TRENDY A PERSPEKTIVY BEZPEČNOSTI

Bc. Jakub Drmola

Konceptualizace kyberterorismu

Vojenské rozhledy, 2013, roč. 22 (54), č. 2, s. 94–102, ISSN 1210-3292

The Conceptualization of Cyberterrorism

Abstrakt:

Cílem této práce je za pomoci dostupných dokumentů, zpráv a odborných textů vymezit fenomén kyberterorismu a zhodnotit jeho roli a výskyt v současném světovém dění. Kyberterorismus je dnes sice velice často diskutovaným jevem, ale jakýkoliv konsenzus ohledně jeho přesného vymezení zatím neexistuje. Kritika současného stavu je shrnuta v závěrečné kapitole, která popisuje příčiny současného stavu, tedy stavu, kdy je kyberterorismus často diskutován, politizován, je opakována jeho nebezpečnost, aniž by k němu v praxi docházelo.

Abstract:

The purpose of this paper is to define cyberterrorism phenomenon with the use of available documents, reports, and expert texts, and to evaluate its role and occurrence in contemporary world's events. The cyberterrorism is very often discussed nowadays, but there is a total lack of any consensus as far as a precision definition is concerned. The critique of current state is summarized at the end of the final chapter, describing leading causes of present situation, i.e. a situation when the cyberterrorism is discussed, politicised, all repeatedly underline its dangerousness, but in practice no cyber attack has occurred.

Klíčová slova:

Konceptualizace, kyberterorismus, elektronický útok, hacker, hackerské komunity, sběr informací, kybernetická kriminalita, průmyslová špionáž.

Key words:

Conceptualization, cyberterrorism, electronic attack, hacker, hackerspace communities, data collection, cyber criminality, industrial espionage.

1. Úvod

Počáteční kapitola se zabývá stručným popisem současného, nutno dodat velice nepříliš dobrého stavu konceptualizace kyberterorismu se zaměřením na situaci v České republice. Následujícím krokem je samotná konceptualizace na základě vybraných definic. Součástí je také zdůraznění klíčových parametrů či vlastností, které by kyberterorismus měl naplňovat. Další kapitola se zabývá popisem některých elektronických útoků, které bývají za kyberterorismus označovány, ale selhávají naplnit jeden či více

definičních parametrů předložených v následující kapitole. Výsledkem má být mnohem užší ohraničení tohoto prozatím nesystematicky užívaného konceptu, a to včetně vyloučení mnoha evidentně „neteroristických“ forem činnosti (přestože ilegálních, elektronických a oběti poškozujících).

2. Současný stav

Jedním z prvních kroků vstříc konceptualizaci kyberterorismu by mohlo být prohlédnutí materiálů publikovaných vládními orgány a institucemi, které se touto problematikou zabývají. Pokusíme-li se nalézt informace o kybernetickém terorismu například na stránkách Ministerstva vnitra České republiky, [1] nedozvíme se prakticky vůbec nic. V několika odstavcích jsou zmiňovány snahy Ruské federace a Čínské lidové republiky o rozvoj jejich kapacit k vedení elektronické války, je popsána pozice USA a Pentagonu, a zmíněni jsou i „bezskrupulózní hackeři“ prodávající informace komukoliv, kdo je zaplatí. Kritizována je volná dostupnost návodů na výrobu výbušnin na internetu a vliv médií, která popularizují požadavky teroristů. O tom co je to vlastně „kybernetický terorismus“ (což je název článku) se zde bohužel nehovoří vůbec nic.

Podobně neúspěšně bychom vysvětlení kyberterorismu hledali i v dalších dokumentech, které se o terorismu a kybernetických hrozbách zmiňují, např. Strategie boje proti terorismu [2] nebo Bezpečnostní strategie České republiky 2011. [3] Jistou útěchu nabízí až Výkladový slovník kybernetické bezpečnosti z roku 2012, [4] který zdůrazňuje snahu vyvolat strach.

V odborné literatuře je situace obdobná a např. Janoušek [5] sice rozlišuje mezi devíti typy „kyberteroristů“, ale řadí mezi ně i finančně či pomstou proti svému zaměstnavateli motivované zločince a hackery, tj. v zásadě téměř každý, kdo podnikne nějaký elektronický útok, je podle něj kyberteroristou. I Jirovský ve své monografii [6] k vymezení kyberterorismu přistupuje velmi vágně a ve výsledku do takového nejasně ohraničeného konceptu může spadnout úplně cokoliv. Někdy je za kyberterorismus pokládáno i užívání informačních a komunikačních technologií k podpoření činnosti již známých „standardních“ teroristických skupin. Tím je myšlena zejména propaganda, rekrutace, komunikace členů, šíření návodů, apod. [7] Zcela zbytečné by bylo hledat jasnou odpověď i v médiích, která také obvykle nejsou schopna rozlišit mezi kyberterorismem a útoky motivovanými prostým finančním obohacení.

