Univerzita Karlova v Praze
Filozofická fakulta
Ústav informačních studií

Diplomová práce

2011 **Bc. Martina Knopová**

Univerzita Karlova v Praze
Filozofická fakulta
Ústav informačních studií

Studijní program: informační studia
Studijní obor: Studia nových médií

Bc. Martina Knopová

Kyberterorismus a digitální pirátství

Diplomová práce

Praha 2011

Vedoucí diplomové práce: MgA. František Zachoval

Oponent diplomové práce:

Datum obhajoby:

Hodnocení:

Prohlášení:

Prohlašuji, že jsem diplomovou práci zpracovala samostatně a že jsem uvedla všechny použité informační zdroje.

V Praze, 19. srpna 2011

……..
podpis diplomanta

Poděkování

Děkuji svému vedoucímu práce MgA. Františku Zachovalovi za cenné rady a připomínky.

Identifikační záznam

KNOPOVÁ, Martina. *Kyberterorismus a digitální pirátství [Cyberterrorism and digital piracy]*. Praha, 2011. 111 s. Diplomová práce. Univerzita Karlova v Praze, Filozofická fakulta, Ústav informačních studií 2011. Vedoucí diplomové práce MgA. František Zachoval

Abstrakt

Diplomová práce se zabývá především zmapováním cílů, motivací, nástrojů a důsledků současných kybernetických válek. V prvé řadě se zaměřuje na charakter kybernetických konfliktů, identifikuje a definuje podstatu kybernetického terorismu; jeho principy, příčiny a hrozby. Kromě popisu obecných metod kybernetického boje klade také důraz na podrobnou analýzu konceptu „Information Assurance," který představuje druh strategie, užívané za účelem definice rizik informační bezpečnosti v kyberprostoru. Analytická část práce se věnuje konkrétním případům mezinárodního kyberterorismu a jeho jednotlivým formám v kybernetických střetech mezi lety 2007 a 2010. Z geopolitického hlediska chronologicky analyzuje jednotlivé kybernetické útoky, k nimž došlo v oblasti evropsko-ruské, asijsko-americké a na Středním východě. Z komparace teoretického modelu „Information Assurance" a dílčích analýz jednotlivých příkladů kybernetických válek tak vyplynulo, že nedodržení tohoto modelu v praxi má za následek narušení informační bezpečnosti daného systému, což v uvedených případech výrazně přispělo ke vzniku kybernetických konfliktů, čímž byla potvrzena platnost a použitelnost konceptu „Information Assurance" při zabezepečování informačních systémů.

Abstract

The thesis “Cyberterrorism and digital piracy” deals with the description of aims, motivation, tools, and consequences of current cyberwars. First of all, it concentrates on features of cyberconflicts while trying to indentify and define the essence of cyberterrorism, its principles, causes, and threats. Besides a description of common cyberwar methods, it provides a reader with a detailed analysis of the “Information Assurance“ concept, which represents a form of strategy used to define risks of information security in the cyberspace. The analytic part of the thesis concerns concrete cases of the international cyberterorism and its forms in the 2007 to 2010 cyberwars. It also analyses some particular cyberattacks from the geopolitical point of view in a chronoligical way, especially those that happened in the European-Russian, Asian-American and Middle-Eastern regions. The comparation of the theoretical “Information Assurance“ model and partial analyses of individual cyberwar examples has showed that not to keep the model reasons in the real disruption of the information security for a particular system. This fact notably contributed to the inception of aforementioned cyberconflicts, therefore the validity and applicability of the Information Assurance“ concept the has been proved.

Klíčová slova

informační systémy, information assurance, kyberterorismus, kybernetická válka,

Obsah

CHARAKTERISTIKA DIPLOMOVÉ PRÁCE

Cílem teoretické části diplomové práce je zmapovat současný stav kybernetického boje, specifikovat jeho charakter a poukázat na jeho provázanost s informačně-komunikačním konceptem „Information Assurance."[1] Cílem praktické části práce je demonstrovat jednotlivé prvky tohoto konceptu na případových studiích klíčových kybernetických útoků vybraných a utřízených dle geopolitického hlediska.

Koncept „Information Assurance," vyvíjející se postupně již od konce 50. let, představuje od přelomu tisíciletí hlavní nástroj analýzy rizik v informačních systémech. „Information Assurance" je tvořen jednotlivými dílčími atributy, které zahrnují *dostupnost* (availability), *integritu* (integrity), *autentizaci* (authentication), *důvěrnost* (confidentiality) a *nepopiratelnost* (non-repudiation), jež jsou klíčovými prvky zabezpečeného přístupu do informačních systémů.[2] Jelikož se snažím ve své práci ověřit, zda je koncept stále aktuálním i pro rychle se vyvíjející a globalizující oblast nových médií, zabývala jsem se v práci dvěma stěžejními otázkami. Zaprvé, zda je stále možné pomocí konceptu „Information Assurance" popsat současné kyberteroristické útoky, a zadruhé, zda by bylo relevantní obranou vůči hrozbám modifikace, zcizení a znehodnocení dat dodržení prvků tohoto konceptu? Pro empirické ověření těchto otázek jsem sestavila hypotézu, kterou jsem ověřovala na případových studiích praktické části práce:

„Koncept ‚Information Assurance' je stále dostatečně aktuální a využitelný pro to, aby dokázal popsat současné kyberteroristické útoky a jeho dodržování vede k eliminaci hrozby útoků."

Praktickým záměrem práce je tedy pomocí případových studií přispět k teoreticky obecnému argumentu, který říká, že principy a příčiny kybernetického technologického boje,

---

[1] Information Assurance" znamená koncept, který identifikuje rizika v informačních systémech a nastavuje efektivní obranu pro nim. Tímto konceptem se zajišťuje souhrn atributů integrity, dostupnosti, důvěrnosti, nepopiratelnosti a autentizace tak, aby uživatel měl jistotu, že data v procesu od vysílače k příjemci nebyla změněna nebo zpřístupněna nepovolaným osobám. Spadají sem veškerá rizika související s informacemi, bez ohledu na typ rizika – mohou být bezpečnostní, právní nebo technologická.

[2] Srov. Novotný, J., Čeleda, P., Dedek, T. *Hardware Acceleration for Cyber Security.* In IST-091 – Information Assurance and Cyber Defence. Antalya (TUR) : NATO Research and Technology Organization, 2010. str. 15.

v současnosti a blízké budoucnosti fungují na principu masového rozšíření informačních a komunikačních technologií, jsou zacíleny především na infrastrukturu kritických systémů. Předpoklad, podložený dalším výkladem uvádí, že v posledních dekádách došlo v technické, ekonomické, kulturní, a tím pádem i mediální, politické a sociální rovině ke změnám, které přetvořily strukturální charakter globální společnosti natolik, že můžeme hovořit o kvalitativně nových rizicích, zranitelných místech a nových technologiích boje.

Druhá analytická část práce se věnuje problematice kybernetického boje, a sice identifikaci jeho podstaty a analýze jeho možností z pohledu vybraných států a nadnárodních organizací. V této části rovněž usiluji o vymezení motivace kybernetických útoků s důrazem na hlavní cíl – *kritickou infrastrukturu*, jež se stala hlavním cílem kyberteroristů při nejzávažnějších kyberútocích, které se odehrály v letech 2007 až 2010. Tyto příklady kybernetických konfliktů jsou analyzovány z geopolitického hlediska, a tudíž rozčleněny na oblast evropsko-ruskou, a to především na útoky na Gruzii a Estonsko, asijsko-americkou, zaměřenou na čínskou kybernetickou strategii a také na význam *Cyber Command*[3] v útoku proti Jižní Koreji a USA, i středo-východní, reprezentovanou především červem "Stuxnet" v Iránu, který se stal významným obratem ve způsobu vedení kybernetických válek. V poslední části jsou jednotlivé konflikty konfrontovány s teoretickým konceptem „Information Assurance," při čemž jsou zároveň vyvozeny důsledky těchto událostí, a tak je v závěru umožněno ověřit platnost úvodem stanovené hypotézy.

Při výběru zdrojů k práci jsem vycházela zejména z děl klasických autorů případně z literatury, na kterou tato díla odkazují. Zároveň podotýkám, že část práce byla napsána na studijním pobytu v Římě, a proto je odborná literatura dílem v italském jazyce.

V teoretické práci je obzvlášť využita metoda popisu, částečně jsem užila i metody komparativní. Díky těmto pracovním metodám byla stanovena výchozí hypotéza, k jejímuž ověření došlo v části analytické, kde byla použita především metoda analytická, pro důkladnější nastínění souvislostí jsem zvolila metodu komparace, jiné pasáže jsou zpracovány metodou popisu. Za účelem zachování jednotného rámce zkoumání, jsem si u vybraných aktérů vypomohla následujícími výzkumnými otázkami:

1. Které instituty mezinárodního práva aktéři užili v rámci oficiální argumentace?

2. Jaké skutečné cíle a zájmy lze dovodit z činů a dlouhodobého chování aktérů?

[3] Organizovaný útvar USA, které dohlíží na elektronickou bezpečnost armádních sítí, sítí amerických úradů a soukromých sítí vysoké důležitosti. Velitelem útvaru je generál Keith Alexander.

3. Do jaké míry byla oficiální argumentace a skutečné kroky v souladu?

Především jsem se tak zabývala okolnostmi, přímo souvisejícími s hledáním odpovědí na výše položené výzkumné otázky a s následným ověřením platnosti hypotézy.

V závěrečné části práce jsem se na základě nabytých poznatků snažila najít odpověď na otázku podstaty a podoby kybernetického terorismu v rámci obecně chápaného kybernetického boje, jeho charakteru a nástrojů, jakož i jeho vztahu k současným technologicky vyspělým společnostem a k formám vedení konfliktů.

TEORETICKÁ ČÁST - Úvod do problematiky informačních technologií

Možnosti kybernetického boje jsou dány informatizací a demokratizací společnosti. S příchodem tzv. „informační společnosti,“[4] závislé na informačních a komunikačních technologiích a zejména na IT infrastruktuře, se rozvinula nová možnost destabilizace informačních systémů, nová hrozba kybernetických útoků. Běžný charakter války 20. století byl převratným způsobem změněn prostřednictvím informačních a komunikačních technologií (dále jen ICT), které umožnily vést bitvu v elektronickém, a touto změnou charakteru boje přiměly společnost ke změně způsobu reakce na válku vůbec.

Společnost založená na znalostech, která využívá moderní ICT v každodenním životě, je a bude stále více ohrožena úmyslným či neúmyslným zneužitím těchto technologií. Současně ale jejich vhodné užití nabízí rozsáhlý potenciál při ochraně společnosti před různými typy hrozeb, včetně terorismu. Předmětem mého výzkumného záměru je proto analýza informačních technologií z hlediska bezpečnosti. Jedná se zejména o systematické rozvíjení konceptu „ Information Assurance,“a jde tak i o výzkum možností a využití informačních technologií pro posílení informační bezpečnosti prostřednictvím vytváření nových přístupů k analýze, monitorování a předvídání potenciálně nebezpečných aktivit.

Zejména v posledních letech se stala bezpečnost informačních systémů velmi důležitou součástí informatiky všech mezinárodních institucí, nadnárodních organizací téměř ve všech oblastech řízení. Její význam poroste hlavně v budoucnu z důvodů užšího zapojení do evropských struktur, a tím následnou technologickou integrací. Jako zvláště alarmující se jeví situace v oblasti bezpečnosti informačních systémů. Od r. 1988, kdy se v USA objevil první vir a jiné další nebezpečné způsoby ohrožení bezpečnosti počítačů (červi, trojští koně), vznikla nová kategorie počítačových programů, tzv. *malware,*[5] čelící těmto bezpečnostním

[4] Poprvé zmíněna v roce 1975 v Norově-Mincově zprávě pro francouzskou vládu. Informační společnost je charakterizovaná vytvářením, využitím, distribucí a manipulací s informacemi coby nejvýznamnější ekonomickou, politickou a kulturní aktivitou. Základními nástroji informační společnosti jsou počítače a telekomunikační prostředky, tedy ICT.

[5] Malware je počítačový program určený ke vniknutí nebo poškození počítačového systému. Výraz *malware* vznikl složením anglických slov „malicious“ (zákeřný) a „software“. Malwarem rozumíme tzv. škodlivý software (malicious software).

rizikům. Současně se ohromným tempem zvyšuje i rozsah napadení počítačů. Zatímco do r. 2004 rostl počet hrozeb ze strany malware pouze lineárně a ne příliš rychle, od r. 2004 se tento lineární růst změnil na růst exponenciální. V r. 2008 bylo již zaznamenáno kolem 1,5 milionu hrozeb ze strany malwaru a během r. 2009 to bylo již 2 miliony. Podle organizace Symantec,[6] zabývající se problémem bezpečnosti počítačů, směřuje kyberkriminalita nejvíce do oblasti získávání a prodeje informací o kreditních kartách (31 % z celkového podílu obchodů), dále potom do prodeje údajů o finančních účtech (20 %). Pokračuje také nárůst útoků využívajících sociální sítě. Nejnovější útoky r. 2010 se zaměřily zejména na společnosti obchodující s cennými papíry na burze, nadnárodní korporace a vládní agentury.

Je nesporné, že otázka bezpečnosti dat se velice zvýšila díky rozšíření konceptu Web 2.0,[7] který je spjat s obrovským nárůstem uživatelské základny, a to především u aplikacích sociálních sítí, jež se staly novou základnou pro útoky počítačových zločinců. Web 2.0 se s počtem svých uživatelů a interaktivním obsahem stal sociální platformou pro kyberteroristické útoky počítačových zločinců. Interaktivní obsah, sociální sítě s otevřenou propojenou komunitou lidí a skupin nabízí útočníkům nový prostor pro šíření počítačových útoků prostřednictvím *nových kanálů,*[8] a také umožňuje provádět útoky *sociálního inženýrství*[9] za účelem *profilace* a *krádeže identity*, což jsou synonyma pro nejvýznamnější informačně bezpečnostní rizika.

Dalším důvodem, proč se zabýváme problematikou ochrany dat, je *vzestup* cílených útoků na jednotlivá zařízení, neboť významně narůstá počet nových hrozeb, které jsou neustále důmyslnější ve své komplexnosti, složitosti a kriminálním úmyslu.

V současnosti se dynamicky vyvíjejí především způsoby obrany a útoků, identifikují se původy hrozeb kyberteroristických útoků, analyzuje se množství škodlivých kódů, diferencují

---

[6] Viz *Symantec Global Internet Security Threat Report. Trends for 2010.* In: Symantec, duben 2010, [cit.1.5.2011]. Dostupný na WWW: <http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiv_04-2009.en-us.pdf >.

[7] O'REILLY, Tim. Web 2.0 Compact Definition: Trying Again. *O'Reilly – Spreading The Knowfledge Of Technology Innovators* [online]. c2006 [cit.1.5.2011].

[8] DI NUCCI, Darcy. Fragmented Future. *Design and New Media.* [online]. 1999

[9] Sociální inženýrství (sociotechnika) je způsob získávání důležitých informací od uživatelů bez jejich vědomí pomocí něhož útočník získá neautorizovaný přístup do počítačového systému.

se způsoby na zajišťování webové bezpečnosti, shrnují se pozitiva i negativa, a společnost se tak zaměřuje na problematiku ztráty elektronických dat více než kdykoliv předtím. Navíc na významu pozoruhodně nabývá i problematika škodlivých kódů v informačních sítích, problematika Web 2.0 služeb a fungování moderních webových aplikací,[10] které přinášejí naprosto *novou zkušenost* s různými formami útoku. Stejně tak dnes hýbe světem i otázka *virtualizace,*[11] takže ochrna dat v informačních systémech nezůstává jenom úkolem pro pracovníky v ICT, ale rovněž se stává vysoce řešenou prioritou ve vysokém managementu, u sociologů, stejně jako u informační vědců.

Organizace soukromé i veřejné stále více akcelerují na outsourcing,[12] cloud technologie[13] a mobilní řešení. Důležitý vedlejší účinek ale zároveň představuje fakt, že více dat je vystaveno *ztrátě* nebo *krádeži.* Tato témata jsou dokonce tak aktuální a dynamická, že se v současnosti můžeme setkat s tak netradičními a netypickými hrozbami,jakými jsou například nové metody pishingu[14] (Whaling, TagNabbing), hardwarová špionáž na úrovni výrobců, či nebezpečné geografické lokace.[15] Kybernetiční útočníci totiž velmi rychle chápou význam *nových technologií,* jakými jsou například *Cloud computingu a virtualizace,*[16] jako prostředek pro využití v jejich činnosti. Dále jsou velmi aktuální otázky monitoringu, které významně přesahují do oblasti legislativy a právních předpisů vůbec. Rozebírají se i nové

[10] Srov. PORTER, Joshua. Why Social Ads Don't Work. *Bokardo Social Web Design* [online]. 2008

[11] V otázkách dnešní informační bezpečnosti řešíme virtualizaci jako jedno z hlavních řešení bezpečnostních problémů. Srov. PORTER, Joshua. Why Social Ads Don't Work. *Bokardo Social Web Design* [online]. 2008

[12] KAKABADSE A.; KAKABADSE N. Outsourcing : Current and Future Trends. *Thunderbird International Business Review* [online]. 2005, vol. 47, no. 2 [cit.7.3.2011]. Dostupný na WWW: <http://people.oregonstate.edu/~sanderni/outsourcing.pdf>.

[13] Srov. ANDERSON, Nate. Tim Berners-Lee on Web 2.0: "nobody evens know what it means". *Ars Technica* [online]. 2006

[14] „Phishing" je podvodná technika používaná na internetu k získávání citlivých údajů (hesla, čísla karet). Srov. Kolouch, J. – Volenecký, P. Trestněprávní aspekty phishingového útoku. Trestní právo, 2008, roč. XII, č. 9, s. 5.

[15] Srov. *Regulation in the Information Society*. In: European Commission, Europe's Information Society, [cit.1.5.2011]. Dostupný na WWW<http://ec.europa.eu/information_society/tl/policy/regulate/index_en.htm> .

[16] Tamtéž

technologie pomocí těch klasických, jako je například antivirová ochrana, filtr spamu či obsahu.[17]

Informační bezpečnost mění svět, s tím, jak se jeho lidská populace stává závislejší na informačních systémech a jejich provozování, kladouce důraz na klíčové pojmy typu „kontinuita provozu," „řízení identit," či „ochrana před automatizovanými útoky." Jedním z nejžhavějších problémů dnešní společnosti je tak ochrana před falšováním identity, kde se subjekt vydává za někoho, kým ve skutečnosti není. Řeší se zde v podstatě *identifikaci jedince* pro provedení různých systémových operací, neboť toto představuje neuvěřitelně silnou zbraň, která ve „*virtuálním prostředí"* předkládá reálné informace. Zatímco v reálném světě dosvědčuje jedinec svoji identitu svým vzhledem nebo identifikačním dokumentem, ve virtuálním světě platí, že v podstatě *neznámý subjekt* se pokouší prokázat svoji *identitu,* a domáhá se tak svých práv pro daný systém. Zvláště nyní, kdy je riziko neautentizovaného přístupu k datům stále vyšší, neboť se zvyšuje okruh osob, které mohou mít přístup k těmto datům.

Z výše uvedených důvodů znamená bezpečnost informačních systémů velmi širokou oblastí sofistikovaných řešení pro danéou problematice, takže funguje na mnoha přístupech a metodách.

Po provedeném průzkumu Eurostatu s názvem „Security related problems experienced through using the Internet for private purposes in the last 12 months*"*[18] se jako zvláště alarmující jeví situace v oblasti bezpečnosti informačních systémů.[19]

---

[17] Zvláště se klade důraz na bezpečnostní monitoring sítí v kontextu s podezřelými jevy a událostmi, které mají vysokou schopnost odhalit slabá místa systému nebo neznámé útoky.

[18] Databáze Eurostat. *Security related problems experienced through using the Internet for private purposes in the last 12 months* [cit.1.5.2011]. Dostupný na WWW< http://appsso.eurostat.ec.europa.eu/nui/setupModifyTableLayout.do>.

[19] *The European Programme for Critical Infrastructure Protection*. [cit.1.5.2011]. In: ProAdrias, Dostupný na WWW< http://www.proadrias.isig.it/Documenti/EPCIP%20memo.pdf>.

BEZPEČNOST DAT V INFORMAČNÍCH SYSTÉMECH

Pod pojmem informační bezpečnost rozumíme obvykle zajištění interních i externích složek informačních systémů a informací, které jsou v nich uchovávány, zpracovány a přenášeny. Pojem bezpečnost IT zahrnuje především pojmy jako *bezpečnost informačních systémů, ochrana informačních systémů, ochrana informací, ochrana informačních technologií*. [20]

Všechny tyto pojmy mají svůj nezanedbatelný význam při popisu a diskuzi o bezpečnosti a ochraně informačních systémů a informací uložených, zpracovávaných a přenášených v takovýchto systémech. Mezinárodní normalizační organizace ITSEC[21] ve svých normách definuje bezpečnost jako *zajištěnost* proti nebezpečím, minimalizaci rizik a jako komplex administrativních, logických, technických a fyzických opatření pro prevenci, detekci a opravu nesprávného použití informačních systémů. Jsou vytvářena tzv. *Kritéria hodnocení bezpečnosti informačních* systémů, tzv. *ITSEC (Information Technology Security Evaluation Criteria).*[22] Tato kritéria byla Evropskou komisí poprvé přijata v r. 1990.[23] Bezpečný informační systém je podle nich takový, který je zajištěn *fyzicky, administrativně, logicky* i *technologicky*.

1.1 Problém ochrany dat v informačních systémech

Jak byly informační technologie aplikovány na moderní organizace, stalo se mnohem snažší informace shromažďovat, ukládat, manipulovat a šířit. Rozvoj informatiky v posledních letech přinesl potřebu shromáždění velkého množství dat v informačních

---

[20] RANNENBERG, Kai: *Recent Development in Information Technology Security Evaluation – The Need for Evaluation Criteria for multilateral Security.* In: Institut für Wirtschaftsinformatik, pdf. [cit.4.6.2011], s. 3 Dostupný na WWW <http://www.is-frankfurt.de/publikationenNeu/RecentDevelopmentinInformation>.

[21] Kritéria ITSEC specifikují sedm tříd zaručitelnosti bezpečnosti IT pod označením E0-E6. ITSEC jsou formulovaná obecněji než původně pro vojenské účely vytvoření TCSEC (Trusted Computer System Evaluation Criteria), která jsou zaměřená na ochranu důvěrnosti informací. (Srov. POŽÁR, J.: c. d., s. 50-52.)

[22] Tamtéž s. 52

[23] *New Approach to technical harmonization and standardization*. In: Portál EU, Summaries of EU Legislation, [cit.4.6.2011]. Dostupný na WWW <http://europa.eu/legislation_summaries/internal_market/single_market_for_goods/technical_harmonisation/l21001a_en.htm>

systémech a databázích. Dnes je pomocí počítačů možné zničit vlastní firmu, obchodní konkurenci, vykrást banku, odstavit jakoukoli síť, narušit vojenskou operaci, formulovat útoky přes síť, ideologicky či myšlenkově propojit lidi kdekoliv ve světě pomocí jakéhokoliv *elektronického zařízení.*

Vzniká tedy potřeba ochrany dat uložených, zpracovávaných a distribuovaných v informačních systémech. Tato data se musí ochránit před *neidentifikovanými* závažnými hrozbami. V případě informačních systémů by proto mělo jít o opatření směřující k zajištění trvalé *dostupnosti* nabízených služeb, k řízení přístupu k datům na základě přístupových práv a ochraně přenášených dat.

1.2 Proč data chránit?

Termín data je poměrně široký a těžko uchopitelný. Mohou sem patřit oblasti citlivých osobních údajů jako jsou rodná čísla, data narození, kontakty v adresářích, profily na sociálních sítích, historie navštívených webových stránek, digitální stopy, dokumenty, fotografie, data z platebních transakcí či obsah elektronické korespondence.[24] Nejen v informatice platí, že každá ochrana, každé omezení nebo zneužití je vykoupeno určitou cenou. Současná doba je založena především na *dostupnosti a integritě informací*,[25] které je potřeba si vyměňovat na veřejné síti. Organizace jsou v podstatě *závislé* na datech, které je nutné si distribuovat přes veřejnou síť. Jedná se primárně o online banky, jež se neobejdou bez zabezpečení a zajištění integrity a dostupnosti dat na svých serverech.

Proč je ale tak důležité data chránit? Je tomu tak proto, že *data jsou nejcennější částí informačního systému, představují nejcennější aktivum každé organizace.* Při nesprávné ochraně se může přihodit, že dojde ke zneužití bankovních účtů, kdy se ke konkurenci mohou dostat utajované firemní strategie či konstrukční řešení. V současnosti nás proto nejvíce zajímají jednotlivá *datová úložiště*, jež se běžně ve firmách[26] používají.

---

[24] POŽÁR, Josef a kol.: *Základy teorie informační bezpečnosti*. Praha 2007, s. 16.

[25] *Information Security and Privacy.* In: OECD, Dostupný na WWW <http://www.oecd.org/department/0,3355,en_2649_34255_1_1_1_1_1,00.html [cit.5.4. 2011]. Zabezpečení přesnosti a kompletnosti informací a metod zpracování>.

[26] WINDLEY, Phillip. *Digital Identity*. Cambridge : O´Reilly Media, 2005. 254 s. ISBN 0596008783.

Nejčastějšími a nejaktuálnějšími důvody, proč chránit data, je především *vzestup cílených útoků.* [27] Narušení dat je i nadále předmětem vážných obav organizací a roste počet podniků, které zaznamenaly více než pět narušení dat během jednoho roku. Dalším důvodem může být neustále rostoucí počet společností, které úspěšně implementovaly technologie pro šifrování dat.[28] Smyslem ochrany dat je uvědomit si, co by pro nás znamenalo zcizení či modifikace dat a jaké hroby z toho plynou. Existuje množina pravidel a mechanismů pro zabezpečení důvěrnosti, integrity a dostupnosti dat spojená se snahou čelit možným hrozbám zevnitř i zvenčí? A jaké jsou v současnosti nejvíce ohrožené cíle internetových útočníků? Největší trendem mezi zneužívanými službami, podle nedávno vydané zprávy společnosti McAfee[29] (v první třetině roku 2011), jsou služeb pro zkracování odkazů, geolokační služby,[30] cílené sociální inženýrství a malware.

Cíle útočníků

- krádeže dat
- zničení dat
- destabilizace systému
- blokování místa nebo určitých zdrojů

V tomto reportu společnosti McAfee se dále píše, že v prvním čtvrtletí roku 2011 přibylo malwaru podepsaného různými bezpečnostními certifikáty, v mnoha případech podvrženými. Útočníci dokázali stále účinněji maskovat odesílatele/autora škodlivé zprávy a předstírat, že jím je někdo, koho adresát zná. Tyto útoky se stále více soustřeďovaly na

---

[27] Směrnice 2002/58/ES o zpracování osobních údajů a ochraně soukromí. Úřad pro ochranu osobních údajů**.** [online]. [cit. 4.3. 2011]. Dostupný na WWW: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:CS:NOT>.

[28] STEWART, James Michael. *CompTIA Security+Review Guide*. Indianopolis : Wiley Publishing, 2008. 288 s. ISBN 9780470404843.

[29] *Virtual Criminology Report – Cybercrime: The Next Wave.* In: McAfee, [cit. 5.5. 2011]. Dostupný na WWW: <https://secure.mcafee.com/it/resources/reports/rp-quarterly-threat-q1-2011.pdf>.

[30] (pozn.: prostřednictvím několika málo kliknutí lze snadno zjistit, kdo, s kým a odkud prostřednictvím sociálních sítí komunikuje, odkud pochází, kdy lidé „chatují“, jaké informace si vyměňuji i jaké používají operační systémy apod.) *Virtual Criminology Report – Cybercrime: The Next Wave.* In: McAfee, Dostupný na WWW: https://secure.mcafee.com/it/resources/reports/rp-quarterly-threat-q1-2011.pdf. >. [cit. 5.5. 2011].

získávání citlivých dat. Firmy všech velikostí po celém světě byly vystaveny rostoucímu množství pokročilých a cílených útoků typu APT (advanced persistent threat),[31] které směřovaly proti archivům emailů, úložištím souborů, databázím a dalším citlivým datům/duševnímu vlastnictví firem.

1.3 Proti čemu data chránit?

Proti čemu data vlastně chráníme? V podstatě jde o to, aby relevantní informace byly dostupné oprávněným osobám pouze v nezbytně nutném rozsahu a jenom tehdy, kdy je to potřebné. Mezi nejznámější strategie kybernetických zločinců patří cílené útoky na hardware a software.[32] Cílené útoky totiž i přes zvýšené náklady přináší jejich původcům mnohem větší zisky než útoky náhodné, přičemž obrana proti cíleným útokům je zdaleka nejobtížnější. Spolu s jejich vyšší výnosností je to důvod, proč k tomuto posunu ve světě kybernetického zločinu dochází. Jako příklad cíleného útoku lze uvést červa Stuxnet. (Viz. Kapitola 11.1), kde se především jednalo o ochranu jednotlivých komponent informačního systému.[33] Jde o bezpečnost *hardware*, bezpečnost *operačního systému* nebo bezpečnost aplikačního *software*. Hardware zahrnuje samotné zařízení, které umožňuje provádět operace s daty. Software je řídící program, který určuje postupnost prováděných operací a zahrnuje i operační systém[34] (systémový software, který zajišťuje řízení a správu hardwaru a základní systémové operace).

Druhým typem je aplikační software, který provádí požadované manipulace s daty, například psání textu.

---

[31] APT (advanced persistent Great). Cílem útoků APT je většinou odcizit citlivá data a průmyslová sabotáž. Více viz Směrnice McAfee. Dostupný na WWW: <http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf> [cit. 4.4. 2011].

[32] Srov. Owens William A., Dam Kenneth W., Lin Herbert S., *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*, Committee on Offensive Information Warfare, National Research Council, USA, 2009.

[33] BANDYOPADHYAY, Samir Kumar ; KIM, Tai-hoon. A Cryptosystem for Encryption and Decryption od Long Confidential Messages. In *Information security and assurance : 4th international conference, ISA 2010, Miyazaki, Japan, June 23-25, 2010 : proceedings*. New York : Springer, 2010. S. 86 - 97. ISBN 9783642133640.

[34] Srov. také: BEAVER, Kevin ; MCCLURE, Stuart. *Hacking for Dummies*. 3rd ed. Indianapolis : Wiley, c2010. 408 s. ISBN 076455784X.

Informační systémy jsou atraktivním *cílem elektronického zločinu*[35] – proniknutí informací do veřejného oběhu. Data bychom měli chránit především proti *aplikačnímu softwaru,* což zahrnuje zejména:

1. Škodlivý software ("malicious software" = "malware"). Jedná se o takový software, jehož účelem je narušit bezpečnost informačního systému. Škodlivý software získává přístup k osobním informacím a provádí jiné nežádoucí příkazy v počítači. Lze jej rozlišit například podle jím prováděných činností, mezi něž nejčastěji patří:

- zničení data a software v počítači
- zablokování počítač
- získání důvěrné informace
- zneužití počítače

Tento malware je útočníky využíván ke sledování zvyklostí týkajících se procházení Internetu či krádeží hesel anebo může útočník získat vládu nad napadeným počítačem. Škodlivý software se do počítače nainstaluje sám, aniž by o tom uživatel věděl, nebo se může nainstalovat s programem, který si uživatel stáhnul z internetu. Vhodnou typologii možností zneužití [36] počítače nabízí i D. Nicol, W. Sanders a K. Trivedi.[37]

2. Možnosti zneužití počítače:

- zapojení do útoků na dostupnost jiných počítačů („distributed denial of service attack" = „DdoS attack")
- rozesílání nevyžádané (většinou reklamní) elektronické pošty – tzv. „spam"[38]

---

[35] Podobným způsobem se diskutuje i v *CISSP: Certified Information Systems Security Professional study guide*. Edited by Ed Tittel, Mike Chapple, James Michael Stewart. San Francisco, Calif. ; London : SYBEX, 2003. xlv, 783 s. ISBN 0782141757.

[36] O těchto zneužitích více ve: Lord William, *USAF Cyberspace Command: To Fly and Fight in Cyberspace*, Strategic Studies Quarterly, Fall 2008, USA, 2008.

[37] Nicol D., Sanders W., Trivedi K., *Model-Based Evaluation: From Dependability to Security* in *IEEE Transcript on Dependable and Secure Computing* 1, No.1, January-March, USA, 2004.

