-7.

3. BUZAN, B., WAEVER, O., DE WILDE, J. *Bezpečnost Nový rámec pro analýzu.* Brno: Barrister & Principal, 2005. 267 s. ISBN 80-903333-6-2.

4. DENNING, Dorothy. Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy. In *ARQUILLA, John, RONFELDT, David. Networks and Netwars: The Future of Terror, Crime, and Militancy*. RAND Corporation, 2001. 352 s. ISBN 978-0833030306.

5. DISTERER, Georg, ALLES, Ame, HERVATIN, Axel. Denial-of-Service (DoS) Attacks: Prevention, Intrusion Detection, and Mitigation. In *JANCZEWSKI, Lech, COLARIK, Andrew. Cyber Warfare and Cyber Terrorism*. Idea Group Inc (IGI), 2008. 532 s. ISBN 9781591409922.

6. DYTRT, Z., MIKULECKÝ, P., NEJEZCHLEBA, M., PRILLWITZ, G., ROUDNÝ, R. (editoři). *Etika podnikání a veřejné správy: Informační společnost – etická výzva pro 21. století.* Sborník z 2. mezinárodní konference, Hradec Králové, 18. – 20. 5. 1999. Praha: VUSTE ENVIS, 1999. 138 s. ISBN 80-902356-5-4.

7. EICHLER, J. *Terorismus a války na počátku 21. století.* Praha: Karolinum, 2007. 352 s. ISBN 978-80-246-1317-8

8. *Encyklopedie Světový terorismus od starověku až po útok na USA.* 1. vyd. Praha: Svojtka & Co., 2001. 536 s. ISBN 80-7237-340-4.

9. EVERARD, Paul. NATO and Cyber Terrorism. In *Responses to Cyber Terrorism*, 2008. 145 s. ISBN 978-1-58603-836-6.

10. FAIRCLOUGH, N. *Critical Discourse Analysis.* London: Longman, 1995. ISBN 0-582-21984-1.

11. FAIRCLOUGH, N. *Language and Power.* London: Longman Inc., 1989. ISBN 0-582-41483-0.

12. FOWLER, R. On critical linguistics. In CALDAS-COULTHARD, C. R., COULTHARD, M. *Text and Practices: Readings in Critical Discourse Analysis.* London: Routledge, 1996, s. 3 − 14. ISBN 0-415-12143-4.

13. HOFFMAN, Bruce. *Inside Terrorism*. Columbia University Press, 2006. 432 s. ISBN 9780231510462.

14. JANCZEWSKI, Lech, COLARIK, Andrew. *Managerial Guide For Handling Cyber-Terrorism And Information Warfare*. Idea Group Inc (IGI), 2005. 229 s. ISBN 9781591405498.

15. JIROVSKÝ, Václav. *Kybernetická kriminalita: Nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha: Grada, 2007. 284 s. ISBN 978-80- 247-1561-2.

16. KLIMEŠ, L. *Slovník cizích slov*. Praha: SPN, 1998. 864 s. ISBN 80-7235-023-4.

17. KUSHNER, Harvey. *Encyclopedia of Terrorism*. SAGE Publications, 2003. 523 s. ISBN 9780761924081.

18. LAQUEUR, Walter. *No End to War: Terrorism in the Twenty-First Century*. Continuum International Publishing Group, 2003. 288 s. ISBN 9780826414359.

19. LAQUEUR, Walter. *The New Terrorism: Fanaticism and the Arms of Mass Destruction*. Oxford University Press, 2000. 312 s. ISBN 9780195140644.

20. LUHMANN, N. *Sociální systémy – nárys obecné teorie,* 1. vyd. Brno: CDK, 2006. 550 s. ISBN 80-7325-100-0.

21. LUHMANN, N., *The Reality of the Mass Media.* 2. vyd. Stanford: Polity Press, ISBN 0-8047-4076-3.

22. MCQUADE III, Samuel. *Encyclopedia of Cybercrime*. Westport: Greenwood, 2008. 232 s. ISBN 978-0313339745.

23. MIKA, O. *Současný terorismus.* Praha: Nakladatelství Triton, 2003. 92 s. ISBN: 80-7254-409-8.

24. MEYER, M. Between theory, method, and politics: positioning of the aproaches to CDA. In Wodak, R. MEYER, M. *Methods of Critical Discourse Analysis.* London: Sage, 2001. 201 s. ISBN 0-7619-6154-2.