Situace není o nic utěšenější ani mimo Českou republiku. Z celého spektra lze uvést několik příkladů: Lieberman [8] považuje i běžný *malware* za formu terorismu. Velmi široké spektrum „kyberterorismu“ popisuje i Saint-Claire. [9]

William Tafoya [10] z FBI varuje před kontinuální snahou teroristů provést kyberútok. Jarvis [11] mezitím mapuje tento rozpor mezi přístupem FBI a akademickou sférou. Velmi skepticky se k hrozbě kyberterorismu staví Green, [12] zatímco Cavelty [13] celý problém vidí jako hlavně institucionální a zkoumá americkou vnitropolitickou debatu o této problematice. Proti příliš širokému konceptu se staví i autoři pod hlavičkou Symantecu [14] a rovnou nabádají přistupovat ke kyberterorismu analogicky s „hmotným” terorismem. Významným autorem a propagátorem kybernetické bezpečnosti (války i terorismu) je Richard Clarke [15] bývalý člen americké národní bezpečnostní rady, který se po roce 2001 stal jedním z hlavních hlasů varujících před „digitálním Pearl Harborem”. Vzhledem k absenci jakýchkoliv dramatických teroristických kyberútoků

po 11. září 2001 (9/11 attacks) a pod vlivem rostoucích aktivit Číny jsou v posledních letech tato varování slyšet spíše ohledně mezistátní kybernetické války. I k této možnosti se ale někteří [16] staví skepticky.

Přestože je tedy kyberterorismus velice hojně diskutovaný fenomén, jeho vymezení se jeví jako ještě problematičtější než vymezení terorismu samotného. Běžně lze nalézt míšení s finanční kriminalitou, průmyslovou špionáží, kybernetickými operacemi na podporu mezistátních válek atd. [17]

3. Konceptualizace

V odborné diskuzi je tak patrná jakási dvojkolejnost. Jedna skupina autorů a odborníků považuje za „kybernetický terorismus" široké spektrum aktivit, které zpravidla alespoň nějak souvisí s terorismem nebo kyberprostorem. Jedná se tak o aktivity velmi různorodé a často velice vzdálené od terorismu samotného. Druhá skupina se naopak snaží kyberterorismus co nejpřesněji vymezit a zabránit dalšímu rozmělňování již nyní velmi abstraktních konceptů.

Tento text vychází z užšího pojetí a považuje za evidentní, že kyberterorismus musí být speciálním případem: *podmnožinou terorismu* obecně. Konkrétně je to takový poddruh terorismu, který je páchán za pomoci informačních a komunikačních technologií. Předložka „kyber-" vypovídá o povaze útoku, nikoliv o aktérech, jejich způsobu komunikace nebo o jejich cílech a motivacích. V zásadě se jedná o pojem na stejné úrovni jako by byl například „letecký terorismus", „sebevražedný terorismus" nebo „bombový terorismus". Při konceptualizaci kyberterorismu rozhodně nelze zapomenout na to, že každá definice a každý případ kyberterorismu musí zároveň spadat i pod obecnější definici terorismu samotného. Tento základní předpoklad vyjádřila i Dorothy Denning [18, 36] svojí definicí, kterou lze zařadit do definic následujících tradici Alexe Schmida. [19] Tyto dvě definice tak tvoří základ konceptualizace kyberterorismu i z pohledu tohoto textu.

V následující podkapitole jsou stručně shrnuty dílčí aspekty a znaky vyplývající z těchto definic, které pomohou lépe ohraničit kyberterorismus a odlišit jej jak od ostatních forem terorismu, tak i od ostatních forem kybernetických útoků. Rozděleny jsou podle motivace útočníků. Je také nutné předem upozornit na to, že tyto skupiny rozhodně nelze považovat za jasně vytyčené, nepřekrývající se, a v praxi jednoznačně určitelné. Jedná se tak spíše o jakousi ideální typologii.

3.1 Znaky

3.1.1 Cíl

Cílem lze myslet zejména konečný záměr, se kterým byl kyberteroristický útok proveden. Zde lze ze zmíněných definic poměrně jednoznačně vyvodit, že cílem je spíše politická změna a ideologická propaganda než finanční profit či přímé oslabení vojenských kapacit protivníka. Za jisté výjimky z tohoto pravidla lze považovat kriminální a psychopatologický terorismus.