Dalším problémem je zobrazování nevyžádané reklamy, přesměrování webového prohlížeče na reklamní stránky apod. – tzv. reklamní software („adware“). Kromě klasických souborových virů, které dnes již netvoří největší část znečištění počítače, se můžeme setkat s ohroženími (jedná se o programová ohrožení)[39] označovanými jako Červ (Worm), Spyware, či Adware. Proto si jednotlivé typy zde představíme:

1. **Počítačový vir** – program, který se šíří bez vědomí uživatele
2. **Trojský kůň** – skrytá část programu nebo aplikace provádějící funkce, se kterou uživatel nesouhlasí
3. **Červ (worm)** –druh superviru, jehož šíření je založeno na bezpečnostních chybách
4. **Back-doors** – (zadní vrátka), které následně umožní útočníkovi ovládat a sledovat počítač
5. **Phising** – podvodný email snažící se vylákat důvěrné informace – hesla atd**.**
6. **Hoax** – poplašná zpráva
7. **Spyware** – software sleduje uživatele nebo informace o jeho počítači a data odesílá
8. **Rootkit** – program k zamaskování určitých aktivit na počítači

Škodlivý software napadl během 12 měsíců počítače dvou třetin uživatelů internetu v Evropské unii.[40] (v Česku 26 %). Nejčastěji měli vir v počítači weboví uživatelé v Bulharsku, kde škodlivý software do počítače pronikl 58 % ze všech bulharských počítačových uživatelů, jak vyplynulo z průzkumu Eurostatu.[41] Na Slovensku napadl vir počítač 47 % PC uživatelů, což je třetí nejvyšší podíl hned po zmiňovaném Bulharsku a Maltě s 50 %. Naopak nejméně škodlivý software pronikal do počítačů v Rakousku s pouhými 14 %

[39] Srov. Mazanec Brian M., *The Art of (Cyber) War* in *The Journal of International Security Affairs*, Spring 2009 – Number 16, USA, 2009.

[40]Srov. Mosca Carlo, Gambacurta Stefano, Scandone Giuseppe, Valentini Marco, I *Servizi di Informazione e il Segreto di Stato (Legge 3 gennaio 2011, n.124)*, Giuffré Editore, Milano, 2011.

[41] Srov. *www.epp.eurostat.ec.europa.eu* [online]. 7.3.2010 [cit. 3.7. 2011]. Dostupný na WWW < http://epp.eurostat.ec.europa.eu/portal/page/portal/information_society/data/main_tables>.

napadených počítačů, Irsku s 15 % a Finsku s 20 %. Podle Security Intelligence Operations,[42] která Cisco Security Report vypracovala, se zisky z hromadných útoků meziročně snížily o více než polovinu, z 1,1 miliardy USD v červnu 2010 na 500 milionů USD v červnu 2011. Množství spamu pak v těchto měsících dokonce kleslo z 300 miliard na 40 miliard za den. Například takzvané „spearphishingové útoky“[43] přinášejí i přes svůj malý objem a větší finanční náročnost na provedení desetkrát větší zisky než hromadné útoky. Předchází jim pečlivější příprava, jsou často sofistikovanější a využívají metod sociálního inženýrství.

[42] Srov. další podobně zaměřená statistika www: *epp.eurostat.ec.europa.eu* [online]. 7.3.2010 [cit. 3.6. 2011]. Dostupný na WWW <http://epp.eurostat.ec.europa.eu/portal/page/portal/information_society/documents/Tab/What%20is%20where%20on%20Eurobase%20status%2008032011.pdf>.

[43] Útoky, které jsou personalizovanou obdobou klasického masového phisingu. Více o tzv. spearphishingových útocích se dočteme v Mosca Carlo, Gambacurta Stefano, Scandone Giuseppe, Valentini Marco, I *Servizi di Informazione e il Segreto di Stato (Legge 3 gennaio 2011, n.124)*, Giuffré Editore, Milano, 2011.

KONCEPT „INFORMATION ASSURANCE“ APLIKOVANÝ V ŘÍZENÍ INFORMAČNÍCH SYSTÉMŮ

Koncept „Information Assurance“ je základním stavebním prvkem služeb *nepopiratelnosti*, *integrity* a *důvěryhodnosti* přenosu informací. Obecné prvky tohoto konceptu bezpečnosti jsou nezbytným předpokladem bezpečnosti komunikačních procesů (komunikačních sítí). Informační bezpečnost můžeme definovat jako vzájemně provázaná opatření organizační, administrativní, personální a fyzické bezpečnosti a opatření bezpečnosti ICT za účelem zajištění *dostupnosti*, *důvěryhodnosti* a *integrity* informací.[44] V podstatě se jedná o to, aby relevantní informace byly dostupné oprávněným osobám pouze v nezbytně nutném rozsahu a jenom tehdy, kdy je to potřebné.

Koncept „Information Assurance“je často považován za nejvhodnější standard, [45] kterým bezpečnostní funkce mohou být zajištěny. Definice pojmů podle „Information Assurance“ jsou následující:[46]

Bezpečná komunikace

- oba komunikující partneři věří na základě vzájemné autentizace,[47] že komunikují s oznámeným partnerem nebo že přijali zprávu z autentizovaného zdroje
- přenášená informace nemůže být odposlouchána, neboť je zajištěna její *důvěrnost*
- přenášená informace není změněna, neboť je zajištěna její *integrita*

---

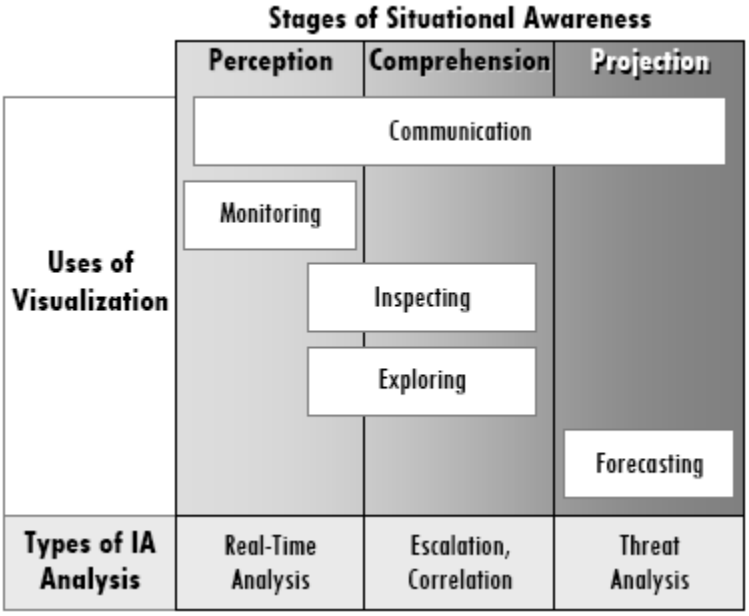
[44] Blyth Andrew, Kovacich Gerald L., *Information Assurance: Security in the Information Environment (Computer Communications and Networks)*, Springer, USA, 2006.

[45] Velmi zajímavou studii týkající se uplatnění konceptu“Information Assurance“ nabízí i italský profesor Dott. Antoni Arije. Antinori Arije, *Information & Communication Technology (I.C.T.), tra mutamento sociale e sicurezza. Uno sguardo al futuro* in *Quaderno dei lavori 2008*, C.I.R.S.D.I.G, Centro Interuniversitario per le Ricerche sulla Sociologia del diritto, dell'Informazione e delle Istituzioni Giuridiche, Messina, 2009.

[46] Landree Eric, Gonzales Daniel, *Implications of Aggregated DoD Information Systems for Information Assurance Certification and Accreditation*, RAND Corporation, USA, 2010.

[47] Autentizace se zde řeší proto, že představuje *nejčastější* hrozbu útoků na tyto bezpečnostní mechanismy a v současnosti je stále více oblíbenou součástí mnoha portálů a webových aplikací.

- komunikace je umožněna pouze *autorizované straně*, neboť je uplatněno *řízení přístupu*
- komunikace nemůže být popřena, neboť je zajištěna *nepopiratelnost* odeslání i přijímání zpráv



Obr. č. 1: Fáze situačního vědomí (Stages of Situational Awareness)[48]

Možnost implementovat bezpečnostní funkce ukazuje předcházeející tabulka. Budování informační bezpečnosti obnáší zajištění interních i externích lidských zdrojů, vyhrazení finančních prostředků, zodpovědnost a v neposlední řadě i smíření se s faktem, že řešení bezpečnosti je nikdy nekončící proces. Podnětem k budování informační bezpečnosti jsou bezpečnostní rizika (ohrožující data a informace), která mohou pocházet z různých zdrojů. Dle určitého zjednodušení rozeznáváme rizika personální, administrativní a technická. V prvním případě selhává personální faktor, ke kterému se přidávají faktory obvykle též spočívající v personální rovině, kdy zaměstnanci zodpovědní za bezpečnost a výpočetní techniku nesplnili své povinnosti nebo podcenili hrozící nebezpečí. Člověk je nejslabším článkem v celém informačním procesu, co se možnosti zneužití týče. Personální rizika jsou ovlivněna životními postoji, psychikou člověka, zainteresováním na pracovním úkolu a celkovým přístupem k dané problematice. V případě úmyslně promyšleného útoku pachatel vychází ze znalosti vnitřního systému, disponuje určitou úrovní oprávnění přístupu a nic mu

[48] Dostupný na WWW: <http://www.securedecisions.com/Members/admin/information-assurance-visualizations/2007-11-12.5465270995/image >. [cit.1.5.2011].

nebrání k provedení útoku.[49] Proto je třeba implementovat dle konkrétní situace účinná technologická opatření, například šifrování síťové komunikace, používání antivirových a antispywarových programů, pravidelné provádění aktualizací, implementace firewallu anebo organizační opatření ve smyslu vypracování bezpečnostních pravidel, směrnic, oddělení intranetu od internetu, časově rozlišených přístupů, certifikace systémů, sofistikované a silné autentizace – (biometrie, používání silných hesel atd.).

1.4 Ochrana logického přístupu k datům

Ochrana logického přístupu k datům patří mezi klíčovou a kontrolní část zabezpečení celého systému, neboť je pro nás částí, která znamená zabránění neautorizovaného využití, zničení nebo momentální či trvalé nedostupnosti informací. Znamená v prvé řadě to, aby se k datům nedostal nikdo, kdo nevlastní přístupová práva, jedná se tak o ověření identity uživatele. Je základním stavebním prvkem bezpečnosti systému, při dodržování nastavených principů mnohonásobně zvýšíme bezpečnost informačního systému, přičemž musí být vyjádřena hierarchie přidělování přístupových práv. Tento typ ochrany je pro nás stěžejní částí, neboť pokrývá celý koncept „Information Assurance.“ [50]

Většina informačních systémů využívá nějaký přístup pro uchovávání a přístup k datům. Zabezpečení dat je množina pravidel a mechanismů pro zajištění důvěrnosti, integrity a dostupnosti dat, která je spojena se snahou bránit data *zvenčí.* Zabezpečení dat se skládá ze tří úrovní:[51] *fyzické* (úroveň hardwaru, zálohování dat), *logické* (softwarové metody pro autentifikaci/autorizaci) a *organizační* (doplňková snaha o ochranu systému). Logické metodě se budeme věnovat do hloubky, protože tvoří kontrolní část zabezpečení celého systému.

---

[49] Qian Yi, Tipper David, Krishnamurthy Prashant, James Joshi, *Information Assurance: Dependability and Security in Networked Systems*, Morgan Kaufmann, USA, 2008.

[50] Hierarchie vyjádření přístupových práv v souvislosti s konceptem Information Assurance můžeme najít i v díle dalšího italského odborníka. Srov.Buonomo Gianni, *La responsabilità del gestore del sistema informatico per omessa adozione di misure di sicurezza in forum multimediale La società dell'informazione - Una rete di norme per il mondo in rete*, InterLex – Diritto, Tecnologia, Informazione, 29 gennaio 1996.

[51] Schou Corey, Shoemaker Daniel, *Information Assurance for the Enterprise: A Roadmap to Information Security*, McGraw-Hill, USA, 2006.

Do podmínek pro *logické* vrstvy bezpečnosti spadá::[52]

- zajištění důvěrnosti dat (confidentality)
- ochrana integrity dat (integrity)
- zajištění dostupnosti dat (availibility):

Ochrana logického přístupu k datům je založena tom, aby do systému neměl přístup uživatel, který k tomu nemá dostatečná přístupová práva. Pro tento účel musíme tedy dostatečně ověřit *identitu* uživatele. Systém tedy potřebuje *důkaz,* že se jedná o tu osobu, za kterou se objekt vydává. Před vlastní autentizací uživatele musí proběhnout *identifikace,* v níž uživatel potvrdí, že je skutečně tím, kým se prohlašuje být.

Nežádoucí odhalení (disclosure), modifikace (alteration) nebo zničení (destruction) určitých informací může vést k finanční ztrátě, poškození informací. Z těchto důvodů je nutné informace před narušením důvěrnosti (confidentality), dostupnosti (availability) a integrity (integrity) odpovídajícím způsobem chránit, a to během celého jejich životního cyklu. Cílem takové analýzy je identifikace informací, které společnost zpracovává a dále určení hrozeb, které by mohly ohrozit důvěrnost, integritu a dostupnost těchto informací. Pro uplatnění konceptu „Information Assurance" je nutné uplatnit tyto čtyři základní pilíře:[53]

1.4.1 Dostupnost (Availability)

Dostupnost klade důraz na zajištění *dostupnosti* a *důvěrnosti* informací bez zajištění jejich *integrity*. Znamená tedy přístup do informačních služeb pro oprávněné uživatele, tedy zajištění toho, aby oprávněné subjekty měly přístup k informacím nebo informačním službám, ale bez zajištění jejich *integrity* může dojít k situaci, že informace jsou sice oprávněné osobě dostupné v okamžiku, kdy je potřebuje, avšak tato osoba nemá žádnou záruku, že nedošlo k jejich nežádoucí modifikaci. Uživatelům zajišťuje i spolehlivý přístup k aktuálním údajům informační služby pro autorizované (důvěryhodné) uživatele. Zahrnuje také včasnost poskytovaných informací. V širokém smyslu se tak jedná o požadavek důvěryhodnosti (přenášení informací v určitém pořádku, určité souslednosti). V neposlední řadě *dostupnost*

---

[52] Qian Yi, Tipper David, Krishnamurthy Prashant, James Joshi, *Information Assurance: Dependability and Security in Networked Systems*, Morgan Kaufmann, USA, 2008.

[53] Tamtéž, s. 27.

značí schopnost předat informace. Jakékoliv zpoždění při předání informace uživateli je považováno za proces znehodnocení (narušení) informace.

4.1.1 Integrita (Integrity)

Zajištění *integrity* odráží přesnost a spolehlivost informačního systému, logickou úplnost hardware a software, který realizuje ochranné mechanismy a zabezpečuje konzistenci datových struktur. Znamená ochranu proti neoprávněné změně nebo zničení informací, představuje tak celistvost systému nebo jeho komponentů, což zajišťuje přesnou shodu mezi odesílateli a přijemci informací při procesu přijímání beze změny archivovaných dat.[54] Pokud budeme klást důraz jen na zajištění *důvěrnosti* a *integrity* informací bez ohledu na zajištění jejich *dostupnosti*, může dojít k situaci, že informace jsou sice dostatečně chráněny proti nežádoucí modifikaci a vyzrazení, ale nejsou dostupné v okamžiku, kdy s nimi oprávněná osoba potřebuje pracovat.[55]

Poznamenáváme, že narušení tohoto atributu dává příležitost *tzv. škodlivým kodům,virům, červům, malware, trojským koním a dalších škodlivým kodům.* Je zajímavé, že pro aktivaci výše uvedených kódů musí být použito aktivního chování, ale ne nutně ze strany uživatele vědomého, které provede instalaci softwaru, nebo prostřednictvím připojení dalších zařízení. V tomto smyslu je daný systém vystaven hrozbám, na které je třeba myslet dopředu, za účelem identifikace bezpečnostních nástrojů a obecněji činnosti zaměřené na ochranu a zabezpečení informací obsažených v tomto systému.

4.1.2 Autentikace (Authentication)

Jedná se o bezpečnostní opatření k určení platnosti přenosu zpráv od uživatele k příjemci. Jedná se o zprávu anebo prostředníka, který ověřuje osobní oprávnění. Atribut souvisí s principem včasné zpětné vazby, která ověřuje identitu.[56] Respektive identita

---

[54] Srov. Willett Keith D. *Information Assurance Architecture*, Auerbach Publications, USA, 2008, s. 201

[55]. „Lidský faktor, se ukáže být tím nejdůležitějším, pokud se jedná o atribut integrity. Ve skutečnosti, především dobrovolné změny údajů obsažených v daném systému, mohou vést k nenapravitelnému poškození systému, instituce, firmy, ale také v celé škále relevance dotyčných informací.“ Baskerville R., *Information Warfare: a comparative framework for Business Information Security* in *Journal of Information System Security*, 1, USA, s. 18, 2005.

[56] Abychom se v celé problematice orientovali, musíme si tedy ujasnit základní pojmy. *Autentizace* tedy znamená *ověřování pravosti* identity **(kdo je to).** Dalším pojmem je autorizace, která znamená *oprávnění* pro určitou činnost **(co může)**. Je důležité zde zmínit, že *autentizace* je základním předpokladem *autorizace*. To

uživatele je pak striktně ovlivněna přístupem do systému a je použita pro všechny komponenty integrovaného připojení v souladu s technicko-provozním využitím za účelem dostupných zdrojů do systému.[57]

4.1.3 Důvěryhodnost (Confidentiality)

Tento atribut zabezpečuje, že informace nebude vyzrazena dalším jednotlivcům, procesům nebo neoprávněnému zařízení. Týká se zachování a ochrany citlivých informací a za tímto účelem zajišťuje oprávnění pro použití úzkému počtu uživatelů, kteří byli řádně informováni. Přístup k důvěrným informacím mají pouze ti, kterým byl přístup skutečně povolen. Jedná se o přístup k důvěrným informacím, kdy uživatel má práva kopírování a distribuce informací. V této souvislosti jde například i o hierarchickou úroveň k přístupu v ochraně dat.

4.1.4 Nepopiratelnost (Non-repudiation)

Nepopiratelnost označuje jistotu, že odesílatel dat má k dispozici důkaz o dodání zprávy a příjemce je uveden údaj o totožnosti uživatele. Tedy jde o to, že zdroj dat nemůže popřít odeslání informací. Jak uvádí Buonomo:[58] „*odesílatel nemůže popřít, že zprávu odeslal a příjemce nemůže popřít, že zprávu obdržel.“* Odesílatel dat má doklad o doručení a příjemce dat má k dispozici zprávu o poslání. Z hlediska technologického vývoje v oblasti informační bezpečnosti se jedná o *digitální podpisy, šifrování, elektronické certifikáty*, které vznikly právě proto, aby umožnily konkrétní potřebu bezpečnosti a ochrany dat.

Výměna informací související s informačně komunikační technologií je procesem, jehož kořeny sahají až do 50.let, a který probíhá paralelně s vývojem technologií pro zabezpečený přenos informací a komunikace v informačních systémech.

---

znamená, že v prvé řadě nás musí systém *rozeznat* od ostatních subjektů, a pak nám přidělí oprávnění pro dané činnosti.

[57] V praxi je potřeba rozlišovat dva pojmy – **autorizaci a autentizaci**, které jsou nesprávně považovány za synonyma. *Autorizace* je proces, při němž se ověřují (server či jiná entita) dostatečná práva pro přístup do určité oblasti pro vykonání akce. Dalším problémem je autentizace dat, které jsou *ochranou* jejich *integrity,* která spočívá v tom, že zabráníme neautorizované nebo nepatřičné modifikaci dat jiným než *autorizovaným* subjektům. A tedy tím zabráníme např. modifikaci stavu na účtech jiným než autorizovaným subjektům.

[58] Gianni Buonomo, *La responsabilità del gestore del sistema informatico per omessa adozione di misure di sicurezza in forum multimediale*. La società dell'informazione - Una rete di norme per il mondo in rete, InterLex – Diritto, Tecnologia, Informazione, 29 gennaio 1996

V rámci několika společných definic je nejpoužívanější definice vyvíjená na Ministerstvu obrany USA,[59] které v r. 2002 definovalo „Information Assurance“ takto:[60]

„Opatření, která slouží k obraně a ochraně informací a informačního systému zajištěním dostupnosti, integrity, autentizace, důvěrnosti a nepopiratelnosti. To znamená, že se zabývá ochranou prostřednictvím zdrojů, týkající se ochrany, detekce a reakce.“

Z výše uvedeného vyplývá, že ve většině případů je třeba věnovat pozornost všem bezpečnostním atributům, ne vždy je však možné a efektivní věnovat všem atributům stejnou pozornost, protože každé opatření něco stojí. V praxi se tak klade na některý atribut větší důraz než na ty ostatní. Jako příklad si vezměme transakční systém v bance. Je vcelku logické, že bude kladen spíše větší důraz na *integritu* a *dostupnost* než na *důvěrnost*, a to především proto, že veškeré transakce, které se uskutečňují v elektronické podobě, musejí být správně a v požadovaném čase zaúčtovány. Důvěrnost je jistě také důležitá a její zajištění je navíc vyžadováno zákonem, nicméně možná ztráta plynoucí z narušení důvěrnosti je ve většině případů mnohem nižší, než ztráta způsobená narušením integrity nebo dostupnosti. Je tomu tak proto, že za únik informací o klientech nebo jejich transakcích, pokud se na to přijde, může být sice udělena pokuta, ku příkladu na základě série občanských stížností a rozhodnutí o náhradě škody, ale ta zdaleka nedosahuje výše možných ztrát v případě narušení integrity nebo dostupnosti.

[59] Ministerstvo federální vlády ve Spojených státech, pověřené koordinací a řízením všech agentur a funkcí vlády vztahující se přímo ke státní bezpečnosti a armádě Spojených států.

[60] US Department of Defence, *Directive 8500.1 “Information Assurance”*, October 24, 2002. [cit.7. 4.2011].

DEFINICE A VYMEZENÍ KYBERTERORISMU

Vymezení kybernetického terorismu není snadné, protože vyžaduje velké množství přístupů a chápání, navíc je často v rozporu i základní terminologie. V čem se shoduje většina přístupů ke kyberterorismu je primární závislost na *infrastruktuře ICT,*[61] kterou využívají teroristické cíle různých skupin.[62] *Kybernetický terorismus* pak můžeme definovat jako představitele *aktivit* vedených nebo koordinovaných státem s cílem získat informační převahu[63] nebo vyřadit technologickou infrastrukturu protivníka.

Vymezení pojmu kybernetický terorismu je velmi komplikované a jeho uchopení je předkládáno více zdroji. Například Severoatlantský pakt definuje kybernetický terorismus jako: *„kybernetický útok užívající či zneužívající počítač nebo komunikační sítě za účelem způsobení dostatečné škody s cílem zastrašit společnost a mající ideologický podtext.“*[64]

Americké ministerstvo vnitra uvádí vysvětlení kybernetického terorismu coby kriminálního aktu vedeného 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. [65] Při definování a vymezování kybernetického terorismu se mnoho autorů (včetně McQuade a také Janczewskiho a Colarika) shoduje na společném střetu reálných subjektů ve virtuální realitě v tzv. *kyberprostoru (cybersapace).*[66]

---

[61]Mezi hlavní sektory závislé na IT infrastruktuře patří zeména: energetika, jaderný průmysl, zdroje a zpracování vody, bankovnictví a finanční sektor, pojišťovací služby, chemický průmysl, zpracovatelé ropy a plynu, soudní moc, bezpečnostní služby, univerzity, atd.

[62] Na kritickou ICT infrastrukturu jako primární akt při vymezení kyberterorismu upozornila např. významná kniha *Full Blown Cyber War: An Information Age War in the Making. Cyber War: The Third World War*. Nebo Srov. Též POŽÁR, Josef. Některé trendy informační války, počítačové kriminality a kyberterorismu. Dostupný na WWW: <http://www.svses.cz/skola/akce/konf/bezp05/texty/pozar.pdf>.

[63] Jeho součástí je tzv. informační válka neboli „válka o informace“. Srov JANCZEWSKI, Lech; COLARIK, Andrew. Managerial Guide for Handling Cyber-Terrorism and Information Warfare. London: IGI Global, 2005. 229 s. nebo Srov. McQUADE III., Samuel. Encyclopedia of Cybercrime. Westport : Greenwood, 2008. 232 s.

[64] EVERARD, Paul: *NATO and Cyber Terrorism*. In: *Response to Cyber Terrorism*. Amsterdam 2008, s. 118-119.

[65] EVERARD, Paul. 119 s.

[66] Srov. DENNING, Dorothy. *Georgetown University* [online]. 23. května 2000 [cit. 6.7. 2011]. Cyber Terrorism: Testimony before the Special Oversight Panel on Terrorism. Dostupný na WWW: <http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html>.

McQuade chápe *kybernetický prostor (cyberspace)* jako metaforu vyjádření virtuálního (ne-fyzického) prostředí vytvořeného propojením počítačových systémů v síti. Většina autorů v literatuře zdůrazňuje,[67] že v kybernetickém prostoru probíhají interakce mezi subjekty stejně jako v reálném světě, ovšem bez nutnosti jejich fyzické aktivity. Informace jsou sdíleny v reálném čase či s určitým zpožděním, lidé mohou nakupovat zboží, sdílet zkušenosti, prozkoumávat obsah, provádět výzkum, pracovat nebo si třeba hrát.[68]

Americká FBI pak tento jev vnímá jako *„politicky motivovaný útok na informační a počítačové systémy, počítačové programy a data.“*[69] Centrum pro strategická a bezpečnostní studia[70] podává vysvětlení kybernetického terorismu coby *„užití nástrojů počítačové sítě s cílem vyřadit národní infrastrukturu či zastrašit vládu i civilní obyvatelstvo.“*[71] M. Janoušek ve svém textu rozlišuje dvě základní formy kybernetického terorismu. První je čistě propagační či informační související s vyjádřením negativního postoje či odmítavou reakcí na konkrétní mezinárodní či národní dění skrze využití možností, jež skýtá kybernetický prostor.[72] Daleko závažnější a nebezpečnější je pak vedení kybernetického teroristického útoku proti informačním sítím s cílem jejich likvidace. Zde se však kybernetický terorista vystavuje dalšímu riziku, kdy si de facto zničí vlastní operační prostor. Na druhou stranu však získá informační převahu a maximální informační vítězství, kdy je atakovaný dezorientovaný a nemůže reagovat na případné další útoky na jiných místech. Teroristické skupiny také mohou využívat kybernetického prostoru pro kontakt se svými členy, často lokalizovanými po celém světě.[73] Tedy jedním z mnoha aspektů kyberterorismu je virtualita, tzv. kyberprostor, ve kterém probíhají boje nebo interakce mezi subjekty a je zde vytvořeno jakési elektronické

---

[67]Denning Dorothy E., *Information Warfare and Security*, Addison-Wesley Professional, UK, 1998., s. 81.
[68] McQUADE III., Samuel. *Encyclopedia of Cybercrime*. Westport : Greenwood, 2008. s. 115.

[69] HUBER, Jordana: *Cyber Attacks „Grossly Underestimated“. Industries lack technology and skill to counter dangerous hackers, security expert says.* In: Financial Post, 26. června 2009, [cit.4.6.2011]. Dostupný na WWW< http://www.financialpost.com/m/story.html?id=1731010>.

[70] EVERARD, Paul: *NATO and Cyber Terrorism*. In: *Response to Cyber Terrorism*. Amsterdam 2008, s. 118-119.

[71] JANOUŠEK, M.: c.d., s. 60. JANOUŠEK, Michal: *Kybernetický terorismus: terorismus informační společnosti.* In: Obrana a strategie, 2006, č. 2, [cit.1.5.2011]. http://www.defenceandstrategy.eu/cs/archiv/rocnik-2006/2-2006/kyberterorismus-terorismus-informacni-spolecnosti.html 3. července, 60-61.

[72] Parafráze JANOUŠEK, M.: c.d., s. 61-62.

[73] Parafráze JANOUŠEK, M.: c.d., s. 61-62.

prostředí pro komunikaci dat prostřednictvím sítí. Tento aspekt zde zdůrazňuji zejména proto, že klíčová infrastruktura je hlavním kritériem terče a zbraní v operačním prostoru. Veškerá fyzická a funkční klíčová infrastruktura je vedena přes boj v elektronickém prostoru[74] elektronicky prostřednictvím elektronických dat a elektronická data jsou také terčem operací.[75]

Tato existenční vazba současné společnosti a ICT je dána především tím, že veškeré transakční operace ve společnosti jsou přímo závislé *na infrastruktuře ICT*, integrované do všech struktur řídících systémů. Prostřednictvím ICT dochází k jejich využívání mezinárodními organizacemi, státními institucemi a rovněž soukromým sektorem, což je způsobeno především tím, že subtypem informační války je válka kybernetická, založená na zvyšování role informace ve společnosti.[76]

1.5 Kybernetická válka

Základem úspěšného vedení kybernetické války je využití ICT v masovém měřítku[77] a její aplikace v informačních systémech, na kterých je založena veškerá klíčová infrastruktura (ekonomika, finančnictví, hospodářství, vojenství), hospodářské, politické i mediální subjekty. [78]

Relativně velmi dobrou typologii kybernetické války, s jasnou koncepcí najdeme v díle Ann Shoebben, který, kromě dalších typů informační války, rozlišuje a podává přesnou definici války kybernetické:
Kybernetickou válku lze charakterizovat obecně jako:[79]

---

[74] MARTIN, Clemens; SCHELL, Bernadette. *Cybercrime: A Reference Handbook*. Santa Barbara: ABC-CLIO, 2004. 247 s.

[75] JANCZEWSKI, Lech.; COLARIK, Andrew. *Cyber Warfare and Cyber Terrorism*. London: IGI Global, 2007. 532 s.

[76] Srov. Webster, Frank. *Theories of the informatik society*. 317 s.

[77] což znamená podle nás, že tato válka je založena na použití *elektronických dat nástrojů* a technologií v masovém měřítku

[78] Podle studie RAND z roku 1995 kupř. 95 % vojenské komunikace cestuje stejnými sítěmi, které využívají civilní osoby a instituce (fax, telefon), tyto uzly představují zranitelné terče. (Srov. např SHOBBEN, Ann. Information Warfare: A Two-Edged Sword [online]. 1995 [citováno 5.4. 2011]. Dostupný na WWW: <http://www.rand.org/publications/randreview/issues/RRR.fall95.cyber/infor_war.html>.

[79] SHOBBEN, Ann. Information War and Cyberspace Security [online]. 1995[cit. 5.4. 2011]. Dostupný z WWW: < http://www.rand.org/publications/randreview/issues/RRR.fall95.cyber/>.

1) relativně levnou a anonymní
2) s nejasnými hranicemi - mezi privátním a veřejným sektorem, válkou a zločinem; samozřejmostí je zohlednění trans-teritoriality, tedy popření geografických hranic
3) boj, který nabízí množství příležitostí k manipulaci s percepcí v kyberprostoru
4) střetnutí, které nezná fronty, potenciální bitevní pole (bojiště) jsou všude, kde jsou přístupné sítě; přibližování (splývání) terčů útoku a jiných uzlů vytváří další zranitelná místa, (jde o faktory integrace a komplexity)[80]

[80] Na podobnou souvislost upozorňuje i HUBER, Jordana: *Cyber Attacks „Grossly Underestimated". Industries lack technology and skill to counter dangerous hackers, security expert says.* In: Financial Post, 26. června 2009, [cit.1.5.2011]. Dostupný na WWW: < http://www.financialpost.com/m/story.html?id=1731010>.

Tabulka č. 1: Užití modelu cíle k analýze útočného procesu

Typ útoku	Cílová vrstva	Technický efekt	Funkční efekt	Operační efekt
Rušení komunikace	Informační systém	Blokování signálu	Ztráta informací	Pozdržené nebo špatné rozhodnutí
Průnik do komunikace – krátké kontrolní zprávy	Informační management	Žádný – komunikační linka dále existuje	Špatné směrování informací, přetížení linky generováním chybných a diagnostických zpráv	Zdržení, zmatek
Průnik do komunikace – krátké informační zprávy	Rozhodovací proces	Žádný – komunikační linka dále existuje	Bezvýznamný	Zdržení, zmatek, špatné rozhodnutí
Viry	Informační systém	Paralyzování systému	Ztráta dat, ztráta funkčnosti uzlu	Pozdržené nebo špatné rozhodnutí
Červy	Informační management	Žádný – síťové linky dále existují a pracují	Zdržení nebo přetížení provázené ztrátou funkčnosti	Zdržení, úvahy o odstavení zasažených uzlů
Psychologické operace/propaganda	Rozhodovací proces	Žádný	Žádný	Ovlivnění rozhodnutí
Vojenské operace/PSYOPS	Rozhodovací proces	Žádný	Žádný	Manipulace s vnímáním (oklamání)

Zdroj: JOHNSON, L.S.: A Major Intelligence Challenge: Toward a Functional Model of Information Warfare[81]

[81] JOHNSON, L.S. *A Major Intelligence Challenge: Toward a Functional Model of Information Warfare* [online]. 1997 [cit. 1. 5. 2011] Dostupný na WWW: <https://www.cia.gov/csi/kent_csi/pdf/v40i5a07p.pdf>.