25. ÖZEREN, S. *Response to Cyber Terrorism*. Amsterdam: IOS Press, 2008. Cyberterrorism and International Cooperation: General Overview of the Available Mechanisms to Facilitate an Overwhelming Task, s. 161. ISBN 9781607503118.

26. San Francisco Chronicle, 23. května 1996. In: BUZAN, B., WAEVER, O., DE WILDE, J.. *Bezpečnost: Nový rámec pro analýzu*. 1. vyd. Brno: Barrister & Principal, 2005. s. 36. ISBN 80-903333-6-2.

27. SEDLÁČKOVÁ, L. *Islám v médiích.* Liberec: Nakladatelství Bor, 2010. 123 s. ISBN 978-80-86807-65-2.

28. SOULEIMANOV, Emil. *Terorismus: Pokus o porozumění*. Praha: Slon, 2011. 354 s. ISBN 978-80-7419-038-4.

29. STRMISKA, Maxmilián. *Terorismus a demokracie: Pojetí a typologie subversivního teroristického násilí v soudobých demokraciích*. Brno: Masarykova univerzita, 2001. 102 s. ISBN 80-210-2755-X.

30. VAN DIJK, T. Critical Discourse Analysis. In TANNEN, D., SCHIFFRIN, D., HAMILTON, H. *Handbook of Discourse Analysis.* Oxford: Blackwell, 2001. 371 s. ISBN 0-631-20595-0.

31. WODAK, R. The discourse-historical approach. In WODAK, R., MEYER, M. *Methods of Critigal Discource Analysis.* London: Sage, 2001. 201 s. ISBN 0-7619-6154-2.

Časopisy

32. Cyber Conflict Studies Association. Proceedings of the Annual Symposium. In *Implication for an Estonia-Like Cyber Conflict for the Government and the Private Sector*. Washington: Georgetown University, 2008.

33. FOLTIN, Pavel, ŘEHÁK, David. Důvody realizace a formy terorismu. In *Obrana a strategie*, 2006, s. 33 – 41. ISSN 1214-6463.

34. FOLTIN, Pavel, ŘEHÁK, David. Historický vývoj terorismu. In *Obrana a strategie*, 2006, s. 45 – 60. ISSN 1214-6463.

35. FOLTIN, Pavel, ŘEHÁK, David. Mezinárodní spolupráce v boji proti terorismu. In *Obrana a strategie*, 2007, s. 57 – 78. ISSN 1214-6463.

36. HOMOLÁČ. J. Diskurz o migraci Romů na příkladu internetových diskusí. *Sociologický časopis*, 2006, roč. 42, č. 2, s. 329.

37. MOGHADDAM, Fathali. The Staircase to Terrorism: A Psychological Exploration. In *American Psychologist*, Vol 60 (2), 2005, p. 161 – 169. ISSN 0003-066X.

Elektronické zdroje

38. ANTAKI, Ch. *Analysing Talk and Text. A Course for the Universidad Autónoma de Barcelona* [online] [cit. 2013-06-13]. Dostupné z: http://www.staff.lboro.ac.uk/~ssca1/tthome.htm.

39. ASHMORE, William. *Impact of Alleged Russian Cyber Attacks* [online] 2009 [cit. 2013-06-23]. Dostupné z: http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA504991.

40. *Belnet: Dedicated Connectivity* [online] 2013 [cit. 2013-06-23]. Dostupné z: http://www.belnet.be/.

41. *BIPT* [online] 2013 [cit. 2013-06-23]. Dostupné z: http://ibpt.be/en/1/Home/Home/Home.aspx.

42. *CERT.at: Computer Emergency Response Team Austria* [online] 2013 [cit. 2013-06-23]. Dostupné z: http://www.cert.at/.

43. *CERT.be: The Federal Cyber Emergency Team* [online] 2013 [cit. 2013-06-23]. Dostupné z: https://www.cert.be/.

44. *CERT-BUND* [online] 2013 [cit. 2013-06-23]. Dostupné z: https://www.cert-bund.de/.