Důležitou charakteristikou je také možnost rozlišit tzv. cílové publikum od přímé oběti. Oběť kyberteroristického útoku je pouze prostředníkem, který má obvykle skrze zastrašení přenést poselství cílovému publiku. Od toho je následně očekávána a vyžadována nějaká akce či naopak absence akce, což je vyvoláno intenzivním strachem.

3.1.2 Publicita

Často zmiňovaná je role médií a snaha teroristů dosáhnout co nejširšího obecenstva skrze ochotná média. Paradoxně často přehlížená je významnost situace opačné: snaha útočníků svůj akt zcela utajit. Pokud u zkoumaného případu zjistíme, že se pachatelé snažili zcela utajit, že k činu došlo (tedy ne jen svoji identitu), je tímto v podstatě diskvalifikován z konceptu kyberterorismu, neboť se sami snažili bránit jakékoliv reakci publika a obecenstva.

3.1.3 Opakovatelnost

Pravý účinek zastrašení a přinucení k jednání je možný pouze tehdy, je-li přítomna hrozba, že dojde k útokům dalším. Kyberterorista tedy musí přesvědčit členy cílového publika, že nebude-li mu vyhověno, může být příští přímou obětí kdokoliv z nich.

Útoky by také měly být součástí jakési souvislé kampaně sledující nějaký deklarovaný cíl. Pokud se jedná o jednorázovou akci, na kterou útočník nemá možnost či zájem navázat, je tím značně zmenšena motivace publika vyhovět jeho požadavkům.

3.1.4 Násilí a strach

Přítomnost násilí je zřejmě nejproblematičtějším bodem kyberterorismu. „Standardní“ terorismus zpravidla staví na fyzickém a často až excesivním násilí, aby generoval strach a hrůzu v publiku. Vzhledem k povaze internetu a dalších sítí je jen velice obtížné skrze tyto útoky způsobit skutečné násilí ve smyslu poškození zdraví lidí, ztrát na životech nebo rozsáhlého zničení majetku. Elektronické útoky jsou však velmi dobře schopny způsobit rozsáhlé ekonomické škody, poškodit prestiž a image nebo nepřímo vést i k fyzickému násilí. V každém případě musí být útokem (nebo hrozbou útoku) generován intenzivní strach či podobný silný psychologický účinek.

3.2 Příklady

Tato kapitola si klade za cíl stručně rozebrat některé typy a příklady útoků či obecně událostí, které někdy bývají označovány jako projevy kyberterorismu.

3.2.1 Finanční obohacení

Elektronické útoky a podvody jejichž cílem je finanční zisk útočníků/pachatelů patří k těm nejčastějším. Nabírají mnoho forem sahajících od přímých útoků na bankovní instituce, přes krádeže databází s informacemi o zákaznících (včetně údajů o platebních kartách) ze serverů elektronických obchodů, až po zasílání podvodných e-mailů vypadajících jako legitimní korespondence požadující po neznalém uživateli důvěrné informace (tzv. phishing). Rozsah této činnosti je obrovský a někdy bývá uváděn jako manifestace kyberterorismu.

Při kritickém pohledu je ale zřejmé, že o kyberterorismus se nemůže jednat z hned několika důvodů. Prvním a nejvíce evidentním problémem je motivace, která je čistě finanční a útoky nenesou jakékoliv politické nebo ideologické poselství. Dalším problémem je fakt, že většina takto působících skupin či jednotlivců se snaží svoje aktivity utajit, neboť šance vylákat z recipienta podvodného e-mailu informace o jeho bankovním účtu je zcela závislá na jeho neznalosti. Stejně tak pokud se útočníkům podaří ukrást tyto údaje z napadeného serveru, jsou použitelné jen do doby, než se na útok přijde. Poté bývají platební transakce z kompromitovaných karet a účtů blokovány. Pachatelé se tak svůj čin snaží utajit před přímým cílem i před jakýmkoliv publikem, což je v rozporu s konceptem kyberterorismu.

3.2.2 Poškození cíle

Dalším druhem útoků, který bývá označován jako kyberterorismus, jsou průmyslové sabotáže řídících elektronických systémů. K nejčastěji zmiňovaným patří údajná exploze transsibiřského plynovodu v roce 1982 [20] a Stuxnet, který sabotoval íránské centrifugy k obohacování uranu v Natanzu. [21]

I zde, stejně jako v předchozím případě, naprosto chybí snaha útočníků o získání publicity, protože úspěšnost těchto útoků zcela závisí na jejich utajení. Rovněž se jedná spíše o přímou sabotáž ve snaze poškodit svého protivníka a omezit jeho kapacity, nikoliv o zastrašení nějaké třetí strany. Navíc jsou tyto útoky doménou především států, čímž se ještě více vzdalují konceptu terorismu, a naopak se blíží klasické válce.