V této souvislosti si můžeme položit otázku, jaký je rozdíl mezi tradičním (vojenským) způsobem boje a kybernetickou válkou?

Tedy, Johnson touto typologií poukazuje na *elektronický aspekt* využívání ICT, kdy dochází ke zlevnění komunikace a snížení nákladů, neboť kybernetická válka nevyžaduje žádnou výlučnou vojenskou technologii ani speciální počet armádních vojáků. Dalším faktorem, který je v typologii zmiňován, jsou jakési „hranice bez terenních omezení."

Boj s manipulacemi v kyberprostoru nabízí možnost dezorientovat nepřítele a popřít teritorialitu.[82] Jak autor poukazuje, střetnutí nezná fronty, ani hranice. Zatímco ve vojenském střetnutí je obvykle kybernetický útok chápán jako podpůrná složka vojenské operace, v boji, která nabízí možnost integrace kyberteroristických nástrojů do vojenského střetnutí, v koncepci kybernetické války se pozornost přesouvá do oblasti infrastruktury.[83]

V další rovině může jít o vyjádření postojů skupiny jedinců propojených „mentálně," prostřednictvím sítě využívajících technickou infrastrukturu, bez ohledu na popření geografických hranic. S odkazem na typologii Ann Shoebben [84]to znamená, že útok může být veden odkudkoliv a kdykoliv, což znamená, že hranice jsou nejasné.[85]

Útoky způsobující škodu elektronických komunikačních systémů a IT infrastruktur ovlivňují mnohem více globální ekonomické a finanční toky než by se mohlo na první pohled zdát. Vedou totiž k šíření a ohrožení této kritické infrastruktury *novými* nástroji, které jsou limitovány pokročilostí IT technologií. S opětovným odvoláním na typologii kybernetické války Anny Shoebben, tak je velmi těžké odhadnout a rozpoznat útok samotný, neboť splývají terče útoku s dalšími zranitelnými místy. Náš přístup je charakterizován tím, že kybernetický boj je považován za boj vedený čistě v elektronickém prostoru za použití čtyř základních vlastností:

---

[82] Srov. SHIMEAL, T. - WILLIAMS, P.,DUNLEVY, G.: Countering Cyber War [online]. 2002 [cit. 1.5. 2011]. Dostupný na WWW: < http://www.cert.org/archive/pdf/counter_cyberwar.pdf>.

[83]Podobně jako jiné prvky moderní armády budou kybernetické síly s největší pravděpodobností integrovány do celkové strategie vedení boje jako součást kombinované operace. Srov. např. ROTSCHILD, Michael: *The Threat from within: the evolution of cyber attacks*. In: Computer Technology Review, březen-duben 2006.
„Z tohoto pohledu je právě tou klíčovou součástí, na které mnohé moderní armády závisejí, a této závislosti si jsou potenciální nepřátelé dobře vědomi." (SHIMEAL, T. - WILLIAMS, P.,DUNLEVY, G.: Countering Cyber War [online]. 2002 [cit. 1. 5. 2011]. Dostupný na WWW: <http://www.cert.org/archive/pdf/counter_cyberwar.pdf>.

[84] Srov. SHOBBEN, Ann. *Information Warfare: A Two-Edged Sword* [online]. 1995 [cit. 1.5. 2011]. Dostupné na WWW<http://www.rand.org/publications/randreview/issues/RRR.fall95.cyber/infor_war.html>.

[85] Tudíž může být např. zneužit íránský jaderný systém stejně tak např. ze strany Spojených států a stejně tak ze strany Velké Británie).

1. **Původ** – znamená zdroj, kterým byl útok spuštěn (stát nebo podporovatel útoku).
2. **Důsledky** – zda-li to byl útok, který způsobil škody.
3. **Motivace** – jestli měl útoky politický motiv.
4. **Složitost** – zda byl požadavek proveden za použití vlastních metod.

1.6 Motivace útoků v kybernetické válce

Dalším faktorem ve vymezení kyberterorismu je *motiv* útoků, který obvykle vede ke stopám politického ovlivňování, neboť představuje záměrný cíl a působí mnoho škod jak nacivilnímu obyvatelstvu, tak i na kritické infrastruktuře. Ve zkoumání kyberterorismu se tento aspekt objevuje velmi často a je nesmírně důležitý, a sice zejména při diskuzi o kyberterorismu, neboť nabývá i hodnotu citovou, čímž se stává velice podstatným faktorem při řízení intenzity útoků. Například podle definice Janczewskiho a Colarika[86] je kyberterorismus *„promyšlený nebo politicky motivovaný útok proti informačním a počítačovým systémům, počítačovým programům nebo datům, jehož výsledkem je násilí proti civilním osobám.“*[87] V pracích D.E. Denninga je kyberterorismu naopak považován za politický útok s konvergencí terorismu a kyberprostoru a je obecně chápán jako nezákonný útok proti počítačům, počítačovým sítím a informacím, které jsou v něm uloženy, nebo za účelem zastrašení nebo donucení vlády či obyvatel k podporování sociálních nebo politických cílů. [88]

Od jiných prostředků se počítačová technologie liší v tom, že je integrována do všech klíčových součástí infrastruktury, na které ostatní složky závisejí. Ucelený koncept v této problematice nabízí typologie úrovní založená na dosahu a intenzitě kybernetické války od autoů jako jsou Shimealle, Williams a Dunlevy, kteří předkládají tři možné alternativy kybernetické války: [89]

---

[86] JANCZEWSKI, Lech; COLARIK, Andrew. *Managerial Guide for Handling Cyber-Terrorism and Information Warfare*. London: IGI Global, 2005. s.105.

[87] Tamtéž, s. 112.

[88] Srov. D. E. Denning viz DENNING, Dorothy. *Georgetown University* [online]. 23. května 2000 Cyber Terrorism: Testimony before the Special Oversight Panel on Terrorism. [cit. 24.4. 2011]. Dostupný na WWW: <http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html>.

[89] SHIMEAL, T. - WILLIAMS, P., DUNLEVY, G.: Countering Cyber War[online]. 2002 [cit.1.5.2011]. Dostupný na WWW:<http://www.cert.org/archive/pdf/counter_cyberwar.pdf>.

1) kybernetickou válku jako doplněk vojenských operací – tedy nasazení v kombinované operaci

2) omezenou kybernetickou válku

3) neomezenou kybernetickou válku

Tento příklad jsem záměrně vybrala proto, neboť autoři[90] nenabízejí jenom tento klasický pohled na počítačové technologie, nýbrž výše uvedená typologie demonstruje také jejich integraci do vojenských operací a zároveň poukazuje i na jejich úroveň implementace. V každém případě kybernetická válka poukazuje na fakt, že ICT technologie jsou integrovány do civilních struktur, a tak se staly významnou zbraní i cílem. Počítačové technologie se proměnily v prvek integrovaný do moderních vojenských organizací a jsou tím pádem součástí vyspělé společnosti jako celku. Informační infrastruktura se stává platformou pro útoky a nástrojem používání jejich cílů. Shimeall, Williams a Dunlevy uvádějí dvě možnosti využití infrastruktury: jako zbraně – a tedy infrastruktura napadla samu sebe, například implementací škodlivého software (worms), anebo cílený zásah lidského operátora (hacking). Existenci technologické války ostatně dokládá i další zpráva McAfee z r. 2009,[91] která upozorňuje na problém hrozící technologické války. Už v roce 2007 mnoho expertů poznamenalo, že jsou vyvíjeny stále sofistikovanější počítačové útoky a že už se nejedná jenom o „špionážní útoky“ v kyberprostoru. Podle obdobných nálezů nadnárodních společností sídlících v USA panuje neshoda, zda-li použít či nikoliv termín „technologická válka,“[92] neboť ve skutečnosti subjekty soukromé i veřejnoprávní posilují svá vybavení v kyberprostoru, jež bývají definovány jako *„technologické závody ve zbrojení.“*[93] Termínem

---

[90] Nejobecněji ji můžeme rozumět jako kriminalitě, namířené přímo proti počítačům, jejich hardwaru, softwaru, datům apod., nebo v které vystupuje počítač či počítačová síť pouze jako nástroj pro páchání trestného činu Např. JIROVSKÝ, Václav. Kybernetická kriminalita . 2007. Pět problémů kybernality, s. 19

[91] *Virtual Criminology Report – Cybercrime: The Next Wave.* In: McAfee, [cit.1.4. 2011]. Dostupný na WWW: <http://www.mcafee.com/us/research/criminology_report/default.html>.

[92] Dokonce se poznamenává, že tady ta nahradila zbraně ze dvou světových válek.

[93] McAfee pověřil Good Harbor Consulting vypracováním zprávy a vedením výzkumu. Zpráva byla připravována Paulem B. Kurtzem, expertem v oblasti informační bezpečnosti., který byl držitel prestižní pozice předsedy Rady pro národní bezpečnost a vnitřní Rady bezpečnosti v Bílém domě za prezidentů Clintona a Bushe mladšího. Jeho tým provedl rozhovory s více než dvaceti experty v mezinárodních vztazích a bezpečnosti dat v informačních systémech. Tým hovořil s více než 20 odborníky v oblasti internetové bezpečnosti na celém světě s cílem posoudit jejich názory na definici počítačové války.

neomezená kybernetická válka v díle Shimealla, Williamse a Dunlevyse se vztahuje na útoky, motivované hlavně politickými účely kriminalitu. Neomezená kybernetická válka má ve svém rozsahu vojenské i civilní cíle, faktický dopad obětí má také ve fyzickém světě. Studie OWASP[94] sestavila první desítku, tzv. top ten žebříček, který odkazuje na rizika a dopady spojené s využitím slabých míst ve webových aplikacích na síti, kde vypracované studie expertů ukazují na několik společných indikátorů,[95] mezi nimiž můžeme uvést klasifikaci kybernetických zločinů *tzv. high tech* hrozeb, které jsou spojeny s moderními technologiemi a navazují na koncept „Information Assurance" (viz 1. kapitola). Mezi tyto faktory patří podle mnoha různých přístupů, a to zejména podle dopadu konkrétního skutku, z hlediska skutkových podstat, podle akčního plánu eEurope+[96] a podle společenského významu chráněných zájmů. My se budeme držet řazení podle mezinárodní dohody o kybernetickém zločinu vypracované Radou Evropy.[97]

1.7 Příklady digitálního pirátství

Mezi nejaktuálnější a nejdebatovanější příklady hrozeb a protiprávních jednání patří především výroba, distribuce a prodej produktů porušujících ochranné známky, autorská a patentová práva (veškeré nelegální stahování hudby, filmu či softwaru). Jejich ekonomické dopady jsou nedozírné. Studie OECD[98] k padělatelství a pirátství, která byla vydána v r. 2010

---

[94] Open Web Application Security Project. [cit.1.5.2011]. Dostupný na WWW: < https://www.owasp.org/index.php/Top_10_2010>.

[95] *Network and Information Society: Proposal for a European Policy Approach.* In: Portál EU, [cit.1.5.2011]. s. 3. Dostupný na WWW: <http://eur-lex.europa.eu/LexUriServ/site/en/com/2001/com2001_0298en01.pdf >.

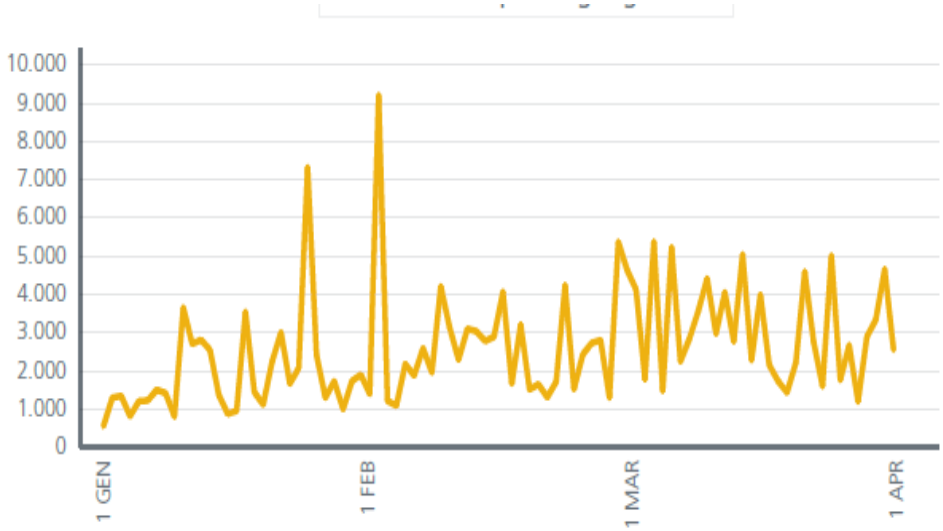
[96] Jedná se o akční plán Evropské unie, jehož podstatou je urychlení realizace základních stavebních prvků informační bezpečnosti. který má dva hlavní podbody. 1). urychlení přístupu k dostupným komunikačním službám pro všechny. 2). přijetí a implementace acquis (legislativy – pozn. autora) se vztahem k informační společnosti. *Critical Information Infrastructure Protection – a new initiative in 2009*. In: European Commission, Europe's Information Society, Dostupný na WWW: <http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/index_en.htm>. [cit.17.4.2011].

[97] Analýza současného stavu a trendů vývoje trestné činnosti na úseku informačních technologií a internetu včetně návrhu řešení, Ministerstvo ČR, s. 3-4; [cit.1.5.2011]. Dostupný na WWW: <http://aplikace.mvcr.cz/archiv2008/dokument/2006/informacni.pdf>.

[98] Srov.*Virtual Criminology Report – Cybercrime: The Next Wave.* In: McAfee. [cit.1.7.2011]. Dostupný na WWW: https://secure.mcafee.com/it/resources/reports/rp-quarterly-threat-q1-2011.pdf .

uvádí, že od r. 2000 obchod s padělaným zbožím neustále rostl a v r 2007 dosáhl hodnoty 250 miliard USD.[99]

Co se týče ztrát průmyslu způsobených nelegálním stahováním, v r. 2004 byly škody filmové sekce vyčísleny na 3,5 miliard dolarů a v roce následujícím to bylo již 5,4 miliard USD.[100] Dnes velmi populárním „sociálním inženýrstvím" jsou označovány *psychologické triky užívané na oprávněné uživatele systému za účelem získání přístupu do tohoto systému.* Jedná se o tak především o webové stránky, na které odkazuje spam nebo například o tzv. phishing. V praxi se jedná o pachatele, který se vydává za bankovní instituci používáním zfalšované adresy odesílatele; jeho cílem je vymámit z uživatelů důvěrné informace (číslo kreditní karty, čísla účtů, přístupové kódy). Za za období od prvního ledna do prvního dubna 2011 se můžeme podívat na následující celosvětové statistiky [101]z oblasti phishingu.



Obr. č. 2 Sociální inženýrství a phising za první čtvrtletí 2011

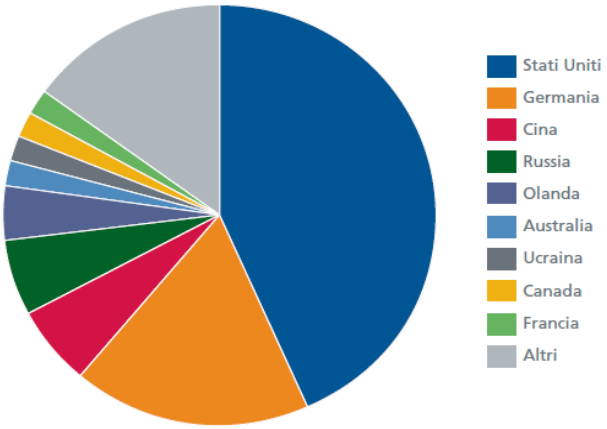
[99] *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. In: Organisation for Economic Cooperation and Development (OECD), [cit.1.7.2011].
Dostupný na WWW: <http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html>.

[100] *OECD Guidelines for the Security of Information Systems. Towards a Culture of Security*. [cit.1.7.2011]. In: Organisation for Economic Cooperation and Development (OECD). Dostupný na WWW: <http://www.oecd.org/dataoecd/16/22/15582260.pdf>.

[101] Srov. *Virtual Criminology Report*. In: McAfee, [cit.1.7.2011]. Dostupný na WWW: <http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q1-2011.pdf>.

Z obrázku je jasně patrné, že po rychlém nárustu v první polovině roku 2010 se počet phisingových stránek pravidelně zvyšoval a ustálil se až ve druhé polovině tohoto roku. V tomto čtvrtletí se identifikovalo asi 2 500 000 stránek za den se dvěma velkými výkyvy na přelomu ledna a února. Hlavními nástrahami v tomto měsíci byly Wells Fargo, PayPal a francouzské bankovní skupiny Caisse d'Epargne.

Dalším zajímavým případem je analýza za poslední trimestr 2010 (viz obrázek č.3), kdy se identifikovalo 14 nových míst denně, která se používají pro nelegální výměnu souborů chráněných autorským právem. [102] Tyto stránky se používali nejčastěji pro distribuci ilegálního softwaru nebo médií jako jsou hudba a filmy chráněných autorskými právy, nezákonných generátorů licenčních klíčů, hacker sofwarů a sériových čísel. Nejvíce je phishing rozšířený ve Spojených státech a v Německu, další příčky pak zaujímá Čína, Rusko a Nizozemí.



Obr. č. 3.[103] Sociální inženýrství a phising v podílu jednotlivých zemí za poslední trimestr 2010.

V Úmluvě Rady Evropy o počítačové kriminalitě se používá termín „počítačové trestné činnosti“ k popisování zločinů krádeže dat, modifikování obsahu a porušování autorských práv.[104] Nicméně existuje i širší definice,[105] která zahrnuje činnosti jakými jsou

[102] Srov. *Virtual Criminology Report*. In: McAfee, [cit.1.7.2011]. Dostupný na WWW: <http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q1-2011.pdf>.

[103] tamtéž

[104] Úmluva Rady Evropy o počítačové kriminalitě, Budapešť, 23. listopadu 2001, Convention on

internetové podvody, neoprávněný přístup, dětská pornografie a „cyberstalking.“ Podle manuálu[106] Organizace spojených národů pro prevenci a kontrolu počítačového zločinu do definice počítačové kriminality patří i podvod, padělání a neoprávněný přístup k informacím. Jak můžeme vidět z výše uvedených definic, digitální pirátství pokrývá velmi široké spektrum útoků. Je proto důležité pochopit rozdíly mezi různými typy digitálního pirátství, protože každý typ vyžaduje jiný přístup ve snaze o zlepšení zabezpečení počítače. Organizace Symantec[107] výstižně popisuje digitální pirátství jako *trestný čin spáchaný za použití počítače, sítě, nebo hardwarového zařízení, kde jsou to počítače nebo zařízení, které se stávají původci nebo cíli trestného činu.* Trestný čin může být proveden samostatně na jednom počítači nebo v kombinaci s jinými počítači a objekty. Pro lepší pochopení široké oblasti digitálního pirátství jej lze rozdělit do dvou kategorií, a sice jako digitální pirátství 1. a 2 typu.

Digitální pirátství 1. typu je obecně charakterizováno tak, že se z pohledu oběti jedná o jednorázovou akci. Například pokud si oběť nevědomky stáhne trojského koně tím, že otevře email s důvěryhodně vypadajícím odkazem, jehož rozkliknutím nainstaluje na počítač program zaznamenávají vše, co je na klávesnici napsáno. Tento typ zločinu je často umožněn tzv. *crimeware programy*, jež ke svému fungování využívají virů, rootkitů a trojských koňů nebo chyb ve webovém prohlížeči.[108]

Je zajímavé, že pro digitální pirátství 1. typu útočníci využívají chyb a zranitelnosti *softwaru*, čímž je poskytnuta silnější pozici útočníkovi. Do tohoto typu počítačové kriminality patří mimo jiné již zmiňovaný phishing, krádeže a manipulace s daty nebo krádeže identity a internetové podvody, například zde lze zařadit služby typu e-commerce.

Digitálního pirátství 2. typu je typické spíše nepřetržitou sérii událostí, které zahrnují opakovanou interakce s obětí. Například, oběť je v chatovací místnosti kontaktována s někým, s kým si během určitého časového období vytvoří osobní vztah. Zločinec využívá určité

Cybercrime - ETS no. 185. [cit.1.7.2011]. Dostupný na WWW: <http://conventions.coe.int/ >.

[105] Tamtéž

[106] LIDÍNSKÝ, Vít a kol.: *eGovernment bezpečně.* Praha 2008, s. 7.; viz také *E-governance and Access to Information.* In: Organizace spojených národů (OSN), Democratic Governance, [cit.1.7.2011]. Dostupný na WWW: <http://ictd.undp.org/e-gov/>.

[107] Manuál OSN pro prevenci a kontrolu počítačového zločinu, OSN 1994. Viz také *Symantec Global Internet Security Threat Report. Trends for 2008.* In: Symantec, červen 2011, [cit.1.7.2011]. Dostupný na WWW: <http://www.symantec.com/content/en/us/about/media/Symantec2009AnnualReport_Proxy_10-K.pdf >.

[108] Matějka, M., Počítačová kriminalita, Praha: Computer Press, 2002, str.37

vazby, které umožňují páchat trestnou činnost na oběti. Tento typ může zahrnovat i teroristické organizace, jež pomocí kódovaných zpráv komunikuje na veřejném fóru a domlouvá plán trestné činnosti jako například praní špinavých peněz.[109] Pro digitální pirátství 2. typu jsou charakteristické činnosti jako cyberstalking, špionáže a další nezákonné teroristické aktivity.

[109] Tamtéž, s. 36

METODY A TECHNOLOGIE KYBERNETICKÝCH ÚTOKŮ

Následující kapitola je jednou z nejdůležitějších, neboť si klade za cíl popsat a analyzovat nástroje a technologie, které jsou využívány pro účely kyberterorismu, zejména se jedná o trestné činy proti *důvěrnosti, integritě* a *dostupnosti* počítačových systémů. Na úvod jen je nutno zmínit, že nástroje a metody kybernetických útoků se samozřejmě neustále vyvíjejí a zlepšují.[110]

Jednotlivé programové prostředky, při kyberútoku nejčastěji používané, vycházejí v zásadě z využití tzv. škodlivého softwaru (malwaru). Jeho hlavní podoby jsou adware,[111] spyware,[112] trojští koně[113] a viry.[114] Zmínit je třeba také využití tzv. *vnitřního nepřítele* (insider threat).[115] Dále je nutné poznamenat, že tempo růstu množství malware se zvýšilo, v r. 2010 až o 50%, jak upozorňuje studie za rok 2010,[116] kdy byl nežádoucí trend nárustu malware zaznamenán hlavně prostřednictvím sociálních médií Twitteru a Facebooku. Tento trend dokládá i Virtuální kriminologická zpráva zpracovaná za poslední čtvrtletí roku 2011.[117]

---

[110] Srov. např. ROTSCHILD, Michael: *The Threat from within: the evolution of cyber attacks*. [cit.1.7.2011]. In: Computer Technology Review, březen-duben 2006.

[111] Adware je speciální programový prostředek sloužící k získávání informací a odposlouchávání na koncových bodech počítačových sítí. V ČR představuje adware nejčastěji šířený škodlivý kód. Na počítače uživatelů se většinou dostává jako součást instalace nejrůznějších zkušebních verzí programů stažených z internetu.

[112] Spyware je speciální softwarový doplněk sloužící k tajnému zasílání uživatelových osobních dat. Původně se jednalo o nástroj využívaný v cíleném marketingu.

[113] Trojští koně jsou speciální druhem počítačových virů, které jsou schopny skrýt svou pravou identitu. Obvykle jsou to tzv. programy zadních vrátek, které jsou schopné spustit určitou činnost v konkrétním čase a bez vědomí regulárního uživatele.

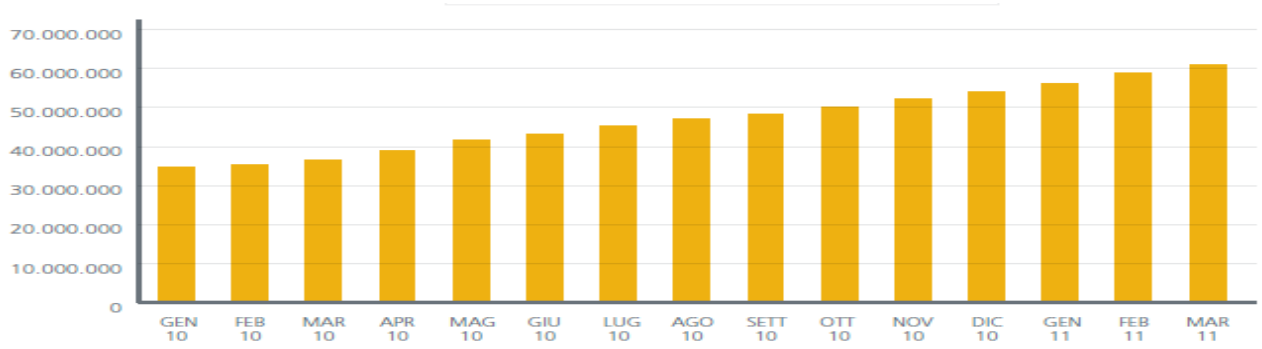
[114] Počítačové viry jsou speciální programové prostředky schopné znefunkčnit některé služby či procesy počítačové sítě.

[115] *Full Blown Cyber War: An Information Age War in the Making. Cyber War: The Third World War*. In: Cyberoam, [cit.1.7.2011]. Dostupný na WWW: <http://newsletters.cyberoam.com/072008/images/FullBlownCyberWar.pdf>.

[116] *The e-government imperative: main findings.* In: Organisation for Economic Cooperation and Development (OECD), Policy Brief, [cit.1.7.2011]. Dostupný na WWW: <http://www.oecd.org/dataoecd/60/60/2502539.pdf>.

[117] *Virtual Criminology Report*. In: McAfee, [cit.1.7.2011]. Dostupný na WWW: <http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q1-2011.pdf >.

Nejčastější technikou hacktivistů a hackerů se zájmem vyjádřit svůj postoj se stal *defacement*, který znamená *přetvoření, modifikování, nahrazení* webových stránek serveru jiným obsahem. Tato technika má na svědomí změnu nebo přesměrování původní webové stránky. Význam pro určité ohrožení kybernetické bezpečnosti je u této metody v možné při úpravě oficiálních informací, (např. úřední deska orgánu veřejné zprávy), které pak vedou k dezinformacím a zmatení uživatele. Rozvoj defacementu v poslední době může být demonstrován na statisíce napadání internetových domén. Pořadí národních domén na špičce vypovídá o momentální úrovni zabezpečení a charakterizuje pozici státu v globální politice.[118]



Tab. 4 Nárust malware za rok 2010 a počátek roku 2011[119]

Jak dokládá následující tabulka, malware je mnohem aktivnější než kdy jindy. Také bude zajímavé analyzovat jak si bude malware stát na konci roku. Podle současné studie McAfee Labs[120] můžeme soudit, že při současném tempu růstu dosáhne až 70 milionů výskytů.[121] Jak je vidět, malware zahrnuje především různé uživatelsky nepříjemné aplikace, které mohou mít za následek množství negativních dopadů na systém.

Velmi zajímavou skupinou infoware je defacement, neboli nahrazení stránek na webovém serveru jiným obsahem, a to zejména se záměrem vylepšení průkaznosti

[118] *Tracking GhostNet: Investigating a Cyber Espionage Network.* [cit.1.7.2011]. In: F-Secure. Dostupný na WWW: <http://www.f-secure.com/weblog/archives/ghostnet.pdf >.

[119] McAfee. *Zpráva společnosti McAfee o virtuální kriminalitě : první celoevropská studie o organizovaném zločinu a internetu* [online]. 2011 [cit. 24.4. 2011]. Dostupný na WWW: <https://secure.mcafee.com/it/resources/reports/rp-quarterly-threat-q1-2011.pdf>.

[120] BARBER, Richard: *Hacking Techniques. The tools that hackers use, and how they are evolving to become more sophisticated.* Computer. Fraud and Security. 1. března 2003, [cit.1.7.2011]. č. 3, p. 9-10.

[121] Tamtéž

provedeného průniku do systému. Ten je záměrně viditelný, pachatel totiž nahrazuje původní webové stránky a většinou vyjadřuje na vložených stránkách i svůj názor nebo názor skupiny (defacement patří do skupiny psychologického infoware).[122] Porovnáme-li nárůst počtu defacementů se vzrůstajícím počtem instalovaných hostů nebo instalovaných webových serverů, je zřejmé, že počet realizovaných útoků vzrůstá daleko rychleji.

Mezi současné trendy defacementu patří také zvyšující se počet útoků souvisejících s politickým, náboženským nebo názorovým střetem. Jako příklad můžeme uvést defacementy webových serverů v indické doméně, kde jejich počet vzrostl ze 45 na 250 během pouhých tří let.[123]

V případě, že se díky defacementu změnění obsahu vládních či armádních komunikačních kanálů, může být následkem také nesprávně vedená obranná akce.[124] Nicméně tzv. *intranet vládních i vojenských struktur*[125]je poměrně dobře chráněnou entitou a nesrovnalosti v něm je možné relativně rychle odhalit.[126]

Meziroční nárůsty jsou řádové, pořadí národních domén na špičce vypovídá o momentální úrovni zabezpečení a charakterizuje pozici státu v globální politice. Z útoků na národní domény není vynechána ani doména „.cz." K větším útoků na ni došlo na sklonku roku 2007 a v druhé polovině roku 2003. S výjimkou skupiny H131 se nejedná o skupiny,

---

[122] Infoware však není pouze předmětem vojenských aktivit. Rysy infoware nalézáme i v tzv. business infoware, které může být jak obranné (bezpečnostní kódy, šifrování), tak i útočné (od marketingových výzkumů až po průmyslovou špionáž nebo blokování internetových zdrojů). Zvláštní kategorií je civilní infoware, které zahrnuje akty občanské neposlušnosti od aktivismu až po informační terorismus. Personální infoware obvykle označuje kybernetické stopování a obtěžování (cyberstalking), digitální pomluvu, zneužití internetových stránek nebo velmi časté zcizení identity.

[123] GEERS, Kenneth: *Cyberspace and the changing nature of warfare*. In: SC Magazine, 7. dubna 2011, [cit.1.7.2011]. Dostupné na WWW: <http://www.scmagazineus.com/Cyberspace-and-the-changing-nature-of-warfare/article/115929/¨>.

[124] Tamtéž

[125] Význam pro určité ohrožení kybernetické bezpečnosti je u této metody v moýné úpravě oficiálních informací (např. úřední deska orgánu veřejné správy), které pak mohou vést k nesprávnému postupu. *Profile of a Real Cyberware.* In: The Washington Times, 5. srpna 2009, [cit.1.7.2011]. Dostupný na WWW: <ttp://www.washingtontimes.com/news/2009/aug/05/profile-of-a-real-cyberwar/>.