45. *CERT-EE* [online] 2013 [cit. 2013-06-23]. Dostupné z: http://www.cert.ee/.

46. *CERT-EU* [online] 2013 [cit. 2013-06-23]. Dostupné z: http://cert.europa.eu/cert/plainedition/en/cert_about.html.

47. *CERT.GOV.PL* [online] 2013 [cit. 2013-06-23]. Dostupné z: http://www.cert.gov.pl/.

48. *CERT-Hungary* [online] 2013 [cit. 2013-06-23]. Dostupné z: http://www.cert-hungary.hu/.

49. *CERT-LT* [online] 2013 [cit. 2013-06-23]. Dostupné z: https://www.cert.lt/.

50. *Communications Regulatory Authority of the Republic of Lithuania* [online] 2013 [cit. 2013-06-23]. Dostupné z: http://www.rrt.lt/en/home.html.

51. *CSIRT.SK* [online] 2013 [cit. 2013-06-23]. Dostupné z: http://www.csirt.gov.sk/.

52. CSIRT.CZ: Incident handling statistics. *CSIRT.CZ* [online] 2013 [2013-06-21]. Dostupné z: http://csirt.cz/files/csirt/statistics/stats.html.

53. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. *Council of the European Union* [online] 2013 [cit. 2013-06-23]. Dostupné z: http://www.psp.cz/sqw/text/orig2.sqw?idd=175262.

54. *Česká národní skupina mezinárodní federace hudebního průmyslu* [online] 2013 [cit. 2013-06-25]. Dostupné z: http://www.ifpicr.cz/.

55. *Česká televize* [online] 2013 [cit. 2013-06-25]. Dostupné z: http://www.ceskatelevize.cz/.

56. Další útok hackerů v ČR: Terčem internetové bankovnictví velkých bank, ČNB i web burzy. *Patria Online, a. s.* [online] 2013 [cit. 2013-06-25]. Dostupné z: http://www.patria.cz/zpravodajstvi/2282801/dalsi-utok-hackeru-v-cr-tercem-internetove-bankovnictvi-velkych-bank-cnb-i-web-burzy.html.

57. DANCHEV, Dancho. *Coordinated Russia vs Georgia cyber attack in progress [online]* 11. srpna 2008 [cit. 2011-09-04]. Dostupné na www: http://www.zdnet.com/blog/security/coordinated-russia-vs-georgia-cyber-attack-in-progress/1670.

58. DENNING, D. E. *Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy* [online]. [Cit. 2013-05-14]. Dostupné na www: <http://www.nautilus.org/infopolicy/workshop/papers/deinning.html>.

59. DENNING, Dorothy. *Cyberterrorism. Georgetown University* [online] 2000 [cit. 2013-06-17]. Dostupné z: http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html.

60. Denial of Service Attacks. *CERT* [online] 2013 [cit. 2013-06-20]. Dostupné z: http://www.cert.org/tech_tips/denial_of_service.html.

61. *DKCERT: Computer Security Incident Response Team* [online] 2013 [cit. 2013-06-23]. Dostupné z: https://www.cert.dk/.

62. *Dopravní podnik hlavního města Prahy* [online] 2013 [cit. 2013-06-25]. Dostupné z: http://www.dpp.cz/.

63. Estonsko v přední linii boje proti kyberterorismu. *EU-Media, s. r. o.* [online] 2009 [cit. 2013-06-23]. Dostupné z: http://www.euractiv.cz/bezpecnost-a-spravedlnost0/clanek/estonsko-v-predni-linii-boje-proti-kyberterorismu-005855.

64. *EUR-Lex: Přístup k právu Evropské unie* [online] 2013 [cit. 2013-06-23]. Dostupné z: http://eur-lex.europa.eu/cs/index.htm.

65. *European Network and information Security Agency (ENISA)* [online] 2013 [cit. 2013-06-23]. Dostupné z: http://www.enisa.europa.eu/about-enisa.

66. *European Police College (CEPOL)* [online] 2013 [cit. 2013-06-23]. Dostupné z: https://www.cepol.europa.eu/index.php?id=about-cepol.

67. *Europol* [online] 2013 [cit. 2013-06-17]. Dostupné z: https://www.europol.europa.eu/search/apachesolr_search/Te-sat%20(Te-Sat%202010,2011,2012).