Do stejné kategorie by bylo možné zařadit i známé útoky proti Estonsku a Gruzii, ke kterým došlo během jejich „rozepří" s Ruskou federací. Zde útoky ani nebyly utajovány (což ani nebylo reálně možné, neboť účinky byly okamžitě zřejmé), a dokonce obsahovaly i politický podtext, ale jejich hlavním cílem bylo přímo poškodit napadenou zemi. Zejména v případě Gruzie šlo o zřejmé instrumentální využití kyberprosotoru jako další domény pro vedení operací na podporu probíhající konvenční války. [22] Navíc nedostupnost bankovních či vládních webových stránek vskutku nelze považovat za něco, co by generovalo teror v pravém smyslu slova.

Dalším scénářem, který někdy bývá uváděn jako příklad kyberterorismu, je australský případ z roku 2000, kdy bývalý zaměstnanec vodárenské firmy ze msty vypustil tisíce litrů splašků do krajiny. Útok ovšem nebyl veden přes internet a bylo k němu využito specializovaného vybavení přímo od výrobce vodárenského systému. Došlo především k ekologickým a finančním škodám. [23] Tento i podobné útoky postrádají systematičnost, politické poselství a jejich cílem je zpravidla poškození pouze přímé oběti a rozhodně ne třeba zastrašení ostatních firem.

3.2.3 Sběr informací

V článcích o kyberterorismu můžeme často najít líčení o rozsahu ruských nebo čínských elektronických útoků proti USA. [24] Cílem těchto útoků je však získávání informací (např. pro vývoj konkurenčních zbraňových systémů), a proto je vhodnější je považovat spíše za „kyberšpionáž" než za kyberterorismus. [25] Podobou funkci plní i nedávno objevené skupiny malware jako jsou např. Flame nebo Red October. [26]

Opět je zde přítomná i snaha činnost utajit, neboť tyto útoky využívají chyb v napadených informačních systémech a děr v jejich zabezpečení. Pokud útok a extrakce informací zůstanou cílové firmě či instituci utajeny (a samozřejmě i veřejnosti), existuje šance na opakované využití této chyby k zisku informací i v budoucnu.

3.2.4 Vandalství a „sport"

Mezi specifickými komunitami jsou rozšířené i formy elektronických útoků, které se naopak pozornost snaží přitáhnout. Tím nejviditelnějším je zřejmě tzv. *defacement,* tedy nahrazení původní legitimní webové stránky novým obsahem, často vulgárním, urážlivým nebo zesměšňujícím. Přestože tyto útoky mohou nést politické nebo náboženské poselství, jsou často prováděny „ze sportu" a téměř jako soutěž. Cíle jsou pak vybírány jen příležitostně a na základě proveditelnosti útoku (někdy jsou dokonce používány automatické nástroje k vyhledání zranitelných serverů), nikoliv podle jejich symbolické hodnoty či politického významu. [27] I v případě skutečně cílených a politicky

motivovaných útoků jsou škody, které cíl utrpí, jen mírné a rozhodě nelze hovořit o terorismu a zastrašování v jejich plném významu.

3.2.5 Politická motivace

Velmi různorodou skupinu tvoří kybernetické útoky, které jsou politicky motivované, a snaží se tedy působit na širší publikum s nějakým politickým nebo ideologickým záměrem. Řada útoků, které by bylo možné označit jako politické, nese mnoho znaků výše zmíněných typů. Klasicky se může jednat o útoky, které se snaží poškodit nějakou službu nebo získat informace. Podstatným rozdílem je ale to, že takový útok nemá za konečný cíl například zpeněžit ukradené informace ale třeba poškodit prestiž nějaké entity, a tím vyslat politické poselství širokému publiku. Často užívaným pojmem je hacktivismus (aneb politický aktivismus za pomoci hackování).