[126] *Profile of a Real Cyberware.* In: The Washington Times, 5. srpna 2010, [cit.1.7.2011]. Dostupný na WWW: <http://www.washingtontimes.com/news/2009/aug/05/profile-of-a-real-cyberwar/>.

které by se politicky profilovaly. Většinou byly napadeny systémy Linux a jednalo se o masový defacement.[127]

Další současnou metodou kybernetických útoků je tzv. *odepření služby (Denial of Service - DoS),* nebo-li také *distribuovaný DoS (Distributed Denial of Service - DdoS).* DDoS útoky jsou asi nejpoužívanější a nejpopularárnější formou útoků ve světě počítačové bezpečnosti. Tento typ útoku stojí za hromadnými ataky nepřátelských webů a za útoky pro odepření služby.[128]

Jak vlastně fungují Dos a DDoS útoky a které techniky se nejčastěji používají? Může jít o útoky, které cílí na konkrétní počítač anebo celou síť. Oproti jiným útokům je třeba podotknout, že útočníci nemají za cíl získat cenná data nebo přístup do systému, ale dojde pouze k vyřazení služby nebo sítě z provozu. Princip útoku Dos spočívá v zahlcení serveru s velkým počtem žádostí o připojení, což vede ke kolapsu a nemožnosti správně fungovat. DDoS útoky jsou speciální variantou DoS útoků, s tím rozdílem, že se na nich podílí více počítačů najednou.[129] Princip spočívá v připojení obrovského množství počítačů a v dostupné konektivitě na webový server, který nestíhá zpracovat a obsloužit kumulované požadavky. DDoS útoky mají výhodu v zesíleném efektu. DDoS útok funguje tak, že se zpravidla útočníci domluví na tom, aby byl útok proveden ve stejnou dobu a přesně ve stejný čas pak najednou vyšlou požadavky na server, který se chystají „shodit." Tento postup se nazývá *synchronizace.* Postupem času, ale uvedený přístup začal být neefektivní, neboť takový útok vyžaduje obrovské množství připojených uživatelů a složitější způsob *koordinace.* Útočníci proto začali používat tzv. *botnety,* tedy sítě vzdáleně ovládaných počítačů propojených pomocí škodlivého programu (trojský kůň apod.). Úkolem botnetů je opakovaně zasílat emaily či žádat o přístup na konkrétní webovou stránku. Infikovaným počítačům se někdy

---

[127] KREBS, Brian: *Report: Russian Hacker Forums Fueled Georgia Cyber Attacks.* In: The Washington Post, 16. října 2008, http://voices.washingtonpost.com/securityfix/2008/10/report_russian_hacker_forums_f.html (15th September 2009); MESERVE, Jeanne: Study Warns of Cyberwarfare during Military Conflicts. In: www.cnn.com/US, 17. srpna 2009, [cit.1.7.2011]. Dostupný na WWW: <http://www.cnn.com/2009/US/08/17/cyber.warfare/index.html >.

[128] MARSAN, Carolyn Duffy: *How close is World War 3.0?* Network World, 24, 27. srpna 2007, č. 33, s. 24; *Symantec Global Internet Security Threat Report. Trends for 2008.,* s.8.

[129] JIROVSKÝ, Václav – HNÍK, Václav – KRULÍK, Oldřich: *Základní definice, vztahující se k tématu kybernetických hrozeb*. In: Ministerstvo vnitra ČR, Dostupný na WWW: <http://web.mvcr.cz/archiv2008/bezpecnost/informacni/zakladni_info.pdf >. *eEurope – An Information Society for All*. In: Euractive.com, Dostupný na WWW: <http://www.euractiv.com/en/infosociety/eeurope-information-society/article-117472# >. [cit.1.7.2011].

také říká „zombie počítače," jelikož jejich běžní uživatelé nemusejí o jejich účasti v kybernetickém útoku ani vědět.[130] Botnety jsou považovány za novou internetovou hrozbou, neboť se jedná o druh kódů, který se šíří nepozorovaně a usazují se hluboko v co největším počtu systémů. V podstatě můžeme botnet definovat jako program, který je tajně nainstalován na uživatelském počítači, obsahuje komunikační a řídící modul a umožňuje neautorizovanému uživateli vzdáleně tento počítač ovládat a využít tak pro plnění různých příkazů. Podle odhadů antivirových společností se počet botnetů blíží k tisíci v rozmezí od velmi jednoduchých až po velmi složité.

Síla botnetu spočívá v tom, že kompromitované počítače provádí na povel jednotné příkazy v jednom okamžiku. Díky botnetu lze provést nárazový útok automaticky, velmi rychle a zaútočit na velké množství obětí zároveň, sítě botnetů se tedy používají na nebezpečných útocích Denial of Service (DoS odepření služby). Jedná se o velkou hrozbu pro ty organizace, které spoléhají na Internet jako prostředek pro komunikaci. Podle studie společnosti Symantec[131] vzrostl počet útoků DoS až o 50% oproti roku 2010 a za vzestupem útoků stojí pravděpodobně majitelé botnetů. [132]

Nejčastěji je ale botnet využíván pro řízení spamu, (dle skupiny Gartner Group je 70 % spamu rozesíláno právě z botnetů). Pro spammery je daleko výhodnější rozesílat spam z obrovské distribuované sítě jednotlivých počítačů, protože ty nejsou předem tak podezřelé jako unifikovaná síť a je jich tolik, že jejich odfiltrování je špatně proveditelné. Mezi dovednosti botnetů patří i typicky spywarové funkce jako *sniffing*. Botnetový modul změní napadený počítač v odposlouchávací stanici, jejímž prostřednictvím monitoruje síťový provoz a získaná data posílá hackerovi. Velmi oblíbené je také rozšíření botnetů o „keylogger," který registruje všechny výstupy z klávesnice. Takto může hacker získat uživatelská jména, hesla, čísla platebních karet, licenční klíče a další citlivé údaje. [133]

Sítě botnetů se stále častěji uplatňují při šíření nového malwaru, jak červů, tak virů. Pro hackera je důležité, aby se nový kód rozšířil co nejrychleji. Proto je nutné jej na počátku

---

[130] Srov např. BARBER, Richard: *Hacking Techniques. The tools that hackers use, and how they are evolving to become more sophisticated.* Computer. Fraud and Security. 1. března 2003, č. 3, p. 9

[131] BARBER, Richard: *Hacking Techniques. The tools that hackers use, and how they are evolving to become more sophisticated.* Computer. Fraud and Security. 1. března 2003, č. 3, p. 9-10.

[132] Tamtéž

[133] *Virtual Criminology Report – Cybercrime: The Next Wave.* [cit.1.7.2011]. In: McAfee, Dostupný na WWW <http://www.mcafee.com/us/research/criminology_report/default.html>.

epidemie začít rozesílat z co největšího počtu míst. Botnety se ale dají využít i pro rafinované podvody, mezi které řadíme ku příkladu zneužití reklamních systémů typu pay-per-click, kde počítače napadené botnetem jsou zneužívány pro automatické klikání na reklamní bannery a tvůrcům botnetu tak nesou nemalé zisky. Infikované počítače mohou být navíc kontrolovány na dálku, a lze tak upravovat seznam reklamních serverů, na které se mají soustředit, a také maximální počet kliknutí z jedné IP adresy. [134]

Jiným trendem dnešní doby je stírání hranic mezi jednotlivými typy malwaru.[135] Takové riziko představují „*zadní vrátka*“ (backdoor) do systému instalovaná různým malwarem (např. Bagle, MyDoom, Mytob). Tato otevřená *zadní vrátka* pak umožňují potenciální průnik zpravidla tak, že otevírají některé porty a na nich naslouchají povelům zvenčí.

Oblíbeným terčem hackerů je využití zranitelností produktů Microsoftu. Zákeřný kód se šíří prostřednictvím tzv. *exploitů* – programů, které využívají známou bezpečnostní chybu.

Současnou frekventovanost těchto typů nástrojů virtuálních útoků dokládá i typologie podle M. A. Vatise, který ve svém pozoruhodném díle „Cyber Attacks During the War on Terrorism“ považuje za klíčové červy, Dos útoky a neautorizované průniky.[136] Tento příklad jsem vybrala záměrně, neboť poukazuje na nejednotný terminologický rámec této problematiky, neboť *červ* je zde chápán jako relativně obecný pojem, který sám sebe klasifikuje na jednu rovinu s prvky v podstatě odlišnými. Nicméně podstatou červů je, že ke svému šíření používají neautorizovaných průniků. Červ je právě dosud vůbec nejkomplexnější záškodnický počítačový program, který v dnešní době dostává podobu superviru a nabývá nebývale ničivých rozměrů. Vysokým nebezpečím červů je právě replikace ve velkém množství dat, která rozesílá kopie sama sebe všem členům daného emailového adresáře, což má za následek tzv. *domino efekt*, který zpomaluje internet a vede k zahlcování webových stránek a jejich velkému zpomalení.[137] Příkladem může být například červ *Stuxnet* uvedený v

---

[134] Tamtéž

[135] Tamtéž, s. 6

[136] VATIS, M. A. Cyber Attacks During the War on Terrorism: A Predictive Analysis [online]. 2001 [cit. 1.5. 2011]. Dostupný na WWW: <http://www.ists.dartmouth.edu/ISTS/counterterrorism/cyber_a1.pdf>.

[137] Tamtéž, s. 21

kapitole č. 11.1 této práce. [138] Červ (worms) je tedy *typem* viru, jehož podstatou je *šíření* v operačním systému a *zneužívání* konkrétních bezpečnostních děr. Oproti tomu DoS útoky jsou jsou jedním z typů útoků na *software.* Můžeme tedy podotknout, že červ je *nástrojem* útoku, DoS je *typ* útoků na software a neautorizovaný průnik je způsob provedení útoku. Z tohoto příkladu vyplývá, že z metodologického hlediska jde o naprosto nesouměřitelné prvky.

Na kvalitativně vyšší úrovni stojí typologie vyvinutá Hosem,[139] která obsahuje 6 možných nástrojů či metod útoku:

1. Logické bomby
2. Trojští koně[140]
3. Červy
4. Zadní vrátka
5. Viry
6. Sniffery[141]

Naopak taxonomie vyvinutá Jírovským[142] zařazuje trojského koně a zadní vrátka do řádu implantační hrozby, která slouží jako základní typ podkladových hrozeb, jež mohou vést k realizaci několika základních z nich. Za nejškodlivější kyberteroristické nástroje se do budoucna považují červy, neboť pokud se namíří proti velkým serverům, způsobí nefunkčnost velkých internetových směrovačů v důsledku jejich zahlcení. Jestliže se dosáhne ještě určitých modifikací, jsou výsledky velmi destruktivní, neboť v současné době obsahují požadavek *komplexnosti,*[143] do kterého se integruje mnoho nových postupů a jedná se i o

---

[138] Tamtéž, s. 15

[139] HOS, Miroslav. *Terorismus a počítače*. In. Terorismus a my. Praha: Computer Press, 2001.

[140] Trojští koně patří mezi nejoblíbenější hackerské nástroje v současnosti a používají se pro různé účely. Od monitorovací činnosti cílového počítače až po zneužití pro útok DoS.

[141] Sniffing je jednoduše řečeno odchytávání komunikace v počítačové síti. Takto získané informace jsou určeny k dalšímu zneužití například v hackingu, nebo v tradičních formách trestné činnosti. K zachytávání komunikace existuje velké množství jak softwarových, tak i hardwarových prostředků. Takto lze získat veškerý obsah nešifrované komunikace, která prochází přes konkrétní uzel sítě. Nejedná se o nástroj útoku, ale spíše o prostředek shromáždění informací. Zajímavostí snifferu je například to, že dokáže analyzovat a složit přenášené informace tak, že výsledek je podobný typickému mailovému archivu ve formě webových stránek.

[142] HOS, Miroslav. *Terorismus a počítače*. In. Terorismus a my. Praha: Computer Press, 2001.

[143] Např. červ Stuxnet používá hned čtyř zranitelností ve Windows.

novou válečnou zbraň.[144] Například Szor v jedné ze svých nejautoritativnějších knih „Počítačové viry“ uvádí, že viry mají potenciál uplatnit se v kybernetickém boji dlouhodobě. Přispívá k tomu i fakt, že se explicitně kopírují a potencionálně vyvíjejí verze sama sebe.[145] Viry Szor chápe jako programy, které rekurzivně šíří buď samy sebe nebo své kopie, tím, že infikují soubory nebo systémové prvky či pozměňují odkazy na tyto objekty. Červy jsou pak, podle něj, viry, které se primárně šíří sítěmi, nicméně některé z nich používají metodu infikování souborů jako vedlejší metodu rozmnožování. To Szor pokládá za samostatný argument pro názor, že červy jsou podskupinou počítačových virů. U samostatných červů pak uvádí tři speciální podskupiny – červy rozesílající e-maily (buď jednotlivě nebo hromadně), dále takzvané „chobotnice“ (neboli červy tvořené sadou více programů rozmístěných na více než jednom počítači v síti) a „králíky“ (programy, které existují v každém okamžiku jen v jedné kopii, která se kopíruje sítěmi spojených hostitelských počítačů). V rámci dané definice je ovšem třeba upozornit, že typ programu šířící se sítěmi neodpovídá charakteristikám viru a dal by se považovat spíše za variantu svébytné třídy (útočných) nástrojů. Stejně tak je možné uvést jako oprávněné a skutečnost reflektující konstatování, že viry ke svému šíření potřebují vhodné prostředí. S tím je spojena i zatím nerozřešená terminologická otázka, zda jsou viry a červy svojí podstatou dva různé typy nástrojů (kódů), nebo zda jde v případě červů o podskupinu virů.

Nicméně například David Procházka[146] označuje viry za jen jeden *podtyp* tzv. malware, do kterého se v obecném smyslu (nesprávně) zařazují např. i červy a jiné druhy škodlivých softwarů. Poukazuje na rozdíl mezi nimi a konfrontuje ho na příkladu virů, které mohou být instančně ničivé (např. mazání souborů na disku) nebo se u některých virů ničivý kód spouští až s relativním zpožděním (např. k určitému datu či po nakažení určitého počtu jiných hostitelů, což se označuje jako *„logická bomba“).* Autor poukazuje na fakt, že nejdůležitějším negativním důsledkem šíření červů je však samotná skutečnost jejich reprodukce, která zatěžuje počítačové systémy, neboť viry se na rozdíl od červů sami šířit nemohou. Dnes jsou klasické počítačové viry na jistém ústupu oproti červům, kteří se šíří prostřednictvím počítačových sítí, hlavně Internetu. Ten samý rozdíl potvrzuje i Carl F.

---

[144] SZOR, Peter. *Počítačové viry – analýza útoku a obrana*. Brno: Zoner, 2006

[145] Tamtéž, s. 13

[146] Tamtéž, s. 7

Endor,[147] jenž vidí klíčový rozdíl mezi oběma v tom, že zhoubný kód buď vyžaduje ke své aktivaci nějakou akci nebo svoji činnost zahájí bezprostředně.[148]

Nicméně podle názoru Vatise[149] se zvyšuje počet útoků, což může souviset s faktem, že díky exploitům a skriptů se techniky útoků zpřístupňují i méně vzdělaným uživatelům. Přeneseno do roviny politicky motivovaných útoků to znamená, že se jednak zvyšuje jejich počet a zároveň roste jejich sofistikovanost. Útočníci napadají weby a šíří desinformace a propagandu, zaměřují se na útoky typu odmítnutí služeb legitimním uživatelům prostřednictvím DoS útoků, užíváním červů a virů a využíváním inherentních zranitelných míst počítačové bezpečnosti, a dopouštějí se tak neautorizovaných průniků do systémů a sítí, které mohou potenciálně vyústit ve vyřazení kritické infrastruktury a poškození životně důležitých dat. Zvyšuje se rozsah, sofistikovanost a koordinovanost kybernetických útoků a nejatraktivnějšími cíli pak jsou cíle s „vysokou hodnotou“ (sítě, servery a routery se symbolickou, finanční, politickou nebo faktickou hodnotou).

1.8 Příklady kybernetických útoků proti státu

Pokusy o počítačovou kriminalitu a průniky do klíčových řídících center klíčové části infrastruktury mohou ohrozit bezpečnost státu jako celku či alespoň jeho části.

V nejnovějších prohlášeních vlád snad všech zemí se setkáváme častěji než kdy jindy s úkolem zvýšit účinnost boje proti kyberkriminalitě, a ochránit tak státní struktury před kyberterorismem.[150] To může vést k vyšší efektivitě boje proti kyberterorismu, která v současné době přesahuje informační území vlastního státu a globální rozměr kybernetického konfliktu má charakter protiopatření, která často přesahují vlastní státní území. V rámci státních struktur je napadání důležitých počítačových systémů (např. jaderných elektráren) kriticky nebezpečné pro chod země a bezpečnost jejich občanů.

---

[147] Tamtéž, s. 26

[148] Některé viry/červy implementují několik různých infekčních mechanismů na různých infekčních frontách. (Např nedávný červ Nimda).

[149] VATIS, M. A. Cyber Attacks During the War on Terrorism: A Predictive Analysis [online]. 2001 [cit. 7.8. 2011]. Dostupný na WWW: <http://www.ists.dartmouth.edu/ISTS/counterterrorism/cyber_a1.pdf>.

[150] JONES, Andy – KOVACICH, Gerald L. – LUZWICK, Perry G.: *Global Information Warfare. How Businesses, Governments and Others Achieve Objectives and Attain Competitive Advantages*. Boca Raton 2002, s. 169.

Metody a motivaci útoků jsme si představili v předchozích kapitolách. V této se budeme věnovat konkrétním příkladům, jak lze skrze kybernetický prostor ohrozit integritu státu, jelikož atributy budoucích střetů začínají dostávat konkrétní struktury, takže po celém světě vznikají vojenské a špionážní struktury pro kybernetické útoky a obranu proti nim. [151]

1.8.1 Kybernetická špionáž

Kybernetická špionáž představuje rozšíření tradičního pojetí špionáže, tedy *nekooperativní* aktivity ve státě, do oblasti kybernetického prostoru za využití postmoderních nástrojů ICT.[152] Můžeme ji také definovat jako akt získání tajných informací bez svolení vlastníka za použití nezákonných metod (crecking, malware, spyware, trojští koně) prostřednictvím internetu, počítačových sítí či jednotlivých počítačů.[153]

Každoroční zpráva McAfee Virtual Criminology Report[154] zkoumá celosvětový vývoj trendů v oblasti kybernetické bezpečnosti. Vstupní data pro tuto studii pocházejí z NATO, FBI a SOCA (Serious Organised Crime Agency). Zpráva odhaduje, že v kybernetické špionáži je aktivních přibližně 120 států a Čína je na vedoucí pozici.[155] Tak, jak je výzvědná služba integrální částí bezpečnostních politik všech států,[156] stala se i kybernetická špionáž součástí bezpečnostních přístupů postmoderních států. Například Martin Hilbert z University of Southern California tvrdí, že roky 1986 - 2007 byly pro informační technologie obdobím dech vyrážejícího rozmachu. Americká CIA pak odhaduje, že státem sponzorovanou kybernetickou špionáží se zabývá 23 zemí s vedoucí pozicí Íránu, Sýrie a Indie.[157]

---

[151] Tamtéž, str. 167

[152] *Virtual Criminology Report – Cybercrime: The Next Wave.* [cit.1.7.2011]. In: McAfee, Dostupný na WWW: <http://www.mcafee.com/us/research/criminology_report/default.html>.

[153] Tamtéž.

[154] *Virtual Criminology Report – Cybercrime: The Next Wave.* [cit.1.7.2011]. In: McAfee, [cit.1.7.2011]. Dostupný na WWW: <http://www.mcafee.com/us/research/criminology_report/default.html>.

[155] WALTERS, Conrad: *Cyber cold war a threat to all.* The Sydney Morning Herald, 24. prosince 2007, [cit.1.7.2011]. Dostupný na WWW: <http://www.smh.com.au/articles/2007/12/23/1198344874193.html>.

[156] Přehled výzvědných služeb států světa viz např. stránky Federace amerických vědců (Federation of American Scientists, FAS), [cit.1.7.2011]. Dostupný na WWW <http://www.fas.org/irp/world/index.html.>.

[157] JONES, Andy – KOVACICH, Gerald L. – LUZWICK, Perry G.: *Global Information Warfare. How Businesses, Governments and Others Achieve Objectives and Attain Competitive Advantages*. Boca Raton 2002, s. 169.

Information Warfare Monitor[158] pak za lídry v oblasti kybernetické špionáže považuje USA, Velkou Británii a Izrael. Tyto země vnímají kybernetický prostor jako strategickou oblast podobně jako zemi, vzduch, moře a vesmír.[159]

Čína coby jeden z předních představitelů v této oblasti[160] využívá tzv. strategické kybernetické špionáže pro získávání informací o nových technologiích.[161] Cílem čínské kybernetické strategie je nelegální získávání dat, technických a ekonomických informací. Podle londýnského International Institute for Strategic Studies[162] se čínské útoky stupňují a zaměřují se na armádu a především na armádní dodavatele Spojených států. Čína se stala také jedním z prvních států, která začala používat tuto metodu oficiálně pro vojenské i politické cíle.[163] Čínští představitelé ohlásili vytvoření „jednotek informačního válečnictví" na 10. Národně lidovém kongresu v r. 2003. [164]

Potvrzuje to i nejnovější zpráva od bezpečnostních expertů z antivirové společnosti McAfee, podle níž se kybernetickým zločincům podařilo proniknout do 72 organizací, včetně OSN a Olympijského výboru. Cílem je získání dat pro vytvoření lepších konkurenčních produktů, které by mohly představovat ekonomickou hrozbu.[165] Dalším cílem je dosáhnout asymetrické výhody proti vojensky silnějším protivníkům (např. USA). Čína se stala také

---

[158] Kanadský veřejně-soukromý výzkumný ústav tvořený Centrem pro mezinárodní studia Torontské univerzity a think tankem SecDev Group a zabývající se výzkumem kybernetického prostoru coby nové strategické domény. V nedávné době vešel Information Warfare Monitor ve známost odhalením kybernetické špionáže vedené proti tibetské komunitě v exilu. Webové stránky ústavu viz http://www.infowar-monitor.net/. [cit.1.7.2011].

[159] *Virtual Criminology Report – Cybercrime: The Next Wave*. In: McAfee, [cit.1.7.2011]. Dostupný na WWW: <http://www.mcafee.com/us/research/criminology_report/default.html >.

[160] Posledním velkým projevem čínské schopnosti využívat možnosti kybernetického prostoru byl špionážní atak na tibetskou komunitu odhalený na jaře 2009.

[161] NAGESH, Gautham: *Latest Security Threat Lies in Trusted Software and Hardware*. [cit.1.7.2011]. In: Nextgov, Dostupný na WWW: <http://www.nextgov.com/nextgov/ng_20080825_7185.php>.

[162] *Tracking GhostNet: Investigating a Cyber Espionage Network* [cit.1.7.2011] , s. 7.
In: F-Secure, Dostupný na WWW: <http://www.f- secure.com/weblog/archives/ghostnet.pdf >.

[163] *Contemporary Security Threats within Cyberspace. NATO and EU Approaches to Cybersecurity*. Maria Enzersdorf, AIES 2009.s. 5

[164] MOORE, Malcolm: *China's global cyber-espionage network GhostNet penetrates 103 countries*. In: http://telegraph.co.uk, 29. března 2009, Dostupný na WWW: <http://www.telegraph.co.uk/news/worldnews/asia/china/5071124/Chinas-global-cyber-espionage-network-GhostNet-penetrates-103-countries.html>. [cit.3.4.2011]

.

[165] Tamtéž

jedním z prvních států, který začal používat tuto metodu oficiálně pro vojenské i politické účely.[166] Často se také předpokládá, že čínská kybernetická špionáž má své cíle v USA a že možnosti Číny jsou nyní v tomto směru tak rozsáhlé, že se USA v podstatě nemůže bránit či dokonce ani zjistit existenci útoků. Vyplývá to ze zprávy zpracované US-China Economic and Security Review Commission.[167]

Kybernetická špionáž se tak stala jedním z významných aspektů státní bezpečnosti. Jednotlivé státy budují jak kybernetické rozvědky, tak kontrarozvědky. Pro ukázku, USA se svými spojenci Velkou Británií, Austrálií, Novým Zélandem a Kanadou spolupracují na projektu globálního monitorovacího a sledovacího systému s názvem Echelon.[168] Ten je schopen sledovat telefonické konverzace, emailové zprávy i faxovou komunikaci. V kontinentální Evropě jsou za nejaktivnější v oblasti kybernetické špionáže pokládány země jako Francie, Švédsko či Německo.[169]

Kybernetická špionáž může být v zásadě dvojího typu. Prvním je tzv. obranná kybernetická špionáž zaměřená na sběr a analýzu dat o možných kybernetických útocích. Jejím cílem je také práce na vytváření účinného systému včasného varování před těmito útoky. Druhou podobu kybernetické špionáže představuje ofenzivní kybernetická výzvědná služba. Jejím cílem je zisk informací s ekonomickou, politickou, bezpečnostní či technologickou hodnotou.[170]

Malwarem, který se pro účely kybernetické špionáže nejčastěji používá je spyware nebo trojský kůň. Dokládá to nejenom příklad kybernetické špionáže z Číny, ale především i poslední statistiky za rok 2010, kdy se objevil značný počet alarmujících nových hrozeb, právě díky malware se Spy nebo Trojským koněm Zeus.[171] Malware se objevuje také jako hrozba pro specializovaný průmyslový malware a padělaný software. Patří tak mezi

---

[166] Tamtéž

[167] DANCHEV, Dancho: *Cyber Intelligence – CYBERINT*. In: Dancho Danchev‘ s Blog, Dostupné na WWW: <http://ddanchev.blogspot.com/2006/09/cyber-intelligence-cyberint.html>. [cit.11.4.2011]

[168] Srov. *Echelon.* In: Federation of American Scientists (FAS), [cit.1.7.2011]. Dostupný na WWW: <http://www.fas.org/irp/program/process/echelon.htm>.

[169] JONES, A. – KOVACICH, G. L. – LUZWICK, P. G.: c.d., s. 4.

[170] DANCHEV, Dancho: *Cyber Intelligence – CYBERINT*. In: Dancho Danchev‘ s Blog, [cit.11.4.2011]. Dostupný na WWW: <http://ddanchev.blogspot.com/2006/09/cyber-intelligence-cyberint.html>.

[171] Tamtéž

nejrozšířenější a také jeden z nejdokonalejších typů hrozeb, s kterými jsme se setkali za poslední rok. Krom toho hraje i velkou úlohu v průmyslových špionážích, na osobní úrovni se jedná o phising, kde je právě největším producentem malware v oblasti kyberútoků. Společnosti po celém světě začínají průmyslové špionáži přikládat stále větší význam, nejen při samotné obraně, ale také při získávání nejnovějších informací o konkurenčních společnostech. Tím vzniká prostor k založení nových odvětví podnikání a poskytování unikátních služeb.[172] Čínský metodický postup je hodnocen jako naprosto jedinečný, neboť Čína rozvíjí tzv. *corporate identity,* která se zaměřuje na shromažďování informací o podnicích pro pekingské zpravodajské agentury.[173]

1.8.2 Kybernetický hactivismus

Většina politicky motivovaných kybernetických útoků je vedena za účelem vyjádření deziluze či nesouhlasu se současným národním nebo mezinárodním děním.[174] Pokud považujeme kybernetický hactivismus za novou aktivistickou metodou použitou v prostředí internetu, hovoříme pak o politicky motivovaném hackování neboli hacktivismu. V tomto pojetí je Internet nejen prostorem pro komunikaci, ale také nástroj pro akci, a sice právě politickou. Příkladem jsou webové stránky, virtuální blokády, automatické emailové bomby, hackování webů, vnikání do počítače a počítačové viry a červy.[175] Hactivismus může být rovněž konstruktivní formou politické neposlušnosti. Od kyberterorismu se liší pravděpodobně v tom, že má za primární cíl stanoveno "poškození" daných webových stránek, což sám považuje za formu protestu s pyšným odkazem na svou technickou „zručnost."

---

[172] DENNING, Dorothy. *Georgetown University* [online]. 23. května 2000 [cit. 4.4. 2011]. Cyber Terrorism: Testimony before the Special Oversight Panel on Terrorism. Dostupný na WWW: <http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html>.

[173] Tamtéž

[174] Tamtéž

[175] "It covers operations that use hacking techniques against a targets Internet site with the intent of disrupting normal operations but not causing serious damage. Examples are web sit-ins and virtual blockades, automated email bombs, web hacks, computer break-ins, and computer viruses and worms." DENNING, Dorothy E. *Activism, Hactivism, 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. Santa Monica : RAND, 2001. s. 239-288. ISBN 0-8330-3030-2. s. 241

Hacktivismus je velmi komplikovaný pojem, neboť v širším slova smyslu do něj můžeme zahrnout jakékoliv používání *digitálních nástrojů* a hodí se pro něj kritéria jako „přestupek“ a „nenásilí.“ Je také spojen s různými druhy činností a technickými *defacementy,* v jejichž formě se nejčastěji vyskytuje. Podle mého mínění je hactivismus charakteristický spíše pýchou na některé technické zdatnosti a schopností zrealizovat je účinným a inovativním způsobem. *Hacking* je myšlen jako metoda pro pronikání do jednotlivých počítačů nebo počítačových sítí a poškozování jejich obsahu. Typickým projevem hactivismu je tzv. „*masový defacement,“* který má za úkol nahradit stovky, desítky, či dokonce tisíce webových stránek.

Hactivistické metody jsou využívány také pro propagování některých ideologií. Způsob, kterým se odděluje hactivismus od souvisejících oblastí jsou v zásadě tři, a to taktické, zásadové a kulturní. [176]

Hacktivismus má v současné době nejméně 9 forem:

- Web site defacements
- Web site redirects
- Denial-of-service attacks
- Information theft
- Site parodies
- Virtual sit-ins
- Virtual sabotage
- Software development

Hactivismus použitý v roce 2001 jako nástroj čínských hackerů pro útok na USA patří mezi typický případ DoS útoků. V rámci kybernetické války došlo ke kybertororistickým útoků na stovkách amerických webových stránek.[177] Hacktivismus se liší od kyberterorismu v několika formách, především může být prvkem sólové aktivity a může být proveden jedním aktérem.

---

[176] Pozn. Zajímavým případ úniku informací předcházela v roce 2001 jednání světového ekonomického fóra ve švýcarském Davosu. Hacktivisté napadli počítačový systém a ukradli osobní údaje účastníkům konference, včetně webových stránek, e-mailových adres. Hacktivisté pak veškeré informace umístili na stránky švýcarských novin. McDonald, 2001. Srov. McDonald, Tim. 2001. "Hackers Invade World Economic Forum." *NewsFactor Network*, February 5. [cit. 4.4. 2011].

[177]Srov. Delio, Michelle. 2001. "Is This World Cyber War I?" *Wired News*. s. 2 Srov. "Denial-of-service attack." 2004. July 30 2004 [20.5.2011]. Dostupné na WWW: <http://en.wikipedia.org/wiki/DOS_attack>. <http://en.wikipedia.org/wiki/DOS_attack>.

Od r. 1998 se hacktivismus rozšířil jak geograficky, tak i tematicky. Příklad vedení části konfliktu v kybernetickém prostoru je možné vidět v rámci izraelsko-palestinského konfliktu. Také během války na Balkáně v druhé polovině 90. let bylo možné sledovat aktivitu srbských hacktivistů, kteří provedli tzv. defacement a na asi 50 různých webových stránkách se objevil vzkaz „Kosovo je Srbsko." V nedávné době jsme byli svědky dosud asi nejvážnějšího kybernetického útoku s prvky hacktivismu v srdci evropské integrace i NATO, a to v Estonsku na jaře 2007.[178]

Během bleskové války mezi Ruskem a Gruzií v srpnu 2008 bylo z ruské strany také použito nástrojů vedení kybernetického boje. Hacktivisté, morálně podporovaní ruskými oficiálními kruhy, pronikli na gruzínské vládní stránky i servery některých částí důležité infrastruktury. Bylo použito zejména nástrojů defacementu, kybernetické propagandy a DoS.[179] Bylo zde zároveň možné sledovat nový trend ve vedení války, kdy jsou využívány možnosti kybernetického prostoru k podpoře klasických vojenských operací. Další novou charakteristikou vedení boje tak může být zapojení civilistů, patrioticky laděných občanů vykonávajících tyto kybernetické útoky.[180]

Jedním z velkých příkladů je i příklad útoku „defacement" na webové stránky amerického ministerstva spravedlnosti. V roce 1996 annonymní hacker počmáral toto místo na prostest Zákona o slušné komunikaci (Communications Decency Act). Protest byl proveden sadou nástrojů a urážek typu „Svoboda projevu v zemi svobody?" nebo „Zbraně v domově statečných?"[181] Defacement tedy můžeme považovat za nejčastější metodu hactivismu.

---

[178] Na přelomu dubna a května 2007 byla estonská elektronická komunikační síť narušena koordinovaným kybernetickým útokem. Cílem se staly vládní servery, ale také webové stránky politických stran, finančních institucí a médií. Pro útoky byl použit zejména tzv. distributivní DoS, ale také defacement. Kybernetické útoky byly reakcí na přesun pomníku Rudé armády z centra Tallinnu. Útoky byly vedeny Kremlem podporovanou skupinou Naši.