68. *Evropské centrum pro boj proti kyberkriminalitě zahajuje činnost. Evropská komise: Zastoupení v České republice* [online] 2013 [cit. 2013-06-23]. Dostupné z: http://ec.europa.eu/ceskarepublika/press/press_releases/13_13_cs.htm.

69. *Exekutorská komora České republiky* [online] 2013 [cit. 2013-06-25]. Dostupné z: http://www.ekcr.cz/.

70. FAIRCLOUGH, N. *Critical discourse analysis. Marges Linquistiques* [online] [cit. 2013-06-13]. Dostupné z: http://www.ling.lancs.ac.uk/profiles/236/.

71. FOLTIN, P., ŘEHÁK, D. *Důvody realizace a formy terorismu. Strategie a obrana* [online] 2005, č. 1 [cit. 2013-05-13]. Dostupné na www: http://www.defenceandstrategy.eu/cs/archiv/rocnik-2005/1-2005/duvodyrealizace-a-formy-terorismu.html.

72. FRANK, L. *Analýza a predikce bezpečnostních hrozeb a rizik v České republice* [online] 2006 [cit. 2011-01-05]. Dostupné z: http://is.muni.cz/th/16735/fss_d/disertace_frank.pdf.

73. GANOR, Boaz. Defining Terrorism: Is One Man´s Terrorist Another Man´s Freedom Fighter? *ICT - International Institute for Counter-Terrorism* [online] 1998 [cit. 2013-06-16]. Dostupné z: http://www.ict.org.il/ResearchPublications/tabid/64/Articlsid/432/Default.aspx.

74. *GovCERT: Center for Cybersikkerhed* [online] 2013 [cit. 2013-06-23]. Dostupné z: http://fe-ddis.dk/cfcs/opgaver/govcert/Pages/default.aspx.

75. GovCertUK. *CESG* [online] 2013 [cit. 2013-06-23]. Dostupné z: http://www.cesg.gov.uk/policyguidance/GovCertUK/Pages/index.aspx.

76. HALLER, Martin. Denial of Service útoky: reflektivní a zesilující typy. *Lupa.cz* [online] 2006 [cit. 2013-06-20]. Dostupné z: http://www.lupa.cz/clanky/denial-of-service-utoky-reflektivni-a-zesilujici-typy/.

77. HUGHES, Rex. *NATO and Cyber Defence: Mission Accomplished?* [online] 2009 [cit. 2013-06-23]. Dostupné z: http://www.carlisle.army.mil/DIME/documents/NATO%20and%20Cyber%20Defence.pdf.

78. Inflow. *Kyberterorismus v informační společnosti* [online] [cit. 2013-05-14]. Dostupné na www: http://www.inflow.cz.

79. *Intergram: Nezávislá společnost výkonných umělců a výrobců zvukových a zvukově obrazových záznamů o. s.* [online] 2013 [cit. 2013-06-25]. Dostupné z: http://www.intergram.cz/cs/.

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

81. JIROVSKÝ, Václav. *Kyberterorismus* [online] 2006 [cit. 2013-06-17]. Dostupné z: www.as4u.cz/filemanager/files/file.php?file=3990.

82. JIROVSKÝ, V. *Společnost ve virtuálním svě*tě. Konference CYTER [online] 2010, č. 01 [cit. 2013-05-14]. Dostupné z: https://cythres.fd.cvut.cz/cyter2010/cs/presentation.php.

83. Koncept politického kyber-terorismu. *Rexter* [online] 2012 [cit. 2013-06-17]. Dostupné z: http://www.rexter.cz/koncept-politickeho-kyber-terorismu/2002/11/01/.

84. *KSČM Brno* [online] 2009 [cit. 2013-06-25]. Dostupné z: http://www.kscm-brno.cz/.

85. KUŽEL, Stanislav. Kybernetická kriminalita I: Co se děje v kyberprostoru. *BusinessIT.cz* [online] 2012 [cit. 2013-06-17]. Dostupné z:

http://www.businessit.cz/cz/kyberneticka-kriminalita-i-co-se-deje-v-kyberprostoru.php.

