Český model
amerického kongresu

Bezpečnost kybernetického prostoru

zpráva Výzkumné služby Kongresu

Jakub Klíma

US embassy

AmCham American Chamber of Commerce in the Czech Republic

ZÁPADOČESKÁ UNIVERZITA V PLZNI

KATEDRA POLITOLOGIE a MEZINÁRODNÍCH VZTAHŮ

PLZEŇSKÝ KRAJ

OBČANSKÝ INSTITUT

1. Úvod

Čím dál větší virtuální propojení a užívání kybernetického prostoru zvyšuje důležitost jeho zabezpečení. Ekonomická prosperita, národní bezpečnost i veškeré činnosti všedního dne závisí na stabilitě, bezpečnosti a odolnosti kybernetického prostoru. Ten by měla zajišťovat vláda svými službami. Tuto problematiku upravuje více než 50 jednotlivých federálních zákonů, přímo či nepřímo upravující jednotlivé aspekty, nicméně chybí zde zastřešující zákonný rámec, který by legislativu sjednotil. Navíc od roku 2002 nebyl přijat žádný významnější