[179] KREBS, Brian: *Report: Russian Hacker Forums Fueled Georgia Cyber Attacks.* In: The Washington Post, 16. října 2008, http://voices.washingtonpost.com/securityfix/2008/10/report_russian_hacker_forums_f.html (15th September 2009); MESERVE, Jeanne: Study Warns of Cyberwarfare during Military Conflicts. In: www.cnn.com/US, 17. srpna 2009, [cit. 4.4.2011]. Dostupný na WWW: < http://www.cnn.com/2009/US/08/17/cyber.warfare/index.html >.

[180] Podobnou situaci je možné sledovat v rámci palestinsko-izraelského konfliktu. Hacktivisté na obou stranách jsou podporováni k vedení kybernetických útoků (hlavně defacementu či DoS) proti druhé straně.

[181] KREBS, Brian: *Report: Russian Hacker Forums Fueled Georgia Cyber Attacks.* In: The Washington Post, 16. října 2008, http://voices.washingtonpost.com/securityfix/2008/10/report_russian_hacker_forums_f.html (15th September 2009); MESERVE, Jeanne: Study Warns of Cyberwarfare during Military Conflicts. In: www.cnn.com/US, 17. srpna 2009, [cit. 4.4.2011]. Dostupný na WWW:

V tomto kontextu musíme určitě zmínit i druhou nejpoužívanější metodu hactivismu - virtuální sabotáž, která se skládá z on-line aktivit zaměřených na manipulaci nebo poškození cílových informačních technologií. Viry stejně jako jiné formy elektronické sabotáže se liší formou útoků používáných k ničení. Na nejslabší úrovni mohou manipulovat se systémem a šířit vir na další počítače. Na útočnější úrovni mohou dokonce zničit i osobní údaje. Tato metoda útoku byla využita v roce 2001 hacktivisty z InJustice jako červ, který byl replikován tím, že nakazil Microsoft Outloc Express, emailový program, který ho sám odesílal přes kontakty v adresářích.

Tím, že internet umožňuje rychlou a relativně levnou výměnu a sdílení informací, poskytuje extremistickým a teroristickým skupinám zcela výjimečné možnosti prezentovat názory, oslavovat terorismus či oprávněnost násilných činů, včetně podněcování dalších (digitálních) teroristických útoků. Všechny tyto informace jsou předávány snadným a rychlým způsobem, přes využití všech multimediálních možností. Internet se tak stal nejdůležitějším prostředkem, kterým teroristické organizace komunikují se svými příznivci. Propaganda z hlediska kyberterorismu bývá často používána jako nejvhodnější nástroj pro šíření anonymního poselství a psychologického ovlivňování publika. Názory se sdělují nejčastěji formou video-sharingu, blogu, přes bezplatné generátory webových stránek a web hosting.[182] Kybernetická propaganda je hlavním prostředkem pro nábor nových aktivistů nebo k obhajobě trestných činů a podněcování k jejich páchání. Velkou příležitost nabízí zejména pro uplatnění při vzájemné výměny informací, k plánování nebo koordinování akcí, výměně finančních prostředků nebo jako návod na výrobu improvizovaných zbraní.[183]

DDoS útoky (distribuované útoky zaměřené na odepření služeb) směřovaly proti cílům s vysokou politickou nebo ekonomickou hodnotou, proti kritickým komunikacím bankovnictví a finančnickým cílům, komunikační infrastruktuře - včetně chatu, mailserverům

---

< http://www.cnn.com/2009/US/08/17/cyber.warfare/index.html >.

[182] GEERS, Kenneth: *Cyberspace and the changing nature of warfare*. In: SC Magazine, 27. srpna 2008, [cit.1.7.2011]. Dostupný na WWW: <http://www.scmagazineus.com/Cyberspace-and-the-changing-nature-of-warfare/article/115929/ >.

[183] DENNING, Dorothy E. *Activism, Hactivism, 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. Santa Monica : RAND, 2001. s. 239-288. ISBN 0-8330-3030-2. s. 201.

a news službám. Největšího rozšíření dosáhly a největší hrozbou se staly červy - někteří výzkumníci předpovídají novou třídu červů (warhole worms, flash worms), kteří budou velmi rychlí a neponechají administrátorům takřka žádný čas na odpověď. Cílem těchto druhů kybernetických útoků je tzv. narušení služby, při kterém dochází k závažnému narušení nebo poškození fungování informačního systémů. DoS útoky znamenají znepřístupnění určité služby (počítače) nebo sítě a rozumí se jím neoprávněný zásah do počítače, který způsobí jeho vyřazení z činnosti, a to buď zahlcením nesmyslnými požadavky nebo zahlcením spojovací cesty s daty, což znemožní uživatelům počítač využívat. Mezi několik případů Ddos útoků patří tzv. mass-mailing list, který spočívá v zahlcení určité emailové schránky, aby se v požadované době stala nepoužitelnou.

CÍLE - KRITICKÁ INFRASTRUKTURA

Definování kritických infrastruktur a s tím související ochrana těchto systémů začaly být diskutovány teprve poměrně nedávno, a to konkrétně v průběhu 90. let 20. století. Podobná témata se sice objevovala již i dříve. Například v průběhu 80. let se v USA rozpoutala debata okolo stavu tamní infrastruktury zahrnující mosty, kanalizace, silnice, přehrady. Právě hrozby spojené s kritickou infrastrukturou patří mezi nejdiskutovanější témata. Co je myšleno tzv. kritickou infrastrukturou ve spojení s kyberterorismem? Jakým způsobem se můžeme bránit? Termínem, který je „klíčový," se stal termín „kritické infrastruktury".[184]

Za nejpravděpodobnější potencionální cíle kybernetického terorismu bývají nejčastěji uváděny *objekty* kritické infrastruktury. V našem případě se jedná o kritickou informační infrastrukturu. Kritickou infrastrukturou se rozumí výrobní a nevýrobní systémy a služby, jejichž nefunkčnost by měla závažný dopad na bezpečnost státu, ekonomiku, veřejnou správu a zabezpečení základních životních potřeb obyvatelstva.[185]

V Evropské unii je takto definována: energetika, jaderný průmysl, informační a komunikační technologie, zdroje a zpracování vody, potravinářství, zdravotnictví, finanční sektor, doprava, chemický průmysl, vesmírný výzkum, vědecká pracoviště a bezpečnostní služby (The Council of the European Union 2006).[186]

Ve Spojených státech je takto definováno: bankovnictví a finanční sektor, pojišťovací služby, chemický průmysl, zpracovatelé ropy a plynu, energetika, soudní moc, bezpečnostní

---

[184] ŘÍHA, Josef. Kritická infrastruktura a riziko mimořádné události. *Urbanismus a územní rozvoj* [online]. 2007, roč. 10, č. 4, [cit. 6.6.2011]. Dostupný na WWW: <http://www.uur.cz/images/publikace/uur/2007/2007-04/08_kriticka.pdf>.

[185] Definice českého Ministerstva vnitra: Dostupný na WWW: <http://www.mvcr.cz/clanek/kriticka-infrastruktura >. [cit.1.7.2011].

[186] V lednu 2009 vstoupila v platnost Směrnice Rady 2008/114/EC, o určování a označování evropských kritických infrastruktur a posouzení potřeby zvýšit jejich ochranu. Ta představuje první krok redukce zranitelnosti uvedených infrastruktur, se zvláštním zaměřením na oblast dopravy a energetiky.Srov. *Směrnice OECD pro bezpečnost informačních systémů a sítí. Směrem ke kultuře bezpečnosti.* In: Archiv stránek bývalého Ministerstva informatiky, [cit.1.7.2011]. Dostupný na WWW: <http://web.mvcr.cz/archiv2009/micr/images/dokumenty/cz_security_guidelines_4_3__03.pdf>.

služby, univerzity, doprava (uvádí se pouze železniční), informační a komunikační technologie, zdroje a zpracování vody.

Klíčová role infrastruktury v oblasti kyberterorismu je patrná i při využití všech ekonomicko-sociálních systémů jako cílů při způsobení úmyslné škody fyzickým osobám.

Celkově vzato se dá říci, že ochrana kritických infrastruktur je v současné době jedním z prioritních zájmů všech vyspělých států.

S ohledem na uvedenou skutečnost může jít o následující kategorie zranitelnosti:

1. *Software* – může obsahovat škodlivý kód.
2. *Hardware* – zranitelnost může být přítomna jak v rámci systému, v jeho součástech a zařízeních, tak v periferních zařízeních připojených k němu. To může být způsobeno na základě dobrovolné změny komponenty, tak nevhodnou konfigurací systémů, která je velmi „atraktivní“ pro útočníka.
3. *Připojením hardwaru/softwaru* - snadno vložitelný kód při jeho přeprogramování nebo automatické aktualizaci.
4. *Komunikační kanály* – může být mostem mezi vnějším prostředím a systémem nebo sítí, které poskytují užitečný přístupový bod pro útočníka.
5. *Konfigurace* – schopnost poskytnout uživateli možnost nastavit systém je ve skutečnosti dobrou příležitostí, jak vědomě či nevědomě snížit bezpečnost samotného systému, čímž se zvyšuje jeho zranitelnost.
6. *Uživatelé/pozorovatelé* – pokud v této souvislosti nebereme v úvahu škodlivou činnost prováděnou dobrovolně, může i tento způsob umožnit uživatelům se mýlit a ve skutečnosti provádět operace v systému, které usnadní práci útočníkovi.
7. *Poskytovatelé služeb* – instalace softwaru anebo konfigurace některých z profilů systému ze strany poskytovatelů přístupu k internetu může být velmi důležitým prvkem pro zranitelnost útočníka.

Lze shrnout, že funkce kritické infrastruktury zahrnují všechny klíčové objekty a rizika s nimi spojená, přitom se jedná především o vznik nových metod, technik a forem IT, které slouží k napadání a páchání trestné činnosti. Můžeme se domnívat, že v první rovině kritická infrastruktura znamená využití informačního systému jako *cíle* způsobení záměrné škody fyzickým osobám, (může jít o cíle finanční nebo získávání materiálů v elektronické podobě).

Druhým cílem je *narušení* základních elektronicko–komunikačních procesů v informačních systémech například ve smyslu nedostupnosti služeb, modifikování obsahů anebo šíření nedovoleného obsahu.

AKTÉŘI

V předchozích kapitolách jsme si definovali kyberterorismus, jeho nástroje a a jeho možnosti použití z hlediska hactivismu a propagandy na konkrétních případech. Asi nejdůležitější neznámou na této úrovni zůstávají osoby, které provádějí útok. Útočníky, v případě kybernetického boje mohou být jak instituce, tak jednotlivci. Aktéři (političtí, vojenští, ekonomičtí atd.) jsou v tomto kontextu obvykle členěni na:

1) *mezinárodní organizace* (chápané doslovně jako organizace více států)
2) *organizace vyvíjející činnost v rámci národních států*
3) *nadnárodní organizace* (některé obchodní korporace, aktivistické sítě)
4) *státy* [187]

Mezinárodní organizace, v návaznosti na stoupající nebezpečí a frekvenci zneužívání informačních systémů, začaly v tomto směru během posledních let rozšiřovat své se aktivity. Z hlediska výzkumu jsou nejzajímavějšími organizace nadnárodní, neboť nedisponují přímou vazbou na konkrétní teritorium, stát ani legislativu. Pro nás mohou být zajímavé tím, že jsou atraktivním terčem, ale rovněž mohou být i aktéry útoků, protože mají nejsilnější elektronické zázemí a nejlepší přístup k novým komunikačním technologiím. Tyto instituce jsou v mezinárodním boji klíčové a mají strategickou pozici vůči ostatním. Důkazem může být například i fakt, že soukromí počítačoví piráti se nedávno pokusil ochromit Bílý dům, Americké ministerstvo obrany, Newyorksou burzu, Akciový trh Nasdaq anebo Národní bezpečnostní agenturu.[188]

Cílem těchto útoků může být získání důvěrných státních či vojenských informací. Jako příklady si můžeme uvést kybernetický útok proti USA a Jižní Koreji (podrobněji kapitola 10.2 této práce). Podle jihokorejských médií byla z útoku obviněna Severní Korea, která má speciální jednotky pro kybernetickou válku. Podobný útok probíhal i v roce 2008 mezi Gruzií a Ruskem, kde stránky gruzínské vlády a tamních firem začaly čelit zvýšenému počtu útoků typů DDoS. Za tamními útoky proti Gruzínské infrastruktuře tehdy podle nezávislých

---

[187] BARBER, Richard: *Hacking Techniques. The tools that hackers use, and how they are evolving to become more sophisticated.* Computer. Fraud and Security. 1. března 2003, č. 3, p. 9-10. Srov. také VATIS, M. A. *Cyber Attacks During the War on Terrorism: A Predictive Analysis* [online]. 2001 [cit. 5.5. 2011]. Dostupný na WWW:<http://www.ists.dartmouth.edu/ISTS/counterterrorism/cyber_a1.pdf>.

[188] Útok se odehrál v Den Americké nezávislosti USA a na jihokorejské servery.

západních expertů byla obviněna Moskva, jelikož tak údajně činila, aby získala tajné informace a uvedla je mimo provoz.[189] Jiné zdroje uváděly, že se na tomto útoku podílely místní tajné služby. Tyto případy kybernetických válek vedených proti kritické infrastruktuře států mohou být příkladem splňujícím podmínky výše uvedené typologie, která za aktéry útoků pokládá organizace vyvíjející činnost v rámci národních států nebo státy samotné.[190] Mezinárodní či národní aktéry považujeme za nejdůležitější autory významných mezinárodních konfliktů. Naopak aktéři na individuální úrovni – jednotlivci a jejich uplatnění v kyberterorismu je poněkud diskutabilní, neboť považovat politicky motivovaného jedince, který se sám podílí na organizaci promyšleného politicky motivovaného útoku, je sporné. Podle nás úloha jednotlivce nachází širší uplatnění např. v *cyberstalkingu* nebo v *hackingu*.[191]

Dokladem toho může být i charakter zmiňovaných útoků, když nebyl obviněn jako aktér těchto událostí žádný jedinec. Význam jednotlivce a jeho uplatnění v případě mezinárodního kybernetického terorismu je tedy spatřován především v možnosti najmout si dostatečně schopné individuum pro tyto účely.[192]

V takovém případě může být uplatněna jiná typologie uvažující z hlediska tzv. *státních aktérů* tři formy participace. Ve většině případů představuje iniciátora útoku *vládní agentura* či skupina úzce napojená na vládní úřad, a pokud její útok splňuje znaky promyšlenosti a politické motivace, je cílen proti informačním a počítačovým systémům a jeho výsledkem je násilí proti *civilním osobám*, pak hovoříme o kybernetickém terorismu, z čehož vyplývá, že se jedná o aktivity *vnitrostátní.* Druhou formou role státu je *státní účast*, která znamená na rozdíl od státního terorismu to, že vybrané cíle jsou vyhodnocovány jako nebezpečné pro stát.[193]

---

[189] RIA Novosti (22.8.2008): *Russia says military pullout from Georgia complete*, [cit. 5.5. 2011]. Dostupné na WWW: <http://en.rian.ru/russia/20080822/116226749.html>.

[190] Government of Georgia (8.8. 2008): *Statement of Government of Georgia regarding the situation in the South Ossetia region of Georgia,* [cit. 5.5. 2011]. Dostupné na WWW*:* <http://www.government.gov.ge/index.php?lang_id=ENG&sec_id=103&info_id=1982>.

[191] *Contemporary Security Threats within Cyberspace. NATO and EU Approaches to Cybersecurity*. Maria Enzersdorf, AIES 2009. s. 16.

[192] Příkladem může být Koncepce nájemných hackerů (Hackers for Hire či H4H). ROLLINS, John; WILSON, Clay. Terrorist Capabilities for Cyberattack: Overview and Policy Issues. *CRS Report for Congress* [online]. [cit. 5.5. 2011]. Dostupný z WWW: <http://www.fas.org/sgp/crs/terror/RL33123.pdf>.

[193] International Terrorism and Security Research 2004. *International Terrorism and Security Research* [online]. 2004 [cit. 5.5. 2011]. State Sponsored Terrorism. Dostupný na WWW: <http://www.terrorism-research.com/state/>.

V současné době existují podezření na existenci speciálních skupin odborníků na ICT, jejichž úkolem je plnit úlohy zadané vládními institucemi. Jedná se tak předně o aktéry pracující na národní objednávku, většinou tedy o útoky s politickou motivací mířící proti kritické infrastruktuře států, například proti státním *velvyslanectvím*. Jedním z takovýchto případů může být i. Čínská lidová republika, jejíž hackeři, ať už pracují pro cizí vlády nebo pro sebe, nebyli schopni narušit nebo eliminovat americkou informační infrastrukturu jako celek. Americké ministerstvo obrany dokonce tvrdí, že hackování je součástí čínských vojenských plánů.

Třetí skupinou je *státní sponzoring*, který je založen na teroristických aktivitách, kterým se dostává státní podpory především v podobě jejich financování. V dubnu 2009 zveřejnilo americké Ministerstvo vnitra seznam zemí, [194] které sponzorují terorismus. Seznam obsahuje čtyři země: Írán, Kuba, Súdán a Sýrie (Office of the Coordinator for Counterterrorism 2009),[195] nicméně příkladem státního sponzoringu může být i Čína. Experti upozorňují, že nejlidnatější země světa je plná neregistrovaných a nehlídaných sítí a počítačů. Jejich uživatelé tak můžou pocházet z jakékoliv části světa, nejen z Číny.

Kybernetické útoky se tedy odvíjí od typologie jejich operačních schopností a znalostí oběti nebo cíle. Pro úspěšnou akci musí útočník vědět, jak využít technologické zranitelnosti systému nebo slabých vlastností oběti při své činnosti.

1. Technicky školení – vyvíjejí vlastní know-how, čímž se vyhýbají externím hackerům.
2. Vytrvalí – strategii berou jako hodnotu skutečného poslání.
3. Motivovaní – cítí se být součástí projektu, který má pro ně také citovou hodnotu.
4. Organizovaní – vyvíjejí potřebný software a hardware.
5. Propojení – jednotliví aktéři se nacházejí často na prostorově distribuovaných místech.[196]

---

[194] *International Terrorism and Security Research* [online]. 2004 [cit. 5.5. 2011]. State Sponsored Terrorism. Dostupný na WWW: <http://www.terrorism-research.com/state/>.

[195] Antinori Arije, *Information & Communication Technology (I.C.T.), tra mutamento sociale e sicurezza. Uno sguardo al futuro* in *Quaderno dei lavori 2008,* C.I.R.S.D.I.G, Centro Interuniversitario per le Ricerche sulla Sociologia del diritto, dell'Informazione e delle Istituzioni Giuridiche, Messina, 2009.

[196] Tamtéž, s. 8

Zejména několik posledních studií potvrzuje, že *hacking* vzrůstá za účelem zasáhnout stále větší počet uživatelů. Hackři jsou motivováni ziskem a vědí, že přitahuje stále větší počet.

9. ANALYTICKÁ ČÁST - Mezinárodní kyberterorismus a formy kybernetické války v letech (2007-2010)

Oblast Evropsko-ruská

9.1 Nejzávažnější případy: Útok na Gruzii a Estonsko

Uplatnění nástrojů kyberterorismu bylo použito v srpnu roku 2008, kdy Rusko zahájilo útoky na Gruzii ve válce o Jižní Osetii. Ruské jednotky vtrhly na území Jižní Osetie na základě údajné agrese ze strany Gruzie.[197] Kybernetický útok vedený proti Gruzii je důležitým mezníkem v historii kybernetické války.[198] Tento kybernetický útok je dokladem toho, jakým způsobem může být využito nástrojů kyberterorismu ve válce, neboť simultánně s civilním vojenským konfliktem probíhaly i útoky v kybernetickém prostoru. Kybernetický útok vedený proti Gruzii je odborníky považován za nový model vedení války, který lze očekávat v budoucích válečných konfliktech.[199] Spolu s kybernetickým útokem na Estonsko v roce 2007 a na Litvu v roce 2008 a na počátku roku 2009 vzrostl význam kybernetických útoků na mezinárodní úrovni.

9.1.1 Cíle

Hlavním cílem útoků byly *gruzínské webové servery.* Tyto útoky probíhaly od 19. do 20. července 2008. Na základě zprávy bezpečnostních expertů z USA, byly potvrzeny rozsáhlé útoky na oficiální webové stránky Gruzie. Podle mluvčího gruzínského velvyslanectví útoky nabraly zvyšující se intenzity v okamžiku napadení Jižní Osetie. Cílem útoků byly webové stránky gruzínského prezidenta Michaila Saakashviliho,[200] webové

---

[197] Ministry of Foreign Affairs of Georgia (8.8. 2008): *Statement of the Ministry of Foreign Affairs of Georgia,* [cit. 5.5. 2011]. Dostupný na WWW: <http://www.mfa.gov.ge/index.php?lang_id=ENG&sec_id=59&info_id=7201>.

[198] Rusko bylo na válku plně připraveno, ale vyvolalo ji gruzínské vedení, které zahájilo vojenské operace jako první.

[199] Reuters (10.8. 2008): *Georgia offers ceasefire as fighting continues,* [cit. 5.5. 2011]. Dostupný na WWW: <http://www.reuters.com/article/gc07/idUSL768040420080810) >.

[200] President of Georgia (9.8. 2008): *Presidential Decree on Declaration of State of War and Full Scale Mobilization*[cit. 5.5. 2011]. Dostupný na WWW: <http://www.president.gov.ge/?l=E&m=0&sm=1&st=70&id=2697>.

stránky ministerstev, zpravodajských agentur, bank a dalších institucí.[201] Téměř všechny z nejdůležitějších vládních internetových stránek byly úspěšně napadeny, včetně internetových stránek předsednictva, ministerstev, soudů a parlamentu. Potom, co ruské jednotky měly vybudovanou pozici v Gruzii, seznam útočných míst byl rozšířen na další internetové stránky, gruzínské finanční instituce, obchodní sdružení, vzdělávací instituce, sdělovací prostředky a gruzínské hackerské fórum, stejně jako i vzdělávací instituce, které pracují v rámci vědy, techniky a medicíny. Obsah webových stránek prezidenta Saakashviliho[202] byl upraven tak, aby připodobňoval prezidenta k nacistickému vůdci Adolfu Hitlerovi. Z těchto důvodů byl obsah přemístěn z gruzínských serverů na americké hostingové servery. Kromě prezidentských stránek byly na servery mimo území Gruzie přesunuty i další weby významných institucí. Zajímavostí je, že některé webové stránky byly přesunuty na hostingové servery v Estonsku, které měly již s podobnými útoky zkušenosti z roku 2007.[203]

9.1.2 Motivace

Kybernetické útoky mely především výrazně narušit schopnost gruzínské vlády vypořádat se s ruským invazivním zásahem do komunikace mezi vládou a veřejností. Byly porušeny všechny transakční operace v zemi, zastaveny plateb a finanční transakce. Útokům z ruské strany předcházela distribuce veřejného seznamu vládních webových stránek na ruských fórech. Tyto útoky byly jasně určeny k tomu výrazně pozastavit uvedení webových stránek do provozu a cílem těchto útoků bylo rovněž zpozdit jakoukoliv mezinárodní odezvu. Útoky byly navrženy tak, aby bylo obtížné zorganizovat účinnou reakci na ruskou přítomnost a byly především určeny k tomu, aby přerušily normální obchodní operace. Krom toho velké banky byly právě těmi organizacemi, které mohly být použity pro komunikaci a koordinaci reakcí mezi různými institucemi. V krizové situaci se stal velmi důležitým také soukromý sektor. Hlavní cíl války představovala jednoznačně podpora ruské invaze do Gruzie a

---

[201] President of Georgia (8.8. 2008): *Declaration of Universal Mobilization by Georgian President Mikheil Saakashvili* [cit. 5.5. 2011]. Dostupný na WWW: <http://www.president.gov.ge/?l=E&m=0&sm=3&st=20&id=2689>.

[202] Reuters (10.8. 2008): *Georgia offers ceasefire as fighting continues*, [cit. 5.5. 2011]. Dostupný na WWW: <http://www.reuters.com/article/gc07/idUSL768040420080810) >

[203] Tamtéž

kybernetické útoky tak byly zařazeny do plánu invaze. [204] Kybernetické útoky odstartovaly ve velké míře během několika hodin, kdy začaly ruské vojenské operace a skončily těsně poté, co byly ruské vojenské operace zastaveny. Útoky měly přinést výhody ruské armádě a zesílit dopad fyzických útoků na gruzínské komunikační sítě.

9.1.3 Nástroje

Provedení většiny útoků bylo metodou DDoS, jejíž princip funguje tak, že útočník, který chce systém napadnout, ovládá tzv. CC server (command and control). K tomuto serveru jsou pomocí botnetu připojeni klienti, kteří vykonávají příkazy CC serveru. Těmito klienty mohou být nedostatečně zabezpečené stanice umístěné po celém světě. Útočník vydá příkaz, aby se ovládané počítače začaly automaticky dotazovat webových stránek na nelogické dotazy. Tyto útoky jsou síťové, což znamená, že útočník používá k zasažení cíle množství počítačů. Pro DDoS útoky se používá určitý počet přístrojů s koordinovaným chováním. Následkem toho webový server nestíhá odbavit všechny dotazy, neboť jich v krátkém období přichází veliké množství.[205] DDos útoky blokují služby sítě záplavovým spojením, dochází tak ke zhroucení serverů a vyčerpání zdrojů, tento typ útoku vyžaduje dostatečné množství klientů botnetu, kteří útočí na napadený systém. Tento typ botnetů byl již znám a v minulosti často používán pro trestnou činnost.

V případě Gruzie byly typy toků DDos použity velmi sofistikovaně. Nástroje použité pro útok DDs byly zahrnuty ve třech různých softwarových aplikacích, určených pro tzv. „zátěžové testy," ve kterých jsou servery zaplaveny packety http. Čtvrtký kus softwaru byl původně navržen pro přidání funkce k webových stránkám, aby byly žádosti vyslané od útočníků poslané na náhodnou nebo neexistující webovou stránku.[206]

---

[204] Ministry of Foreign Affairs of Georgia (8.8. 2008): *Statement of the Ministry of Foreign Affairs of Georgia,* [cit. 5.5. 2011]. Dostupný na WWW: <http://www.mfa.gov.ge/index.php?lang_id=ENG&sec_id=59&info_id=7201>.

[205] President of Georgia (9.8. 2008): *Presidential Decree on Declaration of State of War and Full Scale Mobilization*[cit. 5.5. 2011]. Dostupný na WWW <http://www.president.gov.ge/?l=E&m=0&sm=1&st=70&id=2697>.

[206] Tento typ http útoků byl testován v USA CCU a byla prokázána mnohem větší účinnost než při ICMP útoků, které byly použity v Estonsku. Použít nástroj, který požaduje přístup na neexistenci webové stránky, byla obzvlášť účinná zbraň, protože takto napadeným serverům se brzyvyčerpala výpočetní kapacita, protože hledaly stránky, které neexistovaly. Tento nástroj byl zároveň schopen zacílit sedmnáct různých stránek gruzínských stránek použitím SQL injekce, diskutovaných v on-line útočnických fórech a považovaných za velmi

Hlavní metoda používaná pro udržení a rozšíření kybernetické války byla série komentářů na webových stránkách. Tyto komentáře obsahovaly jak útočnické nástroje, tak seznamy doporučených cílů k útoku. Zajímavé také je, že tyto web posty byly velmi jednoduché na ovládání i pro uživatele bez znalosti větších počítačových dovedností. Hlavní metodou se stalo tzv. *postování,* kdy se používaly různé webové stránky, kromě těch, které byly vytvořeny speciálně pro kybernetický útok ve válce proti Gruzii. Některé adresy webových stránek, které byly použity k uspořádání útoků byly umístěny ve Spojených státech. K dalšímu zajímavému zjištění dochází US-CCU[207], neboť objevilo, že stránky používané v gruzínské kampani byly připraveny pro použití proti Gruzii více než dva roky před útoky. Technická analýza US-CCU ukázala, že grafika používaná na stránce vznikla 10. března 2006, kdy byly vztahy mezi Gruzií a Ruskem v krizi. Stránka s touto grafikou mohla být použita kdykoliv, nicméně byla uschována a použita až ve válce proti Gruzii v srpnu 2008. Tato skutečnost může být dokladem toho, že kybernetické útoky proti Gruzii byly součástí ruského plánu již nějakou dobu.

Důležitým bodem je ale to, že útočníci upustili od provedení toho druhu napadení, který by trvale fyzicky poškodil kritickou infrastrukturu gruzínských webových stránek. Útokům z ruské strany předcházela distribuce veřejného seznamu gruzínských vládních webových stránek na ruských fórech. Tímto způsobem byla zajištěna informovanost zejména rusky hovořích uživatelů internetu, jimiž budou webové stránky atakovány. Jednou ze skupin, které se podílejí na kyberútocích je stránka StopGruzii, kde byl umístěn seznam webových adres neboli cílů útoků. Takto unikátně koordinovaný útok, zaplavil weby gruzínské vlády a portály gruzínských médií žádostmi o přístup, takže způsobil přetížení a dočasný výpadek.[208] V další fázi došlo k distribuci velmi jednoduchého nástroje na http zahlcení zvolené webové adresy. Ve dnech 9. až 10. srpna byla většina gruzínských webových stránek nedostupná.

---

sofistikovanou techniku. Srov. International Crisis Group Europe Report N°183, *Georgia's South Ossetia Conflict: Make Haste Slowly.*Tbilisi/Brussels 2007.

[207] Ministry of Foreign Affairs of the Russian Federation (9.8. 2008): *Inteview by Minister of Foreign Affaires of the Russian Federation Sergey Lavrov to BBC, Moscow, August 9, 2008,* [cit. 5.5. 2011]. Dostupný na WWW: <http://www.mid.ru/brp_4.nsf/e78a48070f128a7b43256999005bcbb3/f87a3fb7a7f669ebc32574a100262597?OpenDocument>.

[208] President of Russia (8.8. 2008): *Beginning of the Meeting on the Conflict in South Ossetia with Defence Minister Anatoly Serdyukov and the Chief of General Staff of the Russian Armed Forces Nikolai Makarov,* [cit. 5.5. 2011]. Dostupný na WWW: <http://www.kremlin.ru/eng/text/speeches/2008/08/09/1139_type82913_205050.shtml>.

Gruzie musela požádat o podporu organizace z jiných zemí, aby o vojenském zásahu mohla informovat okolní svět pomocí internetu. Většina webových stránek velkých firem a státních orgánů byla přesunuta na hosting do jiných zemí. [209] V krátké době nebyly stránky dostupné ani z Gruzie ani ze zahraničí. Rusko v krátké době získalo důležitou "kybernetickou převahu" tím, že zabránilo Gruzii poskytovat přesné informace o stavu bitvy.

9.1.4 Důsledky

Podle nedávné zprávy nezávislého amerického institutu U.S. Cyber Consequences Unit,[210] který začal monitorovat situaci krátce po začátku útoku, dospěla americká CCU k závěru, že všichni hackeři a jejich aktivity měly souvislost s civilní sférou. To znamená, že kybernetické útoky na Gruzii byly prováděny civilisty s malým nebo žádným přímým napojením na ruskou vládu či armádu. Mimo samotného Ruska byl největší počet účastníků z Ukrajiny a Lotyšska. I kdyby v zásadě bylo možné, že by útoky provedli hackaři najatí ruskou armádou, bylo by velmi obtížné a nákladné maskovat jejich zapojení přesvědčivě. Jsou k dispozici velmi podrobné informace o technice útoku, jeho chronologii, snímky z obrazovek z počmáraných webových stránek, fór používaných k organizování a spouštění útoků a doménové adresy útočníků a informací ukazujících na pravděpodobnou totožnost mnoha útočníků. Existuje doměnka, že organizátoři kybernetických útoků měli informace o ruských vojenských záměrech, neboť byli upozorňováni včas o načasování ruských vojenských operací a ve stejném čase byly tyto kybernetické operace prováděny. Mnoho kybernetických útoků totiž korespondovalo s časem, ve kterém byly provedeny vojenské útoky, což znamená, že musela být velmi úzká spolupráce mezi lidmi v ruské armádě a civilními kyberútočníky. Dalším důkazem bylo to, že velkou roli sehrály v útoku sociální sítě působící na internetu, neboť byly hlavním nástrojem pro osoby, kdo prováděly útoky. Ze způsobu provední útoků a jejich důsledků[211] je jasné, že útočníci spolu nekomunikovali jenom přes internetovou poštu,

---

[209] International Crisis Group Europe Report N°151, *Georgia: What now?*, Tbilisi/Brussels 2003.
International Crisis Group Europe Report N°195, *Russia vs Georgia: The Fallout.*
Cornell, S.E.: *Pipeline Power, The War in Georgia and the future of the Caspian Energy Corridor.* Georgetown Journal of International Affairs, Iss 10.1, Winter/Spring 2009, s. 131 - 139.