86. Lisbon Summit Declaration. *NATO: North Atlantic Treaty Organization* [online] 2010 [cit. 2013-06-23]. Dostupné z: http://www.nato.int/cps/en/natolive/official_texts_68828.htm#cyber.

87. *NCSC: Nationaal Cyber Security Centrum* [online] 2013 [cit. 2013-06-23]. Dostupné z: https://www.ncsc.nl/.

88. Nebezpečné komunikační praktiky: Co je hoax. *E-bezpečí* [online] 2008 [cit. 2013-06-23]. Dostupné z: http://www.e-bezpeci.cz/index.php/temata/hoax-spam/91-25.

89. *NorCERT* [online] 2013 [cit. 2013-06-23]. Dostupné z: https://www.nsm.stat.no/Arbeidsomrader/Internettsikkerhet-NorCERT/.

90. *ODS: Občanská demokratická strana* [online] 2013 [cit. 2013-06-25]. Dostupné z: http://www.ods.cz/.

91. *OSA* [online] 2011 [cit. 2013-06-25]. Dostupné z: http://www.osa.cz/.

92. Patria online, a.s. Zpravodajství [online] 2013 [cit. 2013-06-21]. Dostupné z: <http://www.patria.cz/zpravodajstvi/zpravy.html>.

93. PAUKERTOVÁ, Veronika. Úvod do problematiky elektronické informační kriminality. *Ikaros: Elektronický časopis o informační společnosti* [online] 2006 [cit. 2013-06-20]. Dostupné z: http://www.ikaros.cz/elektronicka-informacni-kriminalita.

94. PERL, Raphael. Terrorist Use of the Internet: Threat, Issues, and Options for International Co-operation. *OSCE: Organization for Security and Co-operation in Europe* [online] 2008 [cit. 2013-06-23]. Dostupné z: http://www.osce.org/atu/31428.

95. *Poslanecké sněmovny Parlamentu České republiky* [online] 2013 [cit. 2013-06-25]. Dostupné z: http://www.psp.cz/sqw/hp.sqw.

96. *Registr vozidel republiky* [online] 2011 [cit. 2013-06-25]. Dostupné z: http://www.registr-vozidel.cz/.

97. Rekapitulace (D)DOS útoků ze dnů 4. 3. – 7. 3. *CZ.NIC: Správce domény CZ* [online] 2013 [cit. 2013-06-25]. Dostupné z: http://csirt.cz/files/csirt/Rekapitulace-utoky-20120311.pdf.

98. *Retn.Net* [online] 2013 [cit. 2013-06-25]. Dostupné z: http://www.retn.net/en/.

99. Understanding Denial-of-Service Attacks. *US-CERT: United States Computer Emergency Readiness Team* [online] 2013 [cit. 2013-06-20]. Dostupné z: http://www.us-cert.gov/ncas/tips/ST04-015.

100. *US-CERT: United States Computer Emergency Readiness Team* [online] 2013 [cit. 2013-06-23]. Dostupné z: http://www.us-cert.gov/.

101. VAN DIJK, T. *Discourse and Racism* [online] 2013 [cit. 2013-06-13]. Dostupné z: http://www.discourses.org//OldArticles/Discourse%20and%20racism.pdf.

102. VESELÍK, Patrik. Weby nové maturity čelí útoku hackerů dnes, v době písemek. *FLOPS Magazín pro IT profesionály* [online] 2013 [cit. 2013-06-25]. Dostupné z: http://www.flops.cz/aktuality/celi-weby-nove-maturity-den-pred-pisemkami-take-utoku-hackeru.

103. VAŠÁT, P. *Kritická diskurzivní analýza: sociální konstruktivismus v praxi* [online] 2013 [cit. 2013-06-13]. Dostupné z: http://www.caat.cz.

104. *Vláda České republiky* [online] 2013 [cit. 2013-06-25]. Dostupné z: http://www.vlada.cz/.

105. Wikipedia – the Free Encyclopedia. *Kyberprostor [*online] 2013 [cit. 2013-05-14]. Dostupné z: http://en.wikipedia.org/wiki/Cyberspace.

106. WODAK, R. *What Is Critical Discourse Analysis?* [online] 2013 [cit. 2013-06-13]. Dostupné z: http://www.qualitative-research.net/index.php/fqs/article/view/255/562.

Seznam obrázků

Seznam tabulek