Skupinou, která se touto činností dosud nejvíce proslavila, je **Anonymous**. Jejich obecné ideologické zařazení lze hledat někde na pomezí *single-issue* aktivismu (zejména neomezená svoboda šíření informací na internetu) a anarchismu (zaměřeného proti vládám, korporacím a krajní pravici). V několika případech prokázala i značnou systematičnost a ochotu zaměřit se na jeden cíl po delší dobu. Navíc aktivně komunikují s veřejností a snaží se svoje aktivity často zviditelnit za pomoci médií. Některé jejich útoky lze dokonce interpretovat i jako snahu o odstrašení obecenstva od provádění „nežádoucích" činností. Z tohoto pohledu jsou zřejmě nejzajímavější útoky na podporu serveru WikiLeaks (proti společnostem Visa, MasterCard a dalším), [28] nabourání se do bezpečnostní společnosti HBGary [29] a kampaně proti policistům zasahujícím (z jejich pohledu excesivně) proti demonstrantům hnutí Occupy. [30] Zajímavým příkladem terorismu může být tzv. *kybernetický džihád,* jehož cílem se stávají hlavně oficiální izraelské vládní internetové stránky. [31]

Žádný jejich útok ovšem ani zdaleka nedosáhl dramatičnosti srovnatelné s terorismem. Ve srovnání s aktivitami států (jako byl například Stuxnet a Flame) se dokonce jedná o útoky menšího rozsahu i dopadu.

3.3 Shrnutí

Z výše uvedených typových příkladů [32] lze snadno nabýt dojmu, že kyberterorismus se vlastně ani vůbec nevyskytuje. Tento úsudek samozřejmě závisí na tom, jak úzká či široká definice je užita. Hodnotíme-li dosavadní útoky z pozice striktního vymezení kyberterorismu, nezbývá než konstatovat, že kyberterorismus je doposud neexistujícím a čistě hypotetickým fenoménem, protože i útoky při nichž se aktéři snaží dosáhnout veřejného zastrašení pro politické účely, obvykle postrádají charakter systematické kampaně, a zejména jim chybí dramatický efekt, násilnost a schopnost generovat silný pocit strachu v publiku.

Přestože teoretický potenciál kyberterorismu je obrovský [33] a skýtá útočníkům řadu výhod [34] proti terorismu „konvenčnímu", zůstává prozatím zcela nenaplněn, a to i přesto, že hackeři stále dokáží svět překvapit tím, do jakých systémů se jim podaří dostat. Důvodů, proč k závažným útokům zatím nedochází, je hned několik:

- ty nejcitlivější systémy nejsou vůbec k internetu připojeny a jsou zabezpečeny pomocí tzv. *air-gap* a útok by tak obvykle vyžadoval fyzickou přítomnost,
- sofistikované útoky na průmyslová nebo vojenská zařízení vyžadují detailní přehled o cílovém systému, dlouhou a náročnou přípravu a velmi pokročilé znalosti z oboru,

- elektronické útoky pro „tradiční teroristy“ postrádají silný dramatický a symbolický efekt, kterého mohou dosáhnout pomocí výbušnin a excesivního násilí,
- elektronické útoky vyžadují informační infrastrukturu, kterou rozvojové země (obzvláště mimo města) často postrádají,
- „subkultura hackerů“ obvykle nemá zájem, odhodlání a potřebný ideologický zápal se do těchto rozsáhlých útoků pouštět. [35]

Situace by se tedy dala stručně shrnout tak, že existující teroristické skupiny (např. islamistické) momentálně postrádají technické dovednosti, znalosti a schopnosti tyto postulované dramatické útoky provést, a navíc jim zřejmě i chybí vůle se do těchto útoků pouštět, neboť se jim svým efektem mohou jevit jako podřadné vůči těm bombovým a dalším, jejichž výsledkem je extrémní násilí na civilistech. A naopak ti, kteří by těchto útoků teoreticky schopni být mohli, postrádají organizační strukturu a motivaci se do nich pouštět.

4. Závěr

Na konec asi nezbývá než prozatím souhlasit se závěry Dorothy Denning, [36] že útoky ještě nedosáhly takové úrovně, aby mohly být nazvány kyberterorismem. Žádný dosavadní útok nedosáhl dostatečné intenzity, rozsahu škod a obětí na životech, aby vskutku generoval strach srovnatelný například s bombovými teroristickými útoky. Tento potenciál v sobě sice nesou postulované útoky na průmyslové systémy a infrastrukturu, ale ty jsou prozatím zcela mimo schopnosti současných teroristických skupin a sítí (jako je např. al-Ká'ida nebo různé nacionalistické skupiny). Ty o takovéto formy útoků zpravidla ani nejeví zájem (neboť pro ně postrádají dramatičnost a symbolickou hodnotu) a pokud už se k nim jejich přívrženci odhodlají, jedná se o ty nejjednodušší formy.

Z tohoto hlediska „nadějnějšími“ aktéry jsou hacktivistické entity v čele s Anonymous, které již prokázaly daleko pokročilejší schopnosti a řada jejich útoků nese znaky teroristického kalkulu, zejména útoky proti finančním společnostem, HBGary Federal a útoky na policejní sbory. Úroveň násilí, škod a strachu je však stále relativně nízká. Vzhledem k množství a různorodosti přívrženců Anonymous nelze vyloučit, že se o skutečně kyberteroristický útok v budoucnu nepokusí. Momentálně k tomu ale sklony zdá se nevykazují.

V současnosti je ale třeba konstatovat, že kyberterorismus (ve své úzké definici např. dle Denning) je prozatím v podstatě neexistující fenomén. Na jeho manifestaci si ještě musíme počkat. Podstatné je, že obrovské množství elektronických aktivit, které je rutinně označováno jako kyberterorismus, nemá s terorismem prakticky vůbec nic společného a jedná se spíše o finanční kriminalitu, špionáž, sabotáže či pouhé vandalství. Z „terorismu“ se bohužel v poměrně krátké době stala velice nadužívaná nálepka. Přinejmenším v odborné a akademické sféře, na rozdíl od té mediální, kde již byl koncept terorismu jakž takž vyjasněn a ustálen, lze hovořit o zcela evidentním dvojím metru. Na druhou stranu je nutné uznat, že vývoj za posledních pár let je na tomto poli velice dynamický a výskyt skutečného kyberterorismu je zřejmě jen otázkou času.

Poznámky k textu a literatura:

[1] *Kybernetický terorismus*. Praha: Ministerstvo vnitra České republiky - Odbor bezpečnostní politiky, 2009 [cit. 2013-02-11] Dostupné z < http://www.mvcr.cz/clanek/typologie-terorismu.aspx?q=Y2hudW09NA%3d%3d>.

[2] *Strategie boje proti terorismu.* Praha: Ministerstvo vnitra České republiky - Odbor bezpečnostní politiky, 2010 [cit. 2013-02-11] Dostupné z <http://www.mvcr.cz/soubor/nap-2010-pdf.aspx>.
[3] *Bezpečnostní strategie České republiky.* Praha: Ministerstvo zahraničních věcí ČR, 2011 [cit. 2013-02-11] Dostupné z <http://www.mzv.cz/file/699914/Bezpecnostni_strategie_CR_2011.pdf>.
[4] JIRÁSEK, Petr - NOVÁK, Luděk - POŽÁR, Josef. *Výkladový slovník kybernetické bezpečnosti.* Praha: Policejní akademie ČR, 2012 [cit. 2013-02-11] Dostupné z <http://www.cybersecurity.cz/data/slovnik_v150.pdf>.
[5] JANOUŠEK, Michal. Kyberterorismus: terorismus informační společnosti. *Obrana a strategie,* 2/2006 [cit. 2013-02-11] Dostupné z <http://www.mocr.army.cz/mo/obrana_a_strategie/2-2006cz/janousek.pdf>.
[6] JIROVSKÝ, Václav. *Kybernetická kriminalita*. Praha: Grada, 2007, 284 s. ISBN 978-80-247-1766-1.
[7] JIROVSKÝ, Václav - HNÍK, Václav - KRULÍK, Oldřich. *Kybernetické hrozby: Výzva pro moderní společnost.* Současnost a budoucnost krizového řízení 2006. Praha: T-SOFT s.r.o., 2006.
[8] LIEBERMAN, Danny. *A strategy for combating cyber terror*. Software Associates, 2011 [cit. 2013-02-11] Dostupné z <http://www.software.co.il/2011/07/a-strategy-for-combating-cyber-terror/>.
[9] SAINT-CLAIRE, Steve. *Overview and Analysis on Cyber Terrorism.* Florence: School of Doctoral Studies of the European Union. Department of Engineering and Technology, 2011. [cit. 2013-02-11] Dostupné z <http://www.iiuedu.eu/press/journals/sds/SDS_2011/DET_Article2.pdf>.
[10] TAFOYA, William L. Cyber Terror. *FBI Law Enforcement Bulletin* [cit. 2013-02-11] Dostupné z <http://www.fbi.gov/stats-services/publications/law-enforcement-bulletin/november-2011/cyber-terror>.
[11] JARVIS, George. *Comprehensive Survey of Cyber-Terrorism.* St. Louis: Washington University in St. Louis, Department of Science and Engineering, 2011[cit. 2013-02-11] Dostupné z <http://www.cse.wustl.edu/~jain/cse571-11/ftp/terror.pdf>.
[12] GREEN, Joshua. The Myth of Cyberterrorism. Washington DC, *The Washington Monthly,* 2002 [cit. 2013-02-11] Dostupné z <http://www.washingtonmonthly.com/features/2001/0211.green.html>.
[13] CAVELTY, Myriam Dunn. Cyber-Terror–Looming Threat or Phantom Menace? Haworth Press, *Journal of Information Technology & Politics,* Vol. 4(1) 2007 [cit. 2013-02-11] Dostupné z <http://ethz.academia.edu/MyriamCavelty/Papers/450281/Cyber-Terror_Looming_Threat_or_Phantom_Menace_The_Framing_of_the_US_Cyber-Threat_Debate>.
[14] GORDON, Sarah - FORD, Richard. *Cyberterrorism? Cupertino: Symantec Security Response.* 2003. [cit. 2013-02-11] Dostupné z <http://www.symantec.com/avcenter/reference/cyberterrorism.pdf>.
[15] CLARKE, Richard A. How China Steals Our Secrets. *The New York Times,* 2012 [cit. 2013-02-11] Dostupné z <http://www.nytimes.com/2012/04/03/opinion/how-china-steals-our-secrets.html>.
[16] JACKSON, William. Is a ‚digital Pearl Harbor' in our future? Vienna, *GCN*, 2009 [cit. 2013-02-11] Dostupné z <http://gcn.com/Articles/2009/12/04/digital-Pearl-Harbor.aspx>.
[17] Za jistou šedou zónu lze považovat konvenční, tedy neelektronické útoky, např. pomocí výbušnin, na informační infrastrukturu.
[18] „...the convergence of terrorism and cyberspace. It is generally understood to mean unlawful attacks against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objections. Further, to qualify as cyberterrorism, an attack should result in violence against persons or property, or at the least cause enough harm to generate fear. Attacks that lead to death or bodily injury, explosions, plane crashes, water contamination, or severe economic loss would be examples."; In: SWIMMER, Morton. Cyberterrorism: Oh Really? *Trend Micro,* 3.10. 2010. [cit. 2013-02-11] Dostupné z <http://www.virusbtn.com/pdf/conference_slides/2010/Swimmer-VB2010.pdf>.
[19] „Terrorism is an anxiety-inspiring method of repeated violent action, employed by (semi-) clandestine individual, group or state actors, for idiosyncratic, criminal or political reasons, whereby - in contrast to assassination - the direct targets of violence are not the main targets. The immediate human victims of violence are generally chosen randomly (targets of opportunity) or selectively (representative or symbolic targets) from a target population, and serve as message generators. Threat- and violence-based communication processes between terrorist (organization), (imperiled) victims, and main targets are used to manipulate the main target (audience(s)), turning it into a target of terror, a target of demands, or a target of attention, depending on whether intimidation, coercion, or propaganda is primarily sought", ibid.
[20] Srov. DICKMAN, Frank. Hacking the industrial SCADA network. Houston, *Pipeline & Gas Journal,* November 2009 Vol. 236 No. 11. [cit. 2013-02-11] Dostupné z <http://www.pipelineandgasjournal.com/hacking-industrial-scada-network>; GILLINGWATER, Paul. *The Myth of CyberTerrorism. Insecurity: Musings on Risk Management,* 2009. [cit. 2013-02-11] Dostupné z <http://security-risk.blogspot.com/2009/10/myth-of-cyberterrorism.html>.

[21] ZETTER, Kim. *How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History.* Wired - Threat Level, 2011. [cit. 2013-02-11] Dostupné z <http://www.wired.com/threatlevel/2011/07/how-digital-detectives-deciphered-stuxnet/all/1>; FALLIERE, Nicolas - Ó MURCHÚ, Liam - CHIEN, Eric. *W32 Stuxnet Dossier. Cupertino: Symantec - Security Response,* February 2011. [cit. 2013-02-11] Dostupné z <http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf>.

[22] HOLLIS, David M. Cyberwar Case Study: Georgia 2008. [cit. 2013-02-11] Bethesda, *Small Wars Journal,* 2011. Dostupné z <http://smallwarsjournal.com/jrnl/art/cyberwar-case-study-georgia-2008>; MSHVIDOBADZE, Khatuna. *State-sponsored Cyber Terrorism: Georgia's Experience.* Tbilisi: Georgian Foundation for Strategic and International Studies, 2011[cit. 2013-02-11] Dostupné z <http://www.gfsis.org/media/download/GSAC/cyberwar/State-sponsored_Cyber_Terrorism.pdf>.

[23] ABRAMS, Marshall - WEISS, Joe. *Malicious Control System Cyber Security Attack Case Study.* Maroochy Water Services, Australia. Gaithersburg: National Institute of Standards andTechnology, Computer Security Division, 2008[cit. 2013-02-11] Dostupné z < http://csrc.nist.gov/groups/SMA/fisma/ics/documents/Maroochy-Water-Services-Case-Study_report.pdf

[24] FEUERBERG, Gary. Commission Hears Extent of China's Espionage and Cyber Terrorism. Washington DC, *The Epoch Times,* 2009[cit. 2013-02-11] Dostupné z <http://www.theepochtimes.com/n2/world/china-espionage-cyber-terrorism-16827.html>; ODIOGOR, Hugo. U.S, China bicker over Cyber terrorism. Lagos, *Vanguard,* 2011.[cit. 2013-02-11] Dostupné z <http://www.vanguardngr.com/2011/08/u-s-china-bicker-over-cyber-terrorism/>.

[25] WILSON, Clay. Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress. Washington DC, *Congressional Research Service,* 2008; 2012 [cit. 2013-02-11] Dostupné z <http://www.fas.org/sgp/crs/terror/RL32114.pdf>.

[26] SCHWATRZ, Mathew J. Red October Espinage Network Rivals Flame. Manhasset, *Information Week - Security,* 2013 [cit. 2013-02-11] Dostupné z <http://www.informationweek.com/security/attacks/red-october-espionage-network-rivals-fla/240146215>.

[27] JACOBY, David. Mass Defacements: the tools and tricks. Moskva, *Kaspersky - Securelist,* 2010 [cit. 2013-02-11] Dostupné z <http://www.securelist.com/en/analysis/204792127/Mass_Defacements_the_tools_and_trick>.

[28] ADDLEY, Esther - HALLIDAY, Josh. WikiLeaks supporters disrupt Visa and MasterCard sites in ‚Operation Payback'. London, *The Guardian,* 2012 [cit. 2013-02-11] Dostupné z <http://www.guardian.co.uk/world/2010/dec/08/wikileaks-visa-mastercard-operation-payback>.

[29] BRIGHT, Peter. *Anonymous speaks: the inside story of the HBGary hack.* Ars Technica, 2011. [cit. 2013-02-11] Dostupné z <http://arstechnica.com/tech-policy/news/2011/02/anonymous-speaks-the-inside-story-of-the-hbgary-hack.ars/1>.

[30] MARTIN, Adam. Anonymous Goes After the Pepper Spray Cop's Personal Info. Washington, DC, *Atlantic Wire,* 2011 [cit. 2013-02-11] Dostupné z <http://www.theatlanticwire.com/national/2011/09/anonymous-goes-after-pepper-spray-cops-personal-info/42960/>.

[31] ŘEHÁK, D. - FOLTIN, P. - STOJAR, R. *Vybrané aspekty soudobého terorismu.* Praha: MO ČR-AVIS, 2008, 144 str., ISBN 978-80-7278-443-1, kapitola 6.2.2, Nezbraňové prostředky, str. 75.

[32] Tímto stručným výčtem rozhodně nebyly vyčerpány všechny elektronické útoky, které bývají považovány za kyberterorismus. Další již nejsou podrobněji rozepsány jednak kvůli rozsahu práce a navíc by se důvody, proč je nelze považovat za skutečný terorismus, stále opakovaly. Pro doplnění lze ještě uvést například nabourání se do pozemních satelitních stanic (http://www.bbc.co.uk/news/business-15490687), elektronické útoky na bezpilotní letouny (http://news.bbc.co.uk/2/hi/middle_east/8419147.stm), samotný provoz serveru WikiLeaks (http://news.cnet.com/8301-13578_3-20023941-38.html), a dokonce i pokusy o získání důkazů o existenci UFO ze serverů Pentagonu (http://www.theregister.co.uk/2008/08/09/mckinnon_ufo_cyberterror_analysis).

[33] Často postulované jsou útoky na přehrady, elektrárny, nemocnice, dopravní infrastrukturu, továrny zpracovávající nebezpečné materiály a dokonce i na ZHN národních armád.

[34] Hlavně anonymita a fyzická bezpečnost útočníka, relativně nízká cena a globální dosah odkudkoliv.

[35] Kolují obavy, že by si teroristé mohli skupinu hackerů najmout, nicméně hackerské komunity se většinou nepřátelsky staví k projevům nacionalistického nebo náboženského extremismu, neboť často tíhnou spíše k anarchistickému uvažování. Zároveň ale není možné tuto variantu zcela vyloučit.

[36] DENNING, Dorothy. Whither Cyber Terror? New York, *A Social Science Research Council Essay Forum. "10 Years After September 11",* September 2011 [cit. 2013-02-11] Dostupné z <http://essays.ssrc.org/10yearsafter911/whither-cyber-terror/>; DENNING, Dorothy. Take This Joke Seriously. Toronto, *The Mark,* 2011. [cit. 2013-02-11] Dostupné z <http://www.themarknews.com/articles/5844-take-this-joke-seriously>.