[210] Tamtéž, s. 131-139.

[211] Např. International Crisis Group Europe Report N°183, *Georgia's South Ossetia Conflict: Make Haste Slowly.*Tbilisi/Brussels 2007.

nýbrž využili také novou formu komunikace pomocí sociálních síťí.[212] Dalším ze závěrů je ten, že kyberútočníci byli podporováni ve svých aktivitách ruským organizovaným zločinem. Vedou k tomu důkazy prokazující, že některé webové servery a adresy sloužící k řízení a koordinaci útoků byly již dříve využívané ruskými zločineckými organizacemi.[213] Některé servery, které byly použity při útocích, byly současně připraveny jako hostingový software pro počítačovou kriminalitu. Je zde patrné, že ruské zločinecké organizace se nesnažily skrývat své zapojení do útoku na Gruzii.

Celkový počet jednotlivých útočníků, který byl zapojen ve válce proti Gruzii, byl mnohem větší než při kybernetických útocích proti Estonsku, i když množství zapojených počítačů byl mnohem menší. Počet útočníků byl pravděpodobně mnohem vyšší než bylo vidět v online fórech. Celkový objem protiútoků potřebných k zastavení útoků na gruzínský cíl byl však podstatně nižší než množství potřebné k vyřazení estonského cíle.

9.2 Estonsko-ruský incident

V roce 2007 se zaměřilo zahraniční zpravodajství na další zemi bývalého Sovětského svazu, na Estonsko. Estonské stránky byly nepřístupné ze zahraničí, čímž se země stala izolovanou. Příčina kybernetického útoku na malou pobaltskou zemi spočívala v přesunutí sochy „rudoarmějce“ v Tallinnu, známé spíše svým neoficiálním názvem „Bronzový voják,“[214] estonskými úřady z centra Tallinu na vojenský hřbitov. Přesunutí sovětského pomníku, oslavujícího neznámého Rusa, který padl v boji proti nacistům, podnítilo nepokoje etnických Rusů žijících v Estonsku a blokádu estonské ambasády v Moskvě. Událost také odstartovala období masivních kybernetických útoků na estonské státní webové stránky, zejména na stránky ministerstev a premiérovy Reformní strany. Odstraňování pomníku byla

[212] Jedná se relativně o nový směr ve způsobu komunikace, jehož nedávné rozšíření umožnil web 2.0., který měl dopad v tom, že se zvýšil počet uživatelů počítačů v Rusku a zlepšil se přístup k fórům, ze kterých se rekrutovali kyberútočníci. Tímto f˘orem nebylo podle očekávání hackerské fórum, ale fórum sociálních síťí věnované datování, politice a jiným sdíleným zájmům.[212] Jedno z hlavních fór, které organizovalo útočníky bylo v ruštině. První fórum, které bylo anglicky, mělo hostitele ze San Francisca.

[213] International Crisis Group Europe Report N°189, *Georgia: Sliding towards Authoritarianism?* International Crisis Group Europe Report N°193, *Georgia and Russia: Clashing over Abchazia.*

[214] Conflict Studies Association, *Proceedings of the Annual Symposium "Implication for an Estonia-Like Cyber Conflict for the Government and the Private Sector"* Georgetown University, Washington, USA, 2008.

údajně záminka, neboť Kremlu pravděpodobně vadila snaha Estonska orientovat se na západ, úzké vazby na Brusel a jeho členství v NATO a EU. [215]

9.2.1 Cíle

Útok začal 27. dubna na estonskou kritickou infrastrukturu, kdy byly stránky estonských organizací, ale i parlamentu, bank, ministerstev, televizních stanic a novin zaplaveny útoky typu DoS.[216] Estonsko jako člen Severoatlantského paktu neváhalo problém ještě více vystupňovat a požádalo v rámci aliančních vazeb NATO o pomoc, přestože kybernetický útok není považován za válečné ohrožení země ve smyslu článku 5 Severoatlantické smlouvy.[217] Severoatlantická aliance zareagovala a vyslala do Tallinu tým expertů na „kybernetický terorismus," aby vyšetřil tři týdny trvající kybernetické útoky, které započaly bezprostředně po bouřlivých pouličních nepokojích v Tallinu.[218] Vládní úřad v Talinu ale obvinil Kreml, protože většina útoků odešla z IP adres zaregistrovaných v Rusku, některé adresy dokonce ukazovaly souvislost s bezpečnostními službami v Moskvě.[219] Klíčem k pochopení tohoto konfliktu je nutnost uvědomění si, že v estonská populaci, která čítá 1,3 milionu obyvatel, je zastoupeno ruské etnikum 25,6 %. Historické vazby mezi Estonci a Rusy nejsou harmonické především díky událostem z dob Sovětského svazu (deportace, přesidlování). Přesunutí pomníku tak probudilo nacionalistické tendence a tato nevole vyústila v podobě kybernetických útoků, které byly započaty ve „sváteční den," kdy se připomínalo vítězství sovětských vojsk nad nacistickým Německem.

---

[215] Cyber Conflict Studies Association, *Proceedings of the Annual Symposium "Implication for an Estonia-Like Cyber Conflict for the Government and the Private Sector"* Georgetown University, Washington, USA, 2008. s. 17.

[216] Tamtéž, s. 19.

[217] Severoatlantická smlouva. North Atlantic Treaty Organization. Washington D.C. Dokument schválen 12.9.2001, po útoku na Twin Towers. Tato smlouva stanovuje, že každý útok na jednoho členského státu, je považován za útok na celou alianci. [cit. 5.5. 2011]. Dostupný na WWW: < http://nato.int/docu/pr/2001/p01-124e.htm. >.

[218]Tamtéž, s. 15.

[219] Cyber Conflict Studies Association, *Proceedings of the Annual Symposium "Implication for an Estonia-Like Cyber Conflict for the Government and the Private Sector"* Georgetown University, Washington, USA, 2008. s. 13.

9.2.2 Motivace

Estonská vláda z odpovědnosti oficiálně obvinila Rusko. Zpočátku také existovala jistá podezření o zapojení vládních agentur do tohoto útoku. Většina serverů estonských státních institucí byla dočasně nedostupná a nebyl na ně přístup odjinud než ze strany estonských poskytovatelů. Podle estonských IT specialistů nebylo možné provést tak rozsáhlý útok několika izolovanými hackery bez spolupráce státních institucí.[220] Původní domněnky se však nepotvrdily a za hlavní aktéry tohoto incidentu byli označeni ruští hackeři, kteří pomocí botnetu odstavili vládní webové stránky a weby dalších firem a institucí.

9.2.3 Nástroje

Argumentace o nepravděpodobnosti přímého zapojení vládních agentur vycházela z analýzy útoků, které proběhly z několika míst (místa útoků byla zaznamenána v USA, Brazílii, Kanadě a Vietnamu), a předpokladu, že v případě vedení útoků ze strany vládních agentur by nebylo možné takto masivní distribuované DoS útoky provádět. Nutno podotknout, že nebyly zveřejněny žádné důkazy či podpůrné argumenty, které by vysvětlovaly, proč by nemohly být vedeny útoky i z těchto míst.[221] Podle estonských IT specialistů je totiž nemožné, aby byl takový rozsáhlý útok proveden několika izolovanými hackery bez spolupráce státních institucí. Ta probíhala velmi koordinovaně a sofistikovaně, když byly servery estonských státních institucí bombardovány velkými objemy dat převážně z ruských IP adres. Baltická supervelmoc vyvíjela dokonce silný diplomatický, ekonomický a psychologický tlak, aby ovlivnila politiku vůči ruskému obyvatelstvu Estonska.

9.2.4 Důsledky

Krátce po útocích na Estonsko, bylo v bývalé ex-sovětské zemi založeno CCDCOE (Cooperative Cyber Defence Centre of Excellence). Toto Centrum pro výzkum

---

[220] ASHMORE, William Impact of Alleged Russian Cyber Attacks By. In *Baltic Security & Defence Review*. Baltic Defence College 2009 [cit. 4. 5. 2011]. Dostupný z WWW: <http://www.bdcol.ee/files/files/documents/Research/BSDR2009/1_%20Ashmore%20-%20Impact%20of%20Alleged%20Russian%20Cyber%20Attacks%20.pdf>.

[221] Výsledky vyšetřování přinesly závěry o zapojení generace mladých hackerů, nicméně existují zprávy o možné (byť nevelké) participaci politických elit v tomto konfliktu. Jeden z předních představitelů hackerské skupiny s názvem Nashi pracoval jako asistent poslance, který reprezentoval ve Státní Dumě prokremelsky orientované křídlo. Lze se tak domnívat, že tyto kybernetické útoky byly výsledkem patriotistických tendencí na obou stranách s potencionálním zapojením prorusky (nacionálně) orientovaných politických elit.

kybernetických hrozeb a počítačovou obranu, založené v květnu roku 2008 v estonském hlavním městě Talinu, je mezinárodní organizací zaměřenou na boj s kybernetickými hrozbami a pověřena koordinací počítačové obrany v rámci zemí NATO. Hlavním jejím cílem je zlepšit spolupráci a poskytnout ochranu zemím v rámci vztahů Severoatlantické aliance. Toto specializované centrum má také posílit pozici aliance v boji proti útokům kyberteroristů a zároveň ustanovit právní aspekty počítačové obrany.[222]

Na vzniku centra se podílely finančními prostředky: Estonsko, Lotyšsko, Litva, Německo, Itálie, Slovensko a Španělsko. CCDCOE navazuje vztahy i s nečlenskými státy NATO, vysokými školami, výzkumnými institucemi a dalšími, kteří se chtějí podílet na posílení spolupráce a sdílení informací.[223] Již v roce 2003, před vstupem bývalé sovětské republiky do NATO, navrhovalo Estonsko vytvoření kybercentra. Při summitu NATO v Rize v listopadu 2006 Estonsko upozornilo na útoky proti bezpečnosti dat v informačních systémech. Také v tomto okamžiku byla uznána společná potřeba programů na ochranu počítačových systémů v dlouhodobém horizontu.[224] Cílem CCDCOE je zlepšit a zefektivnit spolupráci a výměnu informací mezi státy NATO prostřednictvím vzdělání, výzkumu, vývoje, sdílení zkušeností v oblasti kybernetických útoků.

Pokud na závěr shrneme rozdíly mezi gruzínsko-ruským kybernetickým incidentem a konfliktem estonsko-ruským, pak můžeme na základě výše uvedených analýz tvrdit, že v Estonsku byly spáchány především škody v přístupu k činnosti v oblasti sociálního a ekonomického systému, a to mezi soukromým a veřejným sektorem, např. e-government, e-banking atd. Naopak v Gruzii bylo jádrem škod[225] „omezení“ a zničení informací a názorů na

---

[222]EurActiv. *EurActiv* [online]. 9. dubna 2009. Estonsko v přední linii boje proti kyberterorismu. [cit. 21. 5. 2011] Dostupný na WWW: <http://www.euractiv.cz/bezpecnost-a-spravedlnost0/clanek/estonsko-v-predni-linii-boje-proti-kyberterorismu-005855>.launches cyber defence centre in Estonia 999.html>

[223] NATO Cooperative Cyber Defence Centre of Excellence Tallinn, Estonia. [cit. 5.5. 2011]. Dostupný na WWW: < http:// www.spacewar.com/reports/NATO_launches_cyber_defence_centre_in_Estonia_999.html>.

[224] EurActiv. *EurActiv* [online]. 9. dubna 2009 [cit. 21. 5. 2011]. Estonsko v přední linii boje proti kyberterorismu. Dostupný na WWW: <http://www.euractiv.cz/bezpecnost-a-spravedlnost0/clanek/estonsko-v-predni-linii-boje-proti-kyberterorismu-005855>.

[225] GARDNER, Greg. Combating Cyber Warfare Against Information and Networks. In *Defense Science Board 2007 Summer Study: Challenges to Military Operations in Support of U.S. Interests*. Albany : Government and Homeland Security Solutions, 2007 [cit. 4. 5. 2011]. Dostupný na WWW: <https://www.cscic.state.ny.us/security/conferences/security/2008/info/Day%201/B1-Gardner%20Combating%20CyberWarfare.ppt>.

gruzínskou vládu libovolných ruských hackerů, takže byl možný dopad v krizi na sociální a kognitivní zkreslení. Primární závislost obou zemí na ICT službách představovala velmi negativní faktor dopadu. Přesný dopad estonsko-gruzínské krize bude muset být posouzen až v dlouhodobém horizontu, kdy někteří ukazatelé boudou mít jasnou vypovídací hodnotu, ale není známo, zda je státní orgány a soukromé organizace budou ochotny zveřejnit. Nicméně diskuze o negativních dopadech kybernetických útoků bude kompletní až s mnoha hodnoceními a reakcemi na tyto jevy v mezinárodním kontextu. Náležitá pozornost a spolupráce mezi mezinárodním společenstvím a Gruzií byla velkým přínosem pro řešení střetu dvou států se zapojením mezinárodního společenství do řešení problému.

Z hlediska aplikace konceptu "Information Assurance" u těchto typů útoku byla jednoznačně narušena oblast integrity dat. Konkrétně došlo ke kopírování a modifikacím informací například při poškození oficiálních gruzínských webových stránek) nebo při modifikacích webových stránek prezidenta Saakashviliho. Jednalo se o aktivní útok na dostupnost a integritu dat (avaibility), který je charakteristický ztrátou, modifikací dat. Integrita dat byla narušena neutorizovaným subjektem zvenčí. Útok byl proveden aktivní formou, jež souvisí se změnou a přidáním hodnoty (defacement). Což dosvědčuje i to, že bylo zabráněno data aktivně využívat ve smyslu nedostupnosti bankovních služeb, internetových stránek atd. Absolutní prevence útoků ovšem zajistitelná není, proto typická ochrana (hlavně před aktivními formami útoků) je založena na detekci útoků a na následné obnově činnosti.

10. Oblast asijsko-americká

10.1 Čína a Google: Operace Aurora

Operace Aurora[226] je označením kybernetického útoku, který začal v polovině roku 2009 a pokračoval až do prosince téhož roku.[227] Útoky, známé jako „rozšířené přetrvávající hrozby," byly cílené na firemní infrastrukturu a krádež duševního vlastnictví společnosti Google. Primárním cílem útočníků byl přístup na Gmail účty čínských aktivistů za lidská práva. Útok byl společností Google v rámci výzkumu uznán nejen jako útok na Google, ale také jako napadení několika dalších amerických organizací a firem. Útok Aurora je považován jako mnohem závažnější než útoky na dalších třicet jiných společností. Zprávu o prvním útoku zveřejnil Google 12. ledna 2010 prostřednictvím svého blogu.[228] Aurora představovala sofistikovanou špionážní operaci, nastavenou tak, aby ukradla informace týkající se duševního vlastnictví velkých korporací. Jednalo se o velkou průmyslovou špionáž více než 30 společností, u kterých byl použit pro získání informací stejnojmenný malware „Aurora." Pravděpodobně se jednalo o útok na několik cílových jedinců, kteří mají přístup ke klíčovým informacím a duševnímu vlastnictví a především k uživatelským účtům.[229] V tomto případě bylo tedy důležité monitorovat schránky elektronické pošty a servery. Mezi tyto velké korporace patřily především společnosti jako Google, Intel, Symantec, Adobe, Northrop, Grumman, Dow Chemical a další velké komerční firmy.

---

[226] Operace byla takto pojmenovaná Dmitri Alperovitchem, viceprezidentem „Threat Research" společnosti počítačové bezpečnosti McAfee. U.S.-China Economic and Security Review Commission – "Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation" [cit. 5.5. 2011]. Dostupný na WWW: <http://www.uscc.gov/researchpapers/2009/NorthropGrumman_PRC_Cyber_Paper_FINAL_Approved%20Report_16Oct2009.pdf >.

[227] U.S. Department of Defense, *Annual Report on the Military Power of the People's Republic of China*, USA, 2008.

[228] Tamtéž.

[229] U.S.-China Economic and Security Review Commission – "Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation" [cit. 5.5. 2011]. Dostupný na WWW: <http://www.uscc.gov/researchpapers/2009/NorthropGrumman_PRC_Cyber_Paper_FINAL_Approved%20Report_16Oct2009.pdf>.

10.1.1 Cíle

Americká společnost VeriSign iDefence,[230] jejíž bezpečnostní laboratoře zveřejnily zprávu s technickými detaily o kybernetickém útoku na Google a další společnosti, identifikovala nástroje a řídící servery pro řízení malwaru. Zpráva jednoznačně prohlašuje, že zdroje IP a servery útoků odpovídají jenom jednomu zahraničnímu subjektu složenému buď ze zástupců čínského státu nebo adres jejich proxy serverů. Pokud jsou tedy závěry zprávy relevantní, vyplývá z nich, že čínská vláda se zabývala již několik měsíců masivní kampaní průmyslové špionáže proti americké společnosti.[231] Diplomatické zprávy z velvyslanectví USA v Pekingu a některé tajné dokumenty publikované dne 28. listopadu 2010, tvrdí, že čínské Politbyro[232] nařídilo vniknutí do počítačových systémů společnosti Google. Zdroje dále poukazují na fakt,[233] že útok byl navržen jako součást koordinované kybernetické války provedené „státními zaměstnanci, odborníky na veřejnou bezpečnost a počítačovými zločinci rekrutovanými čínskou vládou.“[234] Dokument rovněž uvádí, že to bylo součástí války, ve které se hackeři „vloupali do počítačů americké vlády jejím spojencům na západě”[235] a podle deníku The Guardian[236] byly útoky „pod taktovkou vedoucího člena politbyra, který napsal své jméno do globální verze vyhledávače a našel články, které ho osobně kritizovaly.“[237]

---

[230] U.S.-China Economic and Security Review Commission, *2007 Report to Congress*, USA, 2007.

[231] U.S. Department of State, International Security Advisory Board Task Force, *Draft Report on China's Strategic Modernization*, September 2008, USA, 2008. s. 37.

[232] Politický úřad komunistické strany Číny. (ÚV KSČ).

[233] U.S.-China Economic and Security Review Commission, *2007 Report to Congress*, USA, 2007.s. 16.

[234] U.S. Department of Defense, *Annual Report on the Military Power of the People's Republic of China*, USA, 2008.

[235] SCOTT SHANE and ANDREW W. LEHREN (November 28, 2010)."Leaked Cables Offer Raw Look at U.S. Diplomacy". *The New York Times*. [cit. 5.5. 2011]. Retrieved 2010-12-26.

[236] Tamtéž

[237] MOORE, Malcolm: *China's global cyber-espionage network GhostNet penetrates 103 countries*. In: http://telegraph.co.uk, 29. března 2009. [cit. 5.5. 2011]. Dostupný na WWW: <http://www.telegraph.co.uk/news/worldnews/asia/china/5071124/Chinas-global-cyber-espionage-network-GhostNet-penetrates-103-countries.html>.

10.1.2 Nástroje

Celou situaci vyšetřovala společnost McAfee a celá řada amerických společností, které byly zasaženy „Aurorou,“[238] pro niž byl použit specifický kód. Podle něj byly vytvořeny sofistikované techniky, které tvořily jádro operace tím, že získaly přístup na řídící server, jenž měl datové napojení na další významné společnosti.[239] Útok byl veden přes uživatelské webové stránky, které byly připojeny ke vzdálenému serveru. Hrozba přišla *nepřímým* způsobem od kontaktů přátel, kterým byl zaslán link z důvěryhodných zdrojů.[240] Útočníci tedy získaly přístup do organizace tím, že poslaly útok na míru několika cílovým jedincům. Jakmile byl tento malware stažený a instalovaný, otevřel se backdoor,[241] který umožil útočníkům kompletní kontrolu nad systémem a stažení požadovaného materiálu. „Operace Aurora“ byla efektivní v tom, že využila zranitelnosti prohlížeče Microsoft Internet Explorer pomocí zneužití chyby *zero day*[242] (tj. zranitelný kód, pro který v současnosti není k dispozici oprava), a tato chyba byla identifikována jako jeden z klíčových bodů v tomto incidentu, jehož cílem bylo získání přístupu do počítačových systémů. Organizace McAfee Labs analyzovala škodilivý kód, který útok využíval.[243] Zvláštností je, že si bezpečnostní experti okamžitě všimli *sofistikovanosti* útoků.[244] Dva dny po tom, co se zprávy o útoku dostaly na veřejnost, společnost McAfee oznámila, že útočníci využili tzv. „zero-day zranitelnosti.“ Kromě „*zero-day*“byly další chyby nalezeny v Perforce, což je zdrojový kód verzí software používaný Googlem pro řízení zdrojového kódu.[245] George Kurtz, zechnologický šéf

---

[238] U.S.-China Economic and Security Review Commission – “Capability of the People’s Republic of China to Conduct Cyber Warfare and Computer Network Exploitation” [cit. 5.5. 2011]. Dostupný na WWW: <http://www.uscc.gov/researchpapers/2009/NorthropGrumman_PRC_Cyber_Paper_FINAL_Approved%20Report_16Oct2009.pdf>.

[239] U.S. Department of Defense, *Annual Report on the Military Power of the People’s Republic of China*, USA, 2008.

[240] Zpráva přišla od kontaktů a od přátel, takže nebyl považován za nebezpečný odkaz a odkaz se začal ihned využívat

[241] U.S. Department of State, International Security Advisory Board Task Force, *Draft Report on China’s Strategic Modernization*, September 2008, USA, 2008.

[242] Tamtéž

[243] Tamtéž

[244] Tamtéž

[245] U.S. Department of State, International Security Advisory Board Task Force, *Draft Report on China’s Strategic Modernization*, September 2008, USA, 2008.

společnosti McAfee uvedl, že *„se jedná se o zlomový okamžik v dějinách počítačové kriminality,“* a dodal: *„dosud jsme nikdy nebyli svědky toho, aby se terčem tak masivního, cíleného a koordinovaného útoku stala komerční firma. Natolik sofistikované akce byly v minulosti cíleny jen proti armádě.”* [246]

10.1.3 Motivace

Podle některých tajných dokumentů, zveřejněných na stránkách Wikileaks,[247] publikovaných 28. listopadu 2010 byly na politickém summitu v Pekingu přímé zabezpečovací systémy proti Googlu a dalších 34 společnostem Silicon Valley vykazovány ve vyhrazeném telegramu, přenášeném čínskými zaměstnanci americké ambasády v Pekingu.

Stejná nadnárodní společnost vyjádřila svůj nesouhlas s kontrolou a filtrováním internetového obsahu, které odráží plošnou kontrolu všech typů médií a je zásadním problémem pro všechny firmy, které na čínském trhu podnikají. Právě tato cenzura a nedávné útoky měly zásadní vliv při zvažování možnosti, že by mohl Google čínský trh opustit, jelikož je globálním internetovým lídrem hlavně z toho důvodu, že důsledně dbá na soukromí uživatelů.[248] Spor nakonec skončil kompromisem: Google obnovil licenci v Číně, a vláda v Pekingu slíbila, že neporuší pravidla cenzury na internetu.

Výzkumné centrum společnosti McAfee zjistilo, že jméno „Aurora“ byl součástí způsobu cesty do souboru v počítači někoho, kdo vložil dva binární kódy malwaru. Podle téže společnosti bylo hlavním cílem útoku získat přístup a modifikovat zdrojový kód bezpečnostních dodavatelů. Například, pokud se do čínské verze vyhledávače Google zadalo klíčové slovo „Tienanmen“ nebo „4. červen 1989,“ výsledky byly cenzurovány.[249] Experti

---

[246] U.S.-China Economic and Security Review Commission – “Capability of the People’s Republic of China to Conduct Cyber Warfare and Computer Network Exploitation” [cit. 5.5. 2011].
Dostupný na WWW:
http://www.uscc.gov/researchpapers/2009/NorthropGrumman_PRC_Cyber_Paper_FINAL_Approved%20Report_16Oct2009.pdf

[247] Tamtéž

[248] Tamtéž

[249] V Google.cn nabídne vyhledávač sérii propagačních turistických fotografií. Jinde ve světě se však zobrazí fotografie a nezkreslené informace o protestech na náměstí Tchi-an-men z roku 1989, při kterých zahynulo několik tisíc lidí.

dále potvrdili, že cílem útoku bylo získat informace o armádních systémech, politických disidentech a zdrojový kód pro softwarové aplikace.[250]

10.1.4 Důsledky

Po útoku Google uvedl, že učinil revizi svých aktivit v Číně. 13. ledna 2010 tisková agentura All Headline News[251] oznámila, že Kongres Spojených států amerických vyšetřoval Google, protože čínská vláda využila služeb společnosti proti aktivistům pro lidská práva.[252] Google oznámil, že útoky pocházející z Číny a že byly součástí politické a průmyslové špionáže, které využilo bezpečnostní chyby v emailových přílohách a dostalo se tak do velkých finančních sítí, obranných a výzkumných institucí USA. Bezpečnostní experti se proto zaměřili na zkoumání komplexnosti útoku, využívající zero-day chyby v Internet Exploreru. Po týdnu společnost Microsoft vydala aktualizaci zabezpečení pro Internet Explorer.[253] Ihned potom vlády Německa, Austrálie a Francie zveřejnily doporučující prohlášení uživatelům, aby nepoužívali Internet Explorer a další prohlížeče určené pro navigaci na Internetu do té doby, dokud nebude identifikována a odstraněna chyba ze strany Microsoftu a software nebude fungovat správně.

Ve skutečnosti rozpory mezi čínskou vládou a společností Google [254] již byly zahájeny na počátku roku 2009, když v březnu čínská vláda blokovala přístup na Youtube a další online služby Googlu. Čína to měla napravit tím, že přesměruje všechny dotazy ve vyhledávání z Google.cn, na Google.com.hk (Google Hong Kong) a obejde většinu čínských zákonů tím, že nepoužije cenzuru na vyhledávání. Stát Hong-Kong je totiž ve skutečnosti zvláštní oblastí Číny, která je vybavena pravomocí nezávislého soudnictví a nepodléhá většině zákonů o čínských právech, a to včetně těch, které vyžadují omezení volného pohybu informací,

---

[250] U.S. Department of Defense, *Annual Report on the Military Power of the People's Republic of China*, USA, 2008.

[251] U.S. Department of Defense, *Annual Report on the Military Power of the People's Republic of China*, USA, 2008

[252] Tamtéž

[253] MOORE, Malcolm: *China's global cyber-espionage network GhostNet penetrates 103 countries*. In: http://telegraph.co.uk, 29. března 2009, [cit. 5.5. 2011]. Dostupný na WWW: <http://www.telegraph.co.uk/news/worldnews/asia/china/5071124/Chinas-global-cyber-espionage-network-GhostNet-penetrates-103-countries.html>.

[254] POSNER, Gerald. China's Secret Cyberterrorism. *The Daily Beast* [online]. 13. ledna 2010, [cit. 1.7. 2011]. Dostupný na WWW:<http://www.thedailybeast.com/blogs-and-stories/2010-01-13/chinas-secret-cyber-terrorism/full/>.

cenzury internetu a materiálů. Prostřednictvím tohoto přesměrování čínští uživatelé mohli sdílet informace, které by nebylo možné sdílet v Číně v souladu se zákony, které se zaměřují na svobodu slova a projevu, a sice narozdíl od původního čínského nastavení, kdy díky vládní cenzuře byla po zadání požadavku obsahující zakázané klíčové slovo, zobrazena zpráva vysvětlující, proč požadavek nebyl dokončen.

Přesně o rok později, 30. března 2010 bylo vyhledávání na všech stránkách Googlu (včetně Google Mobile) v Číně zakázáno. Jakýkoli pokus o vyhledávání na Googlu způsobil chybu DNS.[255] Když se v říjnu 2010 do italské verze Googlu vložilo klíčové slovo „Google China," byl prvním výsledkem portál Hong Kongu, ale hned pod formulářem pro vložení klíče ve vyhledávání se zobrazil odkaz přesměrovávající na Google v Hong Kongu.

Z hlediska konceptu "Information Assurance" je ze zkoumaného pohledu v případě „Operace Aurora" porušena tzv. důvěryhodnost (confidentiality) dat. Zejména se domnívám, že se jedná o jasný příklad narušení důvěryhodnosti dat, duševního vlastnictví společnosti a citlivá data se tak stala hlavním předemětem zisku. Analýza vede k závěru, že hlavní zájem čínských počítačových hackerů se přesouvá od osobních informací k duševnímu vlastnictví firem, především nejznámějších celosvětově působících společností. Duševní vlastnictví firem je často nedostatečně chráněno, a protože ho lze snadno zpeněžit, stává se v podzemní ekonomice v podstatě novým platidlem. Jak vyplývá ze studie, právě únik dat se pokládá za nejvážnější variantu jejich narušení. Krádeže duševního vlastnictví firem se soustřeďují například na obchodní tajemství, marketingové plány, výsledky výzkumu a vývoje nebo i na zdrojové kódy softwaru.

10.2 USA, Jižní Koreja a význam Cyber Command

4. červenec 2009, den amerického svátku Dne nezávislosti,[256] byl do americké historie zapsán jako jeden z nejhorších dnů internetové historie USA. Podle několika agentur, šlo o nejrozsáhlejší kybernetický útok za několik let. [257] Jednalo se o incident, při němž byly napadeny americké webové servery vládních a státních institucí v USA. Spojené státy zasáhla

[255] Domain Name Systém. Jde o systém sloužící k překladu názvu hostitelů. Protokol upravuje poskytování služeb, tak programů i serverů, které spolupracují při poskytování služeb.
[256] [cit. 5.5. 2011]. Dostupný na WWW: <http://en.wikipedia.org/wiki/Independence_Day_United_States>.

[257]Diani, Mario. 2001. "Social movement networks: Virtual and real." In *Culture and politics in the information age : a new politics?*, edited by F. Webster. London ; New York: Routledge.

sérii útoků typu DDoS, kterým pomocí botnetu bylo zasaženo až na 50 000 počítačů. Tato série útoků byla nasměrována na nejdůležitější americké instituce včetně vlády, bezpečnostních agentur a na desítky vládních a obchodních míst v USA. Tyto útoky přímo zasáhly kritickou infrastrukturu Bílého domu, Federální obchodní komisi, tajné služby a deník Washington Post. [258]

10.2.1 Cíle

Útoky byly velmi masivní a namířeny převážně proti klíčovým americkým institucím a úřadům včetně Bílého domu a Pentagonu.[259] Ochromen byl i provoz amerického ministerstva obrany, newyorská burza, Národní bezpečnostní agentura, ministerstvo pro vnitřní bezpečnost, ministerstvo zahraničí a ministerstvo financí. Útok měl několik fází a trval několik dnů. Ke druhé vlně útoků došlo 7. července 2009 v Jižní Koreji. Zde byly zasaženy webové stránky ministerstva obrany, ministerstva veřejné zprávy a bezpečnosti, Národní zpravodajské služby a webové stránky národního shromáždění. Třetí vlna útoků vyvrcholila dne 9. Července 2009 v Jižní Koreji, kde byly zasaženy instituce jako Národní zpravodajské služby, stejně tak i jedna z největších světových bank a hlavní tisková agentura. Havarijní tým USA spolupracoval s odborníky z ministerstva zahraničí, ministerstva pro vnitřní bezpečnost (DHS) a dalších vládních agentur, aby se pokusily vyřešit tento problém.[260]

10.2.2 Nástroje

Na souvislost mezi útoky v USA a v Jižní Koreji ukazoval stejný typ botnetu, použitého při útocích. [261] Jednalo se o botnet způsobující narušení a krádež dat. Tato narušení zabránila lidem v provádění transakcí, nákupu zboží a podnikání.

---

[258] Denning, Dorothy E. 2010. "Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy". Paper read at *The Internet and International Systems: Information Technology and American Foreign Policy Decisionmaking*, December 10, at San Francisco.

[259] Tamtéž

[260] HAENI, Reto E. *Information Warfare: an introduction* [online].
Washington DC: The George Washington University, 1997 [cit. 23.4.2011].
Dostupný na WWW: <http://www.trinity.edu/rjensen/infowar.pdf>.

[261] *Symantec Global Internet Security Threat Report. Trends for 2010.* In: Symantec, duben 2009, [cit. 5.5. 2011]. Dostupný na WWW <http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiv_04-2009.en-us.pdf >.

Podle organizace Symantec[262] útok probíhal jako *W32. Dozer*.[263] Jedná se o škodlivý malware kód, který je zaměřený na zkopírování dat do šifrovaného souboru a může i za přepsání dat v původním souboru. Je zaměřen na soubory spojené s kancelářskými, obchodními a vývojovými aplikacemi. [264] Jihokorejská tisková agentura Jonhap uvedla, že útoky jsou dílem oficiálního činitele a nesou znaky metod používaných čínskými hackery. Naopak podle některých pramenů, stála za útokem Velká Británie, která útočila na webové stránky v USA a Jižní Koreji. Podle bezpečnostního ředitele Bach Khoa Internet Security (Bkis), který tuto zprávu uveřejnil na svém blogu, se podařilo odhalit adresu hlavního serveru, jehož IP adresa byla registrována společností Global Digital Broadcasting ve Velké Británi. Bkis obdržel žádost od KRCERT (Korea Computer Emergency Rsponse Team)[265], aby byly prošetřeny události spojené s útoky DDoS v USA a Jižní Koreji. Po analýze malwarového vzroce podle KRCERT potvrdil tvrzení, že adresa řídícího server koordinovaných útoků byla umístěna ve Velké Británii.

10.2.3 Motivace

Tyto výsledky byly však v rozporu s některými tvrzeními americké a jihokorejské vlády, které prohlásily, že za útoky je zodpovědná Severní Korea,[266] jejíž cílem mělo být údajně otestovat rychlost reakce Jižní Koreje a USA. Nejaktuálnější studie vydaná společností McAfee (červenec 2011)[267] tuto tezi bez výjimky potvrzuje. Zpráva McAfee, vydaná dva roky po útoku, došla k závěru, že dvě vlny distribuovaných internetových útoků byly především zaměřeny na jihokorejské cíle. McAfee ve své studii Ten Days of Rain (Deset dní nečasu) porovnává útoky DDoS. Výsledkem provedených analýz je závěr, že akce provedené v USA a

---

[262] Tamtéž, s. 45

[263] *Symantec Global Internet Security Threat Report. Trends for 2008.* In: Symantec, duben 2009, [cit. 5.5. 2011]. Dostupný na WWW : <//eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiv_04-2009.en-us.pdf >.

[264] Tamtéž, s. 32.

[265] Tamtéž, s. 17.

[266] *Virtual Criminology Report – Cybercrime: The Next Wave.* In: McAfee, [cit. 5.5. 2011]. Dostupný na WWW: <http://www.mcafee.com/us/research/criminology_report/default.html>.

[267] *Ten Days of Rain. Expert analysis of distribued denial-of-service-attacks targating South Korea*. In. McAfee, [cit. 5.5. 2011]. Dostupný na WWW: <http://blogs.mcafee.com/wp-content/uploads/2011/07/McAfee-Labs-10-Days-of-Rain-July-2011.pdf>.

Jižní Koreji si jsou velmi podobné a mají stejného původce – pravděpodobně Severní Koreu nebo její sympatizanty. Podle studie McAfee cílem akcí bylo zřejmě vyzkoušet, jak je kritická jihokorejská infrastruktura připravena na podobné situace. Studie laboratoří McAfee Labs odhaduje pravděpodobnost totožného původce obou útoků na 95%. Výzkum toto své tvrzení dokládá i provedením detailní analýzy architektury botnetu, stejně jako použitého malwaru. Botnet i malware byly velmi sofistikované, přičemž většina infikovaných počítačů se nacházela v Jižní Koreji. Infikované počítače botnetu byly neustále aktualizovány pomocí nových malwarových kódů. Z infikovaných počítačů byly odstraněny klíčové datové soubory a přepsány nulami, a to včetně sektoru MBR (master boot rekord). V důsledku toho pak postižené počítače nešly v podstatě spustit. Na výzkumu se kromě laboratoří McAfee Labs podílel také bezpečnostní tým US-CERT (Comuter Emergency Response Team) a analytici amerického ministerstva obrany.[268]

10.2.4 Důsledky

Po sérii útoků ve Spojených státech ze dne 23.června 2009 nařídilo ministerstvo obrany USA americkému strategického velení vytvořit US Cyber Command. Důvodem pro vytvoření tohoto útvaru byly stále větší obavy USA na základě zvyšujícího se počtu kybernetických útoků z července 2009. US Cyber Command[269] bylo vytvořeno jako reakce na online trestnou a špionážní činnost, která je podle amerických zpravodajských zdrojů v USA čím dále více na vzestupu.[270] Činnost US Cyber Command řídí americké ministerstvo obrany jako svoji jednotku na obranu proti kybernetickým útokům. Na svých stránkách uvádí, že US Cyber Command se stalo důležitou součástí ve *„využívání, plánování a zefektivnění činnosti vojenské obrany v kybernetickém prostoru".*[271] Toto komando centralizuje operace v kyberprostoru, synchronizuje obranu počítačových sítí americké armády a podporuje její vojenské mise. Tento útvar rovněž chrání vojenské počítačové sítě, které by mohly být důležitou součástí národní bezpečnosti a v případě války by měly strategický význam. Cyber

---

[268] *Virtual Criminology Report – Cybercrime: The Next Wave.* In: McAfee, [cit. 5.5. 2011]. Dostupný na WWW: <http://blogs.mcafee.com/wp-content/uploads/2011/07/McAfee-Labs-10-Days-of-Rain-July-2011.pdf>.
[269] Tamtéž, s. 70.

[270] Tamtéž, s. 59.

[271] Cyber Command je součástí nejvyššího stupně velení ministerstva obrany, které řídí počítačové komunikace v Pentagonu. Srov. U.S. Cyber Command [cit. 5.5. 2011]. Dostupný na WWW: <http://www.defense.gov/home/features/2010/0410_cybersec>.

Command tvoří 15 000 počítačových sítí a přes 4 000 vojenských základen v 88 zemích.[272] Doplňuje tak útvary armády, námořnictví, letectví a námořní pěchoty. Cyber Command můžeme přirovnat k takové organizaci, jakým byla Joint Task Force Computer Network,[273] vytvořená v roce 1998, čítající 24 vojenských počítačových odborníků. US Cyber Command je v provozu od října 2010 a vojenská struktura a Bílý dům se snaží rozšířit jeho kompetenci. Ve skutečnosti, plán vytvořit pracovní skupinu, která se specializuje na rozvoj a ochranu vojenských počítačových sítí, byl projednáván již v polovině 90. let. Názor generála Keitha Alexandera, šéfa Cyber Command, že kdyby se neznámé síle podařilo proniknout do důležitých kritických systémů byl by schopen je vyhodit, a potvrzuje, že *„zlepšení ochrany vojenských informačních sítí je prioritou 21. století,"* jak prohlásil ředitel amerického ministerstva obrany.[274] Záměr Bílého domu, jak řekl generál Alexandr Washington Post, je vytvořit tým složený z různých speciálních sil, FBI, Cyber Command a jiných agentur, které mohou zajistit, že každý má moc a schopnosti nezbytné pro ochranu země. Cyber Command má prozatím vojenské kompetence a podle příkazu prezidenta Spojených států amerických, Baraca Obamy, také kompetence zaútočit na soupeře. Spolupracuje s Národní bezpečnostní agenturou (NSA), která sdružuje organizace na elektronickou špionáž a která má moc vniknout dovnitř cizích sítí pro účely dohledu.

První krok vpřed vidíme již v roce 1995, kdy brzy po útoku nerovým plynem v tokijském metru, oznámila vláda USA otevření nového centra specializujícího se na boj proti činnosti hackerů „National Infrastructure Protection Center." Tato struktura by se spojila s ministerstvem obrany se všemi zeměmi, počítačovými stanicemi a bezpečnostními centry univerzit a soukromých společností. Cílem bylo vytvoření obranného systému jako strategicky důležitého bodu v obraně Spojených států amerických.

Vytvoření této zvláštní sítě jednotek vedlo zřejmě k motivování jiných zemí v této oblasti. Čím dál tím více armád po celém světě vynakládá více prostředků na kybernetickou obranu, včetně Spojených Států s jejich vlajkovou lodí US Cyber Command. [275] V prosinci

---

[272] U.S.-China Economic and Security Review Commission, *2007 Report to Congress*, USA, 2007.

[273] Tamtéž

[274] Watts Sean, *Combatant Status and Computer Network Attacks*, in *Virginia Journal of International Law* 50.2, USA, 2010.

[275] Jarrad Shearer. W32.Stuxnet. [cit. 5.5. 2011]. Dostupný na WWW: <http://www.symantec.com/security_response/writeup.jsp?docid= 2010-071400-3123-99>.

2009 Jižní Korea odpověděla na útoky iniciované Severní Korejí vytvořením Cyber Warfare.[276] Navíc i Velká Británie reagovala na nedávný posun v zájmu vojenské kybernetické války vytvořením prvního Cyber Warfare Intelligence Centre[277] a britská zpravodajská služba připravuje Cyber GCHG.[278] A konečně i Čína připravuje svého zástupce pro kybernetickou válku jako reakci na vytvoření Cyber Command.[279] Experti na válečnou strategii zdůrazňují, že ve virtuální realitě je možné zpracovat, zorganizovat a zrealizovat nejzávažnější válečné útoky.

[276] Siemens AG. SIMATIC WinCC/SIMATIC PCS 7: Information concerning Malware/ Virus/Trojan. [cit. 5.5. 2011]. Dostupné na WWW: <http://support. automation.siemens.com/WW/llisapi.dll?func=cslib.csinfo&objid=43876783>.

[277] U.S. Cyber Command [cit. 5.5. 2011]. Dostupný na WWW: <http://www.defense.gov/home/features/2010/0410_cybersec>.

[278] U.S. Cyber Command [cit. 5.5. 2011].Dostupný na WWW: <http://www.defense.gov/home/features/2010/0410_cybersec>.

[279] Pavel Čeleda, Radek Krejčí, Jan Vykopal, and Martin Drašar. Embedded Malware – An Analysis of the Botnet. In Proceedings of the 2010 European Conference on Computer Network Defense, EC2ND '10, pages 3–10, Washington, DC, USA, 2010.IEEE Computer Society. [cit. 5.5. 2011]. Dostupný na WWW: <http://dx.doi.org/10.1109/EC2ND.2010.15>.

Oblast Středního východu

11.1 Útok superviru Stuxnet v Iráku

Stuxnet je počítačový červ objevený v červnu 2010. Je zajímavý tím, že to je první známý červ, který se soustředí na kontrolu průmyslových systémů. Umí přeprogramovat programovatelné logické automatya své změny skrýt. Na nový červ poprvé upozornila běloruská bezpečnostní firma ViruBlokAD.[280] Stuxnet představuje nový a zcela výjimečně nebezpečný druh hrozby. Stuxnet je jeden z druhů červů, který přeprogramovává průmyslová PC vybavená operačním systémem Windows a softwarem Win CC SCADA.[281] Největší softwarová firma na světě Microsoft zjistila, že Stuxnet byl šířen prostřednictvím tzv. *zero-day* zranitelností[282] v operačním systému Windows.[283] Společnost Symantec na základě analýz kódu došla k závěru, že tento kód je velmi nebezpečný, neboť zneužívá hned čtyři zero-day zranitelnosti najednou[284]

11.1.1 Cíle

Stuxnet zahájil *vícevrstevnatý útok* tím, že nejprve infikoval přes USB zabezpečení systému Microsoft Windows[285] a následně využil zranitelná místa v aplikacích Siemens pro

[280] Je známý tím, že je to první známý červ, který se soustředí na kontrolu průmyslových jaderných systémů a byl naprogramován, aby útočil na systémy SCADA.[280] Siemens AG. SIMATIC WinCC/SIMATIC PCS 7: Information concerning Malware/Virus/Trojan. [cit. 5.5. 2011]. Dostupný na WWW: <http://support.automation.siemens.com/WW/llisapi.dll?func=cslib.csinfo&objid=43876783.>.

[281] Používá se jako průmyslový řídící systém pro sledování a řízení průmyslových procesů a infrastruktury. Podobné systémy se používají pro ropovody, rostliny ve velkých komunikačních systémech, uvnitř letišť, lodí a vojenských zařízení. Užívání softwaru Scada vede k domněnce, že důkladná znalost technologie SCADA a využívání několika zero-day zranitelností, vedou k doměnce, že Stuxnet je podporován a finančně dotován státem.

[282] V informatice označení útoku nebo hrozby, která se v počítači snaží využít zranitelnosti používaného software, a která není ještě obecně známá, resp. pro ni neexistuje obrana.

[283] Microsoft na tuto situaci reagovoval s velkou rychlostí hned po té, co byly zjištěny zero-day zranitelnosti, které červ Stuxnet využíval k infikování počítačů.

[284] Jarrad Shearer. W32.Stuxnet[cit. 5.5. 2011]. Dostupný na WWW: <http://www.symantec.com/security_response/writeup.jsp?docid=2010-071400-3123-99>.

[285] Útok v tomto využívá 4 zero chyby v systému Windows. Do systému se dostává přes infikované USB.

Windows. Za cíl měly být vybrány programovatelné logické automaty.[286] Organizace Symantec, světová společnost pro výrobu antivirů, 24. září 2010 varovala uživatele před novým typem velmi nebezpečného červu. Stejná nadnárodní, původem však německá, společnost vyvinula a zpřístupnila prostřednictvím svých internetových stránek také nástroj pro detekci a odstranění tohoto viru. Stuxnet může tedy potencionálně ovládat nebo měnit řídící procesy v systému a měnit způsob, jakým systém funguje.[287] Stuxnet cíleně používal průmyslově řízené systémy prodávané společností Siemens, které jsou po celém světě široce používány k řízení od jaderných generátorů po chemické továrny anebo rozvody vody. Někteří bezpečnostní experti uvedli, že Spojené státy a Izrael vyvíjely Stuxnet pro útoky na íránský nukleární program.[288] Tímto postojem se potvrdil první úspěšně vedený kybernetický útok na infrastrukturní zařízení a velké průmyslové objekty jako například jaderné elektrárny.

11.1.2 Nástroje

Červ Stuxnet nepatří mezi klasický malware, ale zaměřuje se především na systémy s monitorovacími a řídícími funkcemi. Virus byl vyvinut velmi složitě, a pro jeho rozkódování společnost musela najmout týmy programátorů z různých oborů.[289]
Podle Symantec[290] vir Stuxnet má poprvé v dějinách schopnost ohrozit průmyslově řízené systémy a ovlivnit jejich systémové procesy.[291] V průběhu analýzy chování nakažených počítačů byly nalezeny dva konkrétní servery,[292] které sloužily jako řídící centra pro aktivity

[286] Specializované průmyslové řídící počítače-na SCADA systémy německé společnosti Siemens. Také obsahuje 70 šifrovaných bloků, které nahrazují některé klíčové vlastnosti těchto systémů, jako je porovnávání dat a otevírání souborů

[287] Stuxnet byl schopen přeprogramovat software PLC a dát nové instrukce stroji, kdy se kód jevil jako legitimní, protože tvůrci ukradli tajné digitální podpisy dvou tchwajvanských čipových výrobců (REaltel a LMicron), aby software vypadal jako skutečně certifikovaný.

[288] Jarrad Shearer. W32.Stuxnet. [cit. 12.4. 2011]. Dostupný na WWW: <http://www.symantec.com/security_response/writeup.jsp?docid=2010-071400-3123-99>.

[289] Na rozkódování viru spolupracovaly společnosti Kaspersky a Symantec.

[290] Podle společnosti Symantec se tento virus rozšířil ve více než 120 zemí světa a je považován za dílo profesionální skupiny.

[291] Jednou z funkcí Stuxnetu byla i funkce pro připojení ke vzdálenému internetovému serveru, aby o něm červ přijal další příkazy a mohl jej informovat o své činnosti.

[292] Jednalo se malajský a dánský server todaysfutbol.com a mypremierfutbol.com

tohoto kódu. Ve spolupráci s poskytovateli připojení těchto serverů[293] se podařilo zneškodnit škodlivé komponenty, vyřadit je z činnosti, a tak zabránit dalšímu zneužívání obětím nákazy. Zcela nová schopnost a cíl kódu skutečně poškodit průmyslová zařízení je trendem, který ve svých důsledcích může být mnohem více nebezpečný, než dosavadní snahy o pouhý finanční profit. Zejména je zarážející právě to, jakým směrem se strategický vývoj ubírá a nebezpečí toho, že by obdobně mohly vznikat sítě, které ovládají strategicky významné objekty. Stuxnet bývá často srovnáván s Confickerem,[294] mediálně známým červem, který rovněž využíval zranitelnosti Windows.

11.1.3 Motivace

Eugene Kaspersky v projevu na mezinárodním sympoziu o bezpečnosti, konaném v Monaku na konci září,[295] srovnal moc červu s otevřením Pandořiny skříňky: „*Věřím, že jsme se ocitli ve zlomovém bodě. V tuto chvíli stojíme před začátkem nového světa. V minulosti existovali jenom počítačoví zločinci, ale teď se obávám, že začíná éra kyberterorismu, kyberzbraní a kyberválek.*“[296]

Na konci září 2010 obletěla celý svět informace, zveřejněná v německých novinách Allgemaine Zeitung, že hlavním cílem útoku tohoto superviru v Iránubyla snaha zasáhnout centrální jadernou elektrárnu v Natanz. Tuto zprávu ale z Teheránu velmi rychle popřel mluvčí íránského ministerstva zahraničních věcí. Íránská vláda naopak označila zodpovědného za kyberútok a spojenectví s útočníky Spojené státy, přičemž výše zmíněný mluvčí prohlásil, že Stuxnet není nic jiného než plán narušení národního jaderného programu.[297]

---

[293] (kteří mimochodem o nákaze na serverech neměli ani potuchy). Čestí specialisté na kybernetickou obranu objevili nový kybernetický útok. Tisková zpráva. [cit. 5.5. 2011]. Dostupné na WWW: <http://www.army.cz/images/id_15001_16000/15609/023.doc. >.

[294] Conficker je typ botnetu, který je zneužitelný na libovolnou úlohu (rozesílání spamu, cílené útoky na firemní sítě), ovladatelnou na dálku. Tyto varianty se šíří přes internet, ale i vyměnitelnými médii jako USB. Conficker dominuje statistikám všude ve světě, včetně České republiky.

[295] Jarrad Shearer. W32.Stuxnet. [cit. 12.5. 2011].Dostupný na WWW: <http://www.symantec.com/security_response/writeup.jsp?docid=2010-071400-3123-99>.

[296] Jarrad Shearer. W32.Stuxnet. [cit. 5.5. 2011].]. Dostupný na WWW: <http://www.symantec.com/security_response/writeup.jsp?docid=2010-071400-3123-99>.

[297] Siemens AG. SIMATIC WinCC/SIMATIC PCS 7: Information concerning Malware/Virus/Trojan. [cit. 5.5. 2011]. Dostupný na WWW: <http://support.automation.siemens.com/WW/llisapi.dll?func=cslib.csinfo&objid=43876783>.

Sean McGurk, ředitel National Cybersecurity and Communication Integration Center (NCCIC),[298] potvrdil, že je velmi obtížné určit důsledky červu Stuxnet.[299] Na geopolitické úrovni červ znamená obrovskou mezinárodní hrozbu. Liam O. Murch, bezpečnostní expert společnosti Symantec, odhaduje na 45 tisíc nákaz ve světě, zejména v Iránu, Číně, Indii, Indonésii a Pakistánu.[300] Na podporu tvrzení Liama O. Murcha, je zde teze německého odborníka na počítačové systémy a průmyslové aplikace Ralpha Langera, který ve své analýze uvádí, že nevěří tomu, že by samostatný hacker infikoval tak obrovské množství počítačů, naopak se domnívá, že se jedná o politickou vůli státu.[301] Předpokládá také, že konkrétním cílem byl jaderný reaktor v Natanzu.[302] Evropská unie je v důsledku této reálné hrozby odhodlána vytvořit zákon, který by specificky řešil tento konkrétní problém červu typu Stuxnet.[303] Zvláštností červu Stuxnet je i to, že není navržen tak, aby kradl peníze nebo zasílal spam či odcizoval osobní údaje, ale byl vytvořen za účelem narušení a poškození průmyslových systémů. Jestliže devadesátá léta byla přejmenována na desetiletí kyberzločinců, tak začátek nového tisíciletí je ve znamení strachu před kyberterorismem a kyberválkou.

Cíl a místo útoku, kde tento malware působil, ukazuje na zapojení kriminálních skupin, protože záměrem nebylo infikovat iránský systém, ale sabotovat ho. Společnost Kaspersky Lab má ale vizi poněkud více apokalyptickou a klasifikuje tento útok jako počátek zrození nových armádních závodů ve zbrojení ve světě, a to mnohem více než tomu bylo dosud. "Kybersabotáž" by mohla regulovat rychlost jaderné turbíny, způsobit výbuchy v průmyslových závodech nebo spustit více či méně katastrofální selhání v elektrárnách s vybavením vyvinutým firmou Siemens.

---

[298] Pavel Čeleda, Radek Krejčí, Jan Vykopal, and Martin Drašar. Embedded Malware – AnAnalysis of the Chuck Norris Botnet. In Proceedings of the 2010 European Conferenceon Computer Network Defense, EC2ND '10, pages 3–10, Washington, DC, USA, 2010.IEEE Computer Society. Dostupný na WWW: <http://dx.doi.org/10.1109/EC2ND.2010.15. >.

[299] Tamtéž

[300] Tamtéž

[301] Tamtéž

[302] S odvoláním na fotografie obrazovky systému řídícího reaktoru, který zobrazil varování licence, která vypršela.

[303] Čestí specialisté na kybernetickou obranu objevili nový kybernetický útok. Tisková zpráva. [cit. 5.5. 2011]. Dostupný na WWW: <http://www.army.cz/images/id_15001_16000/15609/023.doc.>.

11.1.4 Důsledky

Téma Stuxnet bylo také ústředním tématem na konferenci o bezpečnosti počítačů ve Vancouveru, která se uskutečnila jako setkání předních odborníků na téma bezpečnosti počítačů v kyberprostoru. Bohužel Organizace Spojených Národů (OSN) se není schopna dohodnout na společné definici terorismu. Záměr je nepochybně jeho důležitou součástí, ale je velmi obtížné ho změřit. Od roku 2007 studijní skupina pro John Jay College of Criminal Justice tuto záležitost vyšetřeje s úmyslem určit reálné riziko kyberteroristického činu. Výsledky ukazují, že cyber terorismus byl nepravděpodobný ještě v roce 1993. [304]O červu Stuxnet se mluví jako o vynikající práci profesionálů a přelomový počin v počítačové bezpečnosti.[305] Poprvé má červ reálnou schopnost vážně poškodit a monitorovat významné průmyslové řídící systémy a ovlivnit procesy, které s těmito systémy souvisejí.

Pokud Stuxnet ukázal, že průmyslová zařízení jsou příliš zranitelná, nyní musí rozhodnout, zda ve skutečnosti představuje první případ počítačového viru pro vojenské účely pro destruktivní útok v reálném světě.

Podle zpráv z 28.července 2010 agentury Reuters americké státní kybernetické společnosti experti varují, že virus Stuxnet se může stát mnohem nebezpečnějším než byl v roce předcházejícím. Ministerstvo pro vnitřní bezpečnost strávilo poslední rok studiem sofistikovaného škodlivého software a dospělo k prvním výsledkům říkajícím, že malware typu Stuxnet se může objevit pouze se státní podporou.

Už v roce 2007 mnoho expertů poznamenalo, že státy neprovozují jenom špionážní útoky v *cyberspace*, ale vyvíjí počítačové útoky stále více sofistikovanější. Mnohé útoky byly motivovány především politickými účely a bylo taky velmi obtížné je označit za počítačovou kriminalitu.

Z hlediska konceptu "Information Assurance" byl červ Stuxnet odlišný v charakteru hrozby i motivace potenciálního útočníka (kontrola řídících systémů), frekvenci a kritičnosti uplatnění hrozby. Je jisté, že cílem byla analýzu toku vyměňovaných zpráv, resp. frekvence zasílání, analýza adres, neoprávněné kopírování a monitoring informací (což poukazuje na porušení

---

[304] *Symantec Global Internet Security Threat Report. Trends for 2008.* In: Symantec, duben 2009, [cit. 5.5. 2011]. Dostupný na WWW: <http://www.symantec.com/connect/blogs/stuxnet-introduces-first-known-rootkit-scada-devices>.
[305] Tamtéž

zdrojů a cílů zpráv), neautorizované použití zdrojů (krádeže hardwarových a softwarových komponent, včetně používání neoprávněných kopií), neautorizované používání informačních systémů a služeb jimi poskytovaných. Zde byla podle nás porušena vzhledem ke konceptu „Information Assurance“ jednak *důvěrnost* informací (kdy neautorizovaný subjekt si neoprávněně zpřístupnil aktiva - Stuxnet prováděl odposlech při datových přenosech po síti) a rovněž i *modifikace* dat – neautorizovaný subjekt zasáhnul provedl změny uložených nebo přenášených dat či přidal funkce do systému. Podle konceptu „Information Assurance“ bychom mohli říct, že došlo i k *neporiatelnosti* (non-repudiaton) dat. Byl prokazatelně zaměřen i na autenticitu dat, (tj. nastal případ, kdy neautorizovaná strana vytvořila podvržení transakce nebo iniciovala dodání falešných dat. Takto komplexní druh útoku je předpokladem kybernetických hrozeb budoucnosti a dokladem trendu ve zvýšení sofistikovanosti útoků. Za tímto typem útoku stojí obvykle profesionálně zdatní jedinci, čímž je útok na data mnohem nebezpečnějším a zajištění ochrany dat před takto komplexním druhem útoku daleko komplikovanějším.

KOMPARACE A ZÁVĚR

Ve své práci jsem se pokusila potvrdit hypotézu nezbytnosti aplikování konceptu „Information Assurance“ na vybraných příkladech kybernetických válek. Použitá metoda zkoumání problematiky kyberterorismu a uplatnění konceptu „Information Assurance“ po stránce teoretické i analytické upozornila na uplatnění této koncepce v kritické infrastruktuře ICT.

V první části, teoretické, jsme rozebrali problematiku informačních a komunikačních technologií, zejména v části řešící problematiku ochrany dat v informačních systémech, dále jsme se věnovali jednotlivým částem informačního systému a shrnuli jsme nejzásadnější hrozby bezpečnosti informačních systémů.

V druhé teoretické části, nazvané „Koncept Information Assurance aplikovaný v řízení informačních systémů,“ jsme se zaměřili zejména na ochranu logického přístupu k datům a jeho hlavních částí zahrnujících atributy dostupnosti informací, integrity, důvěryhodnosti a nepopiratelnosti, které společně tvoří koncept „Information Assurance,“ jenž je v praxi spojen s využíváním, zpracováním, uložením a přenosem informací a dat mezi systémy. Díky tomuto konceptu je infromačním systémům poskytnut důkaz o věrohodnosti informací, což významně napomáhá definovat požadavky na zajišťění všech potřebných atributů při zabezpečení počítačové bezpečnosti.

V části nazvané „Definice a vymezení kyberterorismu“ jsme se pokusili definovat a vymezit základní stanovení kybernetického terorismu, jeho vazby na kybernetickou válku, poukázali jsme na různorodou terminologii a definovali podstatu kybernetického hactivismu s uvedením praktických příkladů ve formách kybernetické špionáže a propagandy. Významnou částí byla problematika kritické infrastruktury jakožto nejdůležitějších cílů kybernetických útoků a aktérů, kteří se na těchto útocích podílejí.

V analytické části práce jsme se snažili o chronologický rozbor významných případů kybernetických válek nedávné minulosti, utříděný dle světových geopolitických oblastí míst vzniku jednotlivých kybernetických konfliktů. Z tohoto úhlu pohledu šlo tedy především o konflikty evropsko-ruské oblasti, a to zejména o střety v Gruzii a Estonsku, kde jsme se zaměřili na hodnocení a komparaci motivace a příčin těchto hlavních kybernetických konfliktů. Následující díl analytické části je věnován kybernetickým útokům v asijsko-americké oblasti, tedy především kybernetickému střetu mezi komerční firmou Google a Čínskou lidovou republikou, který je typický značnou sofistikovaností kybernetických

nástrojů. V oblasti asijsko-americké jsme se dále zaobírali kybernetickými útoky proti USA a Jižní koreji a zrozením nového typu „virtuální armády“ s předlohou v její americké *verzi US Cyber Command*. Posledním geopolitickým makroregionem, kterým jsme se z hlediska kybernetických konfliktů zaobírali, byla oblast Středního východu, kde se jako první rozšířil nejnovější supervir Stuxnet, představující významnou změnu v oblasti nástrojů kybernetických válek. Jak již bylo řečeno, je zajímavý tím, že jako první červ ve světě přeprogramovává průmyslová zařízení a dokáže svou kontrolu nad těmito systémy skrýt.

Lze shrnout, že v případech Gruzie a Estonska se obě strany dovolávaly stejných institutů mezinárodního práva a oficiálně směřovaly ke stejným cílům (sebeobrana, vzájemná obvinění z etnických čistek, nastolení nebo obnovení míru a ochrana civilního obyvatelstva). Tato skutečnost logicky vylučuje možnost, že by úmysly obou stran byly opravdu takovové, jak jejich představitelé prohlašovali. Naopak se jeví velmi pravděpodobné, že obě strany sledovaly jiné mocenské cíle. Tomu nasvědčuje jak jejich chování v letech předcházejících konfliktu, tak i kroky v jeho průběhu. Hlavní cíle tedy pravděpodobně představovaly především oficiální webové stránky jako stránky předsednictva, soudů a parlamentu, a to ve smyslu narušení základních komunikačních operací. Pro uživatele měl tento akt za následek nedostupnost, modifikaci obsahu i omezení služeb, ve skutečnosti byl tedy narušen koncept „Information Assurance.“ Z častého porušování mezinárodního práva během konfliktu lze dovodit i jeho nezpůsobilost zajistit mezinárodní spravedlnost. Jak Rusko, tak i Gruzie porušovaly pravidla mezinárodního humanitárního práva, což mělo dopady zejména na civilní obyvatelstvo.

Problém „Operace Aurora“ – Číny a komerční firmy Google stanovil na mezinárodním poli otázky hackerů a nejrůznějších skupin, které Čína používá k omezování projevu na vlastním území. Čínský útok na Google mohl být kybernetickou krádeží, neboť se na mezinárodním poli poprvé objevil kybernetický útok do citlivých oblastí komerčních firem (dodavatelé armády, zpravodajské složky). Tento typ útoku byl zcela jistě útokem orientovaným na krádež značného množství informací. Tento případ může být ukázkou průmyslové špionáže a zneužití dat v komerčních firmách a dokladem mezinárodní otázky v oblasti dodržování lidských práv ze strany Číny, tamní cenzury informací, porušování zákonů, přičemž ve sporu obě strany užívaly v první řadě své vlastní politické nástroje a mezinárodní právo sloužilo spíše k dodatečné obhajobě.

Jak tomu bylo například v případě USA a Jižní Koreje, kybernetické útoky často evokují dojem státem objednaného útoku. Je těžké předvídat, jakým způsobem budou ukradená data využita a zda budou následně využita v konkurenčním boji při získávání

zakázek, strategickém mezistátním vyjednávání nebo například při vývoji nových produktů. Jednalo se o další z mnoha útoků cílených na získání potřebných dat. V případě Stuxnetu a Iránu se dospělo na mezinárodním poli k obavám etickým, neboť tento supervir dospěl až do takové fáze, jakými jsou řízení jaderných zařízení, kdy jej někteří odborníci na Stuxnet označují za první „řízenou kybernetickou střelu."

Můžeme potvrdit, že současné počítačové útoky se vyvíjejí a jsou stále více sofistikovanější. Mnohé útoky byly motivovány především politickými účely a bylo také velmi obtížné je označit za počítačovou kriminalitu. Podle dostupných poznatků můžeme tvrdit, že vzrůstají útoky na národní státy, a ty tak posilují své kapacity v kyberprostoru. Rizika a dopady proběhlých událostí ukazují na několik společných indikátorů do budoucnosti, kterou lze spatřit především v tom, že vlády ještě zvětší své úsilí při přípravě na budoucí kyberteroristické útoky a stanoví podmínky za kterých útoky musí aktivovat princip obrany mezinárodních paktů jako například NATO, kdy útok na jednoho, znamená útok proti všem. Je velmi důležité poznamenat, že je to pravděpodobně soukromý sektor, který bude první oběí v křížové palbě moci (viz Google a Aurora). Všechny státy mají tak společné to, že je nejvíce ohrožena kritická infrastruktura jejich systémů – zejména elektronické bankovnictví a finanční sektor.

Tímto byl splněn jeden ze stěžejních cílů práce, a to shrnout a systematicky utřídit informaci o kybernetickém terorismu, z pohledu aplikace konceptu „Information Assurance". Byly ukázány praktické i teoretické přístupy k rozvoji poznání nové teorie válčení v kybernetickém prostororu.

Pokud dále, ve světle výše uvedených závěrů, posuzuji v úvodu stanovenou hypotézu, pak ji považuji za fakticky ověřenou. Během práce se mi podařilo získat velké množství informací, které se týkají zkoumané problematiky. Jejich ověřováním, tříděním a promýšlením širších souvislostí jsem si vytvořila jasný a pevný osobní názor nejen na vlastní konflikty v oblastech kybernetických bojů, ale posunula jsem i svůj náhled na mezinárodní politiku a mezinárodní vztahy obecně.

Koncept „Information Assurance" měl za cíl ověřit význam jednotlivých atributů (dostupnosti, integrity, autentizace, důvěryhodnosti a nepopiratelnosti) jako významných složek informační bezpečnosti v kyberteroristických útocích. Z výše uvedených analýz můžeme vyvodit závěr, že tento koncept má rozhodně stále svůj význam v informačních systémech s vysokými bezpečnostními požadavky. Cílem analýzy bylo prozkoumat, jaký atribut a by přispěl ke zvýšení informační bezpečnosti. Mým doporučením je v prvních dvou případech (Gruzie a Estonska) posílit atribut integrity, který by zajistil dostupnost

autorizovaným uživatelům, neboť data při přenosu nemohou být neautorizovaně měněna a nelze je modifikovat ani v místě jejich dlouhodobého uložení. Pro zajištění integrity lze použít např. mechanismů kryptografických hashovacích funkcí, digitálního podpisu a certifikátů na bázi asymetrické kryptografie. Pro zajištění integrity softwaru je přirozeně nutné používat také adekvátní aktuální antivirové nástroje. Po zkušenostech s výše uvedenými případy lze také upozornit na požadavek autentičnosti, jenž by měl být poskytnut například formou dostatečně důvěryhodného prokázání identity Dalším doporučením je nepochybně zabezpečení potřebného informačního rozsahu důvěrnosti, která má zásadní význam z hlediska ochrany soukromých dat, a to jak pro zachování soukromí, tak i pro možnosti zneužití informačních služeb, (a který by se dal efektivně využít při činských hackerských operacích. Zejména koncept „Information Assurance“ poukazuje na fakt, že důvěrnost informačního systému, je jedním ze základních požadavků, jenž lze zabezpečit pomocí šifrování, skrývání identit počítačů organizace za firewally nebo pomocí řízení přístupu k souborům ku příkladu na WWW serverech. Nedílnou součástí bezpečnostní politiky on-line provozovaných informačních systémů musí být opatření zajišťující trvalou dostupnost jeho informačně komunikačních služeb, tj. zamezující neoprávněnému vyčerpání zdrojů vnějšímu útočníkem nebo nedokonale vyškoleným vlastním zaměstnancem organizace, což by mohlo pomoci eliminovat útoky v rámci informačních systémů.

Závěrečná odpověď na vytyčenou hypotézu v úvodu práce je taková, že pokud by jednotlivé státy dodržely všechny prvky konceptu „Information Assurance“, tak teoreticky mohly zabránit kyberteroristickému útoku. U všech výše jmenovaných útoků došlo k porušení alespoň jednohoto atributu konceptu „Information Assurance,“ tudíž lze konstatovat, že je koncept stále platný a i přes rychlý vývoj nových multimediálních médií stále využitelný.

Dílčí části (po jednotlivých výše zmíněných tématech) práce mohou být samostatně použity jako významný informační podklad, který vyhodnocuje současný stav výsledků výzkumů v oblasti kybnerterorismu a bezpečnosti dat. Přínosem je též systematické utřídění poznatků o kybernetickém terorismu, orientované na odhalení jeho dosud takřka nepoznaných nebo nepopsaných částí. Logicky zdůvodněné závěry umožnily formulovat vlastní názory na budoucnost kybernetického terorismu v rovině teoretické, terminologické i praktické. Systematické utřídění informací s ohledem na koncept „Information Assurance” je využitelné i pro další výzkum. Pro zpracování tématu bylo nezbytné seznámit se a v potřebné míře analyzovat značně rozsáhlý soubor různorodých informací, které jsou k problematice dosažitelné.

Doufám tedy, že jsem svou prací přispěla k rozšíření dostupných poznatků o kyberterorismu v českém jazyce a pomocí systematických analýz osvětlila největší hrozby, kterými kyberterorismus disponuje, čímž jsem snad budoucí čtenáře této práce přesvědčila o nutnosti ochrany dat a motivovala je ke snaze přispět k jejímu zajištění v budoucnu.

POUŽITÁ LITERATURA

Ars Technica. *IT and business computing insights* [online]. Condé Nast Digital, c2011. Tim Berners-Lee on Web 2.0: "nobody evens know what it means". By Nate Anderson. 2007, [cit. 7.7. 2011]. Dostupný na WWW:<http://arstechnica.com/business/news/2006/09/7650.ars>.

ASHMORE, William. Impact of Alleged Russian Cyber Attacks. In *Baltic Security & Defence Review*. Baltic Defence College, 2009 [cit. 7.7. 2011]. Dostupný na WWW: <http://www.bdcol.ee/files/files/documents/Research/BSDR2009/1_%20Ashmore%20-%20Impact%20of%20Alleged%20Russian%20Cyber%20Attacks%20.pdf>.

ANTINORI, Areje. *Information & Communication Technology (I.C.T.), tra mutamento sociale e sicurezza. Uno sguardo al futuro in Quaderno dei lavori 2008.* Messina : C.I.R.S.D.I.G, 2009.

BANDYOPADHYAY, Samir Kumar ; KIM, Tai-hoon. A Cryptosystem for Encryption and Decryption od Long Confidential Messages. In *Information security and assurance : 4th international conference, ISA 2010, Miyazaki, Japan, June 23-25, 2010 : proceedings*. New York : Springer, 2010. s. 97. ISBN 9783642133640.

BARBER, Richard. Hacking Techniques : the tools that hackers use, and how they are evolving to become more sophisticated. In *Computer*. Fraud and Security, 1st March 2003, no. 3, p. 9-10.

BASKERVILLE, R. Information Warfare: a comparative framework for Business Information Security. In *Journal of Information System Security*. 2005, no. 1. ISSN 2010-2658.

BEAVER, Kevin ; MCCLURE, Stuart. *Hacking for Dummies*. 3rd ed. Indianapolis : Wiley, c2010. 408 s. ISBN 076455784X.

BLYTH, Andrew ; KOVACICH, Gerald L. *Information Assurance: Security in the Information Environment.* USA : Springer, 2006. Edition: Computer Communications and Networks. 280 p. ISBN 9781846282669.

CISSP: Certified Information Systems Security Professional study guide. Edited by Ed Tittel, Mike Chapple, James Michael Stewart. San Francisco, Calif. ; London : SYBEX, 2003. xlv, 783 s. ISBN 0782141757.

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

CELEDA, Pavel, KREJČÍ Radek, VYKOPAL,Jan and DRAŠAR,Martin. Embedded Malware – An Analysis of the Chuck Norris Botnet. In Proceedings of the 2010 European Conference on Computer Network Defense, EC2ND ’10, pages 3–10, Washington, DC, USA, 2010. IEEE Computer Society. Dostupný na WWW: <http://dx.doi.org/10.1109/EC2ND.>.

Čestí specialisté na kybernetickou obranu objevili nový kybernetický útok. Tisková zpráva. Dostupný na WWW: <http://www.army.cz/images/id_15001_16000/15609/023.doc.>.

ARQUILLA, John, RONFELDT, David. *Networks and Netwars : the Future of Terror, Crime, and Militancy*. DENNING, Dorothy E. Activism, Hactivism, and Cyberterrorism : the Internet as a Tool for Influencing Foreign Policy Santa Monica : RAND, 2001. s. 288. ISBN 0-8330-3030-2.

DENNING, Dorothy E. *Information Warfare and Security*. 1st ed. UK : Addison-Wesley Professional, 1998. ISBN 978-0201433036.

DENNING, Dorothy E. *Georgetown University* [online]. 23. května 2000 [cit.1.7.2011]. Cyber Terrorism: Testimony before the Special Oversight Panel on Terrorism. Dostupný na WWW: <http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html>.

DI NUCCI, Darcy. Fragmented Future. *Design and New Media.* [online]. 1999, vol.53, April [cit.1. 7. 2011]. Dostupný na WWW:<http://www.cdinucci.com/Darcy2/articles/Print/Printarticle7.html> ISSN: 0737-8831

EVERARD, Paul. NATO and Cyber Terrorism. In: *Response to Cyber Terrorism*. Amsterdam, IOS Press, 2008.

Full Blown Cyber War: An Information Age War in the Making. Cyber War: The Third World War. In: Cyberoam. [cit. 1. 7. 2011] Dostupný na WWW: <http://newsletters.cyberoam.com/072008/images/FullBlownCyberWar.pdf >.

Full Blown Cyber War: An Information Age War in the Making. Cyber War: The Third World War. In: Cyberoam. [cit. 1. 7. 2011] Dostupný na WWW: <http://newsletters.cyberoam.com/072008/images/FullBlownCyberWar.pdf >.

GARDNER, Greg. Combating Cyber Warfare Against Information and Networks. In *Defense Science Board 2007 Summer Study: Challenges to Military Operations in Support of U.S. Interests*. Albany : Government and Homeland Security Solutions, 2007 [cit. 1. 7. 2011]. Dostupný na WWW: <https://www.cscic.state.ny.us/security/conferences/security/2008/info/Day%201/B1-Gardner%20Combating%20CyberWarfare.ppt>.

GEERS, Kenneth: *Cyberspace and the changing nature of warfare*. In: SC Magazine, 27. srpna 2008 [cit. 1. 7. 2011]. Dostupné na WWW: <http://www.scmagazineus.com/Cyberspace-and-the-changing-nature-of-warfare/article/115929/>.

HUBER, Jordana. Cyber Attacks „Grossly Underestimated“. Industries lack technology and skill to counter dangerous hackers, security expert says. In *Financial Post*, 26. června 2009 [cit. 1. 7. 2011] Dostupný na WWW: <http://www.financialpost.com/m/story.html?id=1731010>.

International Crisis Group Europe Report N°151, *Georgia: What now?*, Tbilisi/Brussels 2003.
International Crisis Group Europe Report N°195, *Russia vs Georgia: The Fallout.*
Cornell, S.E.: *Pipeline Power, The War in Georgia and the future of the Caspian Energy Corridor.*
Georgetown Journal of International Affairs, Iss 10.1, Winter/Spring 2009, s. 131 - 139.

OECD. *Information Security and Privacy* [online]. [cit. 1. 7. 2011]. Dostupné z WWW: <http://www.oecd.org/department/0,3355,en_2649_34255_1_1_1_1_1,00.html>.

International Terrorism and Security Research [online]. 2004 [cit. 1. 7. 2011]. State Sponsored Terrorism. Dostupné na WWW: <http://www.terrorism-research.com/state/>.

JANCZEWSKI, Lech ; COLARIK, Andrew. *Managerial Guide for Handling Cyber-Terrorism and Information Warfare*. London: IGI Global, 2005. 229 s. ISBN 978-1591405498.

JANOUŠEK, Michal. Kybernetický terorismus: terorismus informační společnosti. In *Obrana a strategie*, 2006, č. 2, [cit. 1. 7. 2011]. Dostupný na WWW: <http://www.defenceandstrategy.eu/cs/archiv/rocnik-2006/2-2006/kyberterorismus-terorismus-informacni-spolecnosti.html>.

SHEARER, Jarrad . W32.Stuxnet. [cit. 1. 7 . 2011]. Dostupné na WWW: <http://www.symantec.com/security_response/writeup.jsp?docid=2010-071400-3123-99>.

JIROVSKÝ, Václav – HNÍK, Václav – KRULÍK, Oldřich: *Základní definice, vztahující se k tématu kybernetických hrozeb*. In: Ministerstvo vnitra ČR, . [cit. 1. 7 . 2011]. <http://web.mvcr.cz/archiv2008/bezpecnost/informacni/zakladni_info.pdf>.

JOHNSON, L.S. *A Major Intelligence Challenge: Toward a Functional Model of Information Warfare* [online]. 1997 [cit. 1. 7. 2011] Dostupné na WWW: <https://www.cia.gov/csi/kent_csi/pdf/v40i5a07p.pdf>.

KAKABADSE A.; KAKABADSE N. Outsourcing : Current and Future Trends. *Thunderbird International Business Review* [online]. 2005, vol. 47, no. 2 [cit. 1. 7. 2011]. Dostupný na WWW: <http://people.oregonstate.edu/~sanderni/outsourcing.pdf>.

KOLOUCH, J. ; Volenecký, P. *Trestněprávní aspekty phishingového útoku. Trestní právo,* 2008, roč. XII, č. 9, s. 5 – 12. ISSN 1211-2860.

KREBS, Brian: *Report: Russian Hacker Forums Fueled Georgia Cyber Attacks.* In: The Washington Post, 16. října 2008, http://voices.washingtonpost.com/securityfix/2008/10/report_russian_hacker_forums_f.html (15th September 2009); MESERVE, Jeanne: Study Warns of Cyberwarfare during Military Conflicts. [cit. 1. 7. 2011]. In: www.cnn.com/US, 17. srpna 2009 Dostupné na WWW: <http://www.cnn.com/2009/US/08/17/cyber.warfare/index.html>.

KREBS, Brian. Report: Russian Hacker Forums Fuelled Georgia Cyber Attacks. In *The Washington Post*, 16. října 2008, 119 [cit. 1. 7. 2011]. Dostupné na WWW: <http://voices.washingtonpost.com/securityfix/2008/10/report_russian_hacker_forums_f.html>.

LANDREE, Eric ; GONZALES, Daniel. *Implications of Aggregated DoD Information Systems for Information Assurance Certification and Accreditation*. USA : RAND Corporation, 2010.

LORD William, *USAF Cyberspace Command: To Fly and Fight in Cyberspace*, Strategic Studies Quarterly, Fall 2008, USA, 2008.

MARTIN, Clemens; SCHELL, Bernadette. *Cybercrime: A Reference Handbook*. Santa Barbara: ABC-CLIO, 2004. 247 s.

MARSAN, Carolyn Duffy: *How close is World War 3.0?* Network World, 24, 27. srpna 2007, č. 33, s. 156

MATĚJKA, M., Počítačová kriminalita, Praha: Computer Press, 2002, str.237

MAZANEC Brian M., *The Art of (Cyber) War* in *The Journal of International Security Affairs*, Spring 2009 – Number 16, USA, 2009.

McAfee. *Zpráva společnosti McAfee o virtuální kriminalitě : první celoevropská studie o organizovaném zločinu a internetu* [online]. 2004 [cit. 1. 7. 2011]. Dostupný na WWW: <http://www.fi.muni.cz/~xbitto/McAfee_kriminalita.pdf>.

McAfee. *Zpráva společnosti McAfee o virtuální kriminalitě : první celoevropská studie o organizovaném zločinu a internetu* [online]. 2010 [cit. 1. 7. 2011]. Dostupný na WWW: <http://us.mcafee.com/en-us/local/docs/MTMW_Report.pdf>.

McAfee. *Zpráva společnosti McAfee o virtuální kriminalitě : první celoevropská studie o organizovaném zločinu a internetu* [online]. 2010 [cit. 1. 7. 2011]. Dostupný na WWW: <http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf>.

McQUADE III., Samuel. *Encyclopedia of Cybercrime*. Westport : Greenwood, 2008. 232 s

MESERVE, Jeanne: *Study Warns of Cyberwarfare during Military Conflicts*. In: cnn.com/US, 17. srpna 2009, [cit. 1. 7. 2011]. Dostupný na <http://www.cnn.com/2009/US/08/17/cyber.warfare/index.html>.

Ministry of Foreign Affairs of Georgia (8.8. 2008): *Statement of the Ministry of Foreign Affairs of Georgia*, Dostupný na WWW: <http://www.mfa.gov.ge/index.php?lang_id=ENG&sec_id=59&info_id=7201);
Ministry of Foreign Affairs of the Russian Federation (9.8. 2008): *Inteview by Minister of Foreign Affaires of the Russian Federation Sergey Lavrov to BBC, Moscow, August 9, 2008* Dostupné z WWW: <(http://www.mid.ru/brp_4.nsf/e78a48070f128a7b43256999005bcbb3/f87a3fb7a7f669ebc32574a100262597?OpenDocument)>.

MOORE, Malcolm. China's global cyber-espionage network GhostNet penetrates 103 countries. In *Telegraph.co.uk*, 29. března 2009 [cit. 1. 7. 2011]. Dostupný na WWW: <http://www.telegraph.co.uk/news/worldnews/asia/china/5071124/Chinas-global-cyber-espionage-network-GhostNet-penetrates-103-countries.html>.

MOSCA, Carlo ; GAMBACURTA, Stefano ; SCANDONE, Giuseppe ; VALENTINI, Marco. I *Servizi di Informazione e il Segreto di Stato (Legge 3 gennaio 2011, n.124).* Milano : Giuffré Editore, 2011.

NAGESH, Gautham: *Latest Security Threat Lies in Trusted Software and Hardware*. In: Nextgov, Dostupný na WWW: <http://www.nextgov.com/nextgov/ng_20080825_7185.php>.

NICOL D., SANDERS W., TRIVEDI K., *Model-Based Evaluation: From Dependability to Security* in *IEEE Transcript on Dependable and Secure Computing* 1, No.1, January-March, USA, 2004.

Network and Information Society: Proposal for a European Policy Approach. In: Portál Evropské unie, Dostupný na WWW: <http://eur-lex.europa.eu/LexUriServ/site/en/com/2001/com2001_0298en01.pdf >.

New Approach to technical harmonization and standardization. In: Portál EU, Summaries of EU Legislation. [cit. 1. 7. 2011]. Dostupný na WWW: <http://europa.eu/legislation_summaries/internal_market/single_market_for_goods/technical_harmonisation/l21001a_en.htm>

Novotný, J., Čeleda, P., Dedek, T. *Hardware Acceleration for Cyber Security.* In IST-091 – Information Assurance and Cyber Defence. Antalya (TUR) : NATO Research and Technology Organization, 2010.

OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. In: Organisation for Economic Cooperation and Development (OECD), [cit. 1. 7. 2011]. Dostupný na WWW: <http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html>

O'REILLY, Tim. Web 2.0 Compact Definition: Trying Again. *O'Reilly – SpreadingThe Knowfledge Of Technology Innovators* [online]. 2006 [cit. 1. 7. 2011] Dostupný na WWW: <http://radar.oreilly.com/archives/2006/12/web-20-compact.html>

OWENS, William A., Dam Kenneth W., Lin Herbert S., *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*, Committee on Offensive Information Warfare, National Research Council, USA, 2009.

PORTER, Joshua. *Bokardo Social Web Design*[online]. 2008, říjen [cit. 1. 7. 2011]. Why Social Ads Don't Work. Dostupný na WWW: <http://bokardo.com/archives/why-social-ads-dont-work/>

POSNER, Gerald. *The Daily Beast* [online]. 13. ledna c2010, [cit. 1. 7. 2011]. China's Secret Cyberterrorism Dostupný na WWW: <http://www.thedailybeast.com/blogs-and-stories/2010-01-13/chinas-secret-cyber-terrorism/full/>.

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

Projekt OECD k padělatelství a pirátství. Ministerstvo průmyslu a obchodu, 2010 [cit. 1. 7. 2011]. Dostupné na WWW: <http://www.mpo.cz/dokument45250.html>.

Protection and Security of Networked Critical Infrastructures (SCNI). In: Euroepan Commission, JRC, Institute for the Protection and Security of the Citizen, [cit. 1. 7. 2011]. Dotupný na WWW: <http://ipsc.jrc.ec.europa.eu/showaction.php?id=22>.

President of Georgia (9.8. 2008): *Presidential Decree on Declaration of State of Warand Full Scale Mobilization,* [cit. 1. 7. 2011]. Dostupný na WWW: <http://www.president.gov.ge/?l=E&m=0&sm=1&st=70&id=2697>.

President of Georgia (8.8. 2008): Declaration of Universal Mobilization by Georgian President Mikheil Saakashvili. [cit. 1. 7. 2011]. Dostupný na WWW: <http://www.president.gov.ge/?l=E&m=0&sm=3&st=20&id=2689>.

President of Russia (8.8. 2008): *Beginning of the Meeting on the Conflict in South Ossetia with Defence Minister Anatoly Serdyukov and the Chief of General Staff of the Russian Armed Forces Nikolai Makarov,* [cit. 1. 7. 2011]. Dostupný na WWW: <http://www.kremlin.ru/eng/text/speeches/2008/08/09/1139_type82913_205050.shtml>.

QIAN Yi, Tipper David, Krishnamurthy Prashant, James Joshi, *Information Assurance: Dependability and Security in Networked Systems*, Morgan Kaufmann, USA, 2008.

RANNENBERG, Kai: *Recent Development in Information Technology Security Evaluation – The Need for Evaluation Criteria for multilateral Security.* In: Institut für Wirtschaftsinformatik, [cit. 1. 7. 2011]. Dostupný na WWW: <http://www.is-frankfurt.de/publikationenNeu/RecentDevelopmentinInformation.pdf >.

Regulation in the Information Society. In: European Commission, Europe's Information Society, [cit. 1. 7. 2011]. Dostupný na WWW: <http://ec.europa.eu/information_society/tl/policy/regulate/index_en.htm>.

Reuters (10.8. 2008): *Georgia offers ceasefire as fighting continues,* Dostupný na WWW: http://www.reuters.com/article/gc07/idUSL768040420080810); [cit. 1. 7. 2011]. Dostupný na WWW <http://www.uscc.gov/researchpapers/2009/NorthropGrumman_PRC_Cyber_Paper_FINAL_Approved%20Report_16Oct2009.pdf>.

ROTSCHILD, Michael: *The Threat from within: the evolution of cyber attacks*. Computer Technology Review, s. 256, c 2006.

ŘÍHA, Josef. *Urbanismus a územní rozvoj* [online]. 2007, roč. 10, č. 4, [cit. 1. 7. 2011]. Kritická infrastruktura a riziko mimořádné události Dostupný na WWW: <http://www.uur.cz/images/publikace/uur/2007/2007-04/08_kriticka.pdf>.

SHIMEAL, T. ; WILLIAMS, P. ; DUNLEVY, G. *Countering Cyber War* [online]. 2002 [cit. 1. 7. 2011]. Dostupný na WWW: <http://www.cert.org/archive/pdf/counter_cyberwar.pdf>.

SHOBBEN, Ann. *Information War and Cyberspace Security* [online]. 1995 [cit. 1. 7. 2011]. Dostupný na WWW: <http://www.rand.org/publications/randreview/issues/RRR.fall95.cyber/>.

SCHOU *Corey, Shoemaker Daniel, Information Assurance for the Enterprise: A Roadmap to Information Security, McGraw-Hill, USA, 2006.*

Siemens AG. SIMATIC WinCC/SIMATIC PCS 7: Information concerning Malware/Virus/Trojan. [cit. 1. 7. 2011]. Dostupný na WWW: <http://support.automation.siemens.com/WW/llisapi.dll?func=cslib.csinfo&objid=43876783>.

SMEJKAL, Vladimír. *Informační a počítačová kriminalita v České republice* [online]. [cit. 1. 7. 2011]. Dostupný na WWW: <http://www.mvcr.cz/casopisy/studie/diskuse/analyza.html>.

Směrnice 2002/58/ES o zpracování osobních údajů a ochrraně soukromí. Úřad pro ochranu osobních údajů**.** [online]. [cit. 1. 7. 2011]. Dostupný na WWW: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:CS:NOT>.

Symantec Global Internet Security Threat Report. Trends for 2008. In: Symantec, duben 2009, [cit. 1. 7. 2011]. Dostupný na WWW: <http://www.symantec.com/content/en/us/about/media/Symantec2009AnnualReport_Proxy_10-K.pdf>.

Symantec Global Internet Security Threat Report. Trends for 2008. In: Symantec, duben 2009, [cit. 1. 7. 2011]. Dostupný na WWW: <http://www.symantec.com/content/en/us/about/media/Symantec2009AnnualReport_Proxy_10-K.pdf>.

Symantec Global Internet Security Threat Report. Trends for 2008. In: Symantec, duben 2009, [cit. 1. 7. 2011]. Dostupný na WWW: <http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiv_04-2009.en-us.pdf>.

Symantec Global Internet Security Threat Report. Trends for 2008. In: Symantec, duben 2009, [cit. 1. 7. 2011]. Dostupný na WWW: <http://www.symantec.com/content/en/us/about/media/Symantec2009AnnualReport_Proxy_10-K.pdf >.

STEWART, James Michael. *CompTIA Security+Review Guide*. Indianopolis : Wiley Publishing, 2008. 288 s. ISBN 9780470404843

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

The e-government imperative: main findings. Organisation for Economic Cooperation and Development (OECD) [online], Policy Brief, březen 2003 [cit. 1. 7. 2011]. Dostupný na WWW: <http://www.oecd.org/dataoecd/60/60/2502539.pdf>.

The European Programme for Critical Infrastructure Protection. In: ProAdrias, [cit. 1. 7. 2011]. Dostupný na WWW: <http://www.proadrias.isig.it/Documenti/EPCIP%20memo.pdf >.

Tracking GhostNet: Investigating a Cyber Espionage Network. F-Secure [online]. [cit. 1. 7. 2011]. Dostupný na WWW: <http://www.f-secure.com/weblog/archives/ghostnet.pdf>.

Úmluva Rady Evropy o počítačové kriminalitě, Budapešť, 23. listopadu 2001, Convention on Cybercrime - ETS no. 185. [cit. 1. 7. 2011]. Dostupný na WWW: <http://conventions.coe.int/>.

U.S.-China Economic and Security Review Commission – "Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation" [cit. 1. 7. 2011]. Dostupný na WWW: <http://www.uscc.gov/researchpapers/2009/NorthropGrumman_PRC_Cyber_Paper_FINAL_Approved%20Report_16Oct2009.pdf>.

U.S. Department of Defense, *Annual Report on the Military Power of the People's Republic of China*, USA, 2008.

U.S.-China Economic and Security Review Commission – "Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation". U.S.-China Economic and Security Review Commission, *2007 Report to Congress*, USA, 2007.

U.S. Department of State, International Security Advisory Board Task Force, *Draft Report on China's Strategic Modernization*, September 2008, USA, 2008.

WINDLEY, Phillip. *Digital Identity*. Cambridge : O´Reilly Media, 2005. 254 s. ISBN 0596008783.

www.epp.eurostat.ec.europa.eu [online]. 7.3.2010 [cit. 1. 7. 2011]. Dostupný na WWW <http://epp.eurostat.ec.europa.eu/portal/page/portal/information_society/data/main_tables>.

www: *epp.eurostat.ec.europa.eu* [online]. 7.3.2010 [cit. 1. 7. 2011]. Dostupné na WWW: <http://epp.eurostat.ec.europa.eu/portal/page/portal/information_society/documents/Tab/What%20is%20where%20on%20Eurobase%20status%2008032011.pdf>.

Virtual Criminology Report – Cybercrime: The Next Wave. In: McAfee, Dostupný na WWW: <http://www.mcafee.com/us/research/criminology_report/default.html>.

VATIS, M. A. *Cyber Attacks During the War on Terrorism: A Predictive Analysis* [online]. 2001 [cit. 1. 7. 2011]. Dostupný z WWW: <http://www.ists.dartmouth.edu/ISTS/counterterrorism/cyber_a1.pdf>.

Virtual Criminology Report – Cybercrime: The Next Wave. McAfee [online]. [cit. 1. 7. 2011]. Dostupný na WWW: <https://secure.mcafee.com/it/resources/reports/rp-quarterly-threat-q1-2011.pdf >.

WALTERS, Conrad: Cyber cold war a threat to all. In *The Sydney Morning Herald*, 24. prosince 2007, [cit. 1. 7. 2011]. Dostupný na WWW: <http://www.smh.com.au/articles/2007/12/23/1198344874193.html>.

WEISMEN, Robyn. 2001. "Palestinian Hacktivism and Viruses Collide." *NewsFactor Network*, March 20. Washington DC: The George Washington University, 1997 [cit. 1. 7. 2011].

WATTS Sean, *Combatant Status and Computer Network Attacks*, in *Virginia Journal of International Law* 50.2, USA, 2010.

WILLET Keith D., *Information Assurance Architecture*, Auerbach Publications, USA, 2008. [cit. 1. 7. 2011]. Dostupný na WWW: <http://www.securedecisions.com/Members/admin/information-assurance-visualizations/2007-11-12.5465270995/image>.

Pojmový aparát

Vybrané pojmy z textu byly zpracovány na základě několika elektronických zdrojů, jejichž seznam je dostupný na konci pojmového aparátu v oddílu *použité zdroje*.

ARPANET (Advanced Research Projects Agency Network): Jedná se o předchozí verzi dnešní sítě Internet, která vznikla v USA. Historie sítě je počítána od roku 1969 do roku 1990.

Botnet: Síť počítačových programů, jejímž úkolem je vykonávání rutinních operací jako sběr dat, odesílání a zpracování požadavků. Lze ji použít jak pro účely kybernetického terorismu, tak i k opačným.

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

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

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

DoS útoky (Denial of Service): typ útoku na počítač nebo síť, který má způsobit nedostupnost dané služby, typicky síťového připojení. Obvykle se provádí tak, že je cílový systém zahlcen ohromným množstvím nesmyslných dotazů (Root).

DNS (Domain Name System): Domain Name System (nebo Service) je internetová služba zajišťující překlad doménových jmen (www.seznam.cz) na IP adresy (77.75.72.3) a obráceně (Root).

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

Chatroom: Místnost určená k vzájemné komunikaci internetových uživatelů, kteří jsou připojeni na stejném komunikačním kanálu případně na jedné internetové stránce, které poskytuje tyto služby. Jedná se o rychlejší podobu diskusního fóra.

IM: IM je zkratka slov Instant Messaging. IM je internetová služba, která umožňuje komunikaci mezi uživateli, kteří jsou připojeni na stejném komunikačním protokolu (SEO slovník).

IP (Internet Protocol): Datový protokol používaný pro přenos dat přes paketové sítě. Tvoří základní protokol dnešního Internetu. Každé zařízení komunikující prostřednictvím IP rozhraní má přiřazený jednoznačný identifikátor (IP adresu), který jej na Internetu odlišuje od jiných síťových zařízení. Každý poslaný paket zahrnuje IP adresu odesílatele a IP adresu příjemce (ADSL – slovníček pojmů).

IRC (Internet Relay Chat): je IM protokol umožňující komunikaci mezi více uživateli v chatroom. IRC byl jednou z prvních možností komunikace.

Mbps (Megabit per second): Jednotka přenosové rychlosti. Udává, kolik megabitů je přeneseno za jednu sekundu. 1 Megabit = 1 000 000 bitů.

P2P (peer-to-peer): označení architektury počítačových sítí, ve které spolu komunikují přímo jednotliví uživatelé. Dnes e označení Peer to peer vztahuje hlavně na výměnné sítě, prostřednictvím kterých si mnoho uživatelů může vyměňovat data (Saferinternet).

Paket: Jednotka přenosu dat, která je směrována technickým a programovým vybavením sítě ze zdroje do cíle určení (Adpnet).

PGP klíče (Pretty Good Privacy): certifikát, pomocí kterého je možné šifrovat a dešifrovat elektronické zprávy a ochránit tak její obsah před potencionálním zneužitím.

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

Phreaking: souhrnný termín pro vloupávání se do telefonních systému, převážně za účelem vedení bezplatných hovorů, odposlouchávání nebo narušování telefonních služeb

Pirátství: Nejčastěji vnímáno ve spojitosti s porušováním autorského práva. Jedná se o úmyslnou distribuci počítačových dat, které jsou chráněny autorským zákonem prostřednictvím např. P2P sítí.

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

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

TCP (Transmission Control Protocol): Nejpoužívanější přenosový protokol v IP sítích, poskytující spolehlivé přenosy s navazováním spojení. Použitím TCP mohou aplikace na sesíťovaných počítačích vytvořit mezi sebou spojení, přes které mohou přenášet data. Protokol garantuje spolehlivé doručování ve správném pořadí a rozlišuje data pro vícenásobné, současně běžící aplikace na stejném počítači (ADSL – slovníček pojmů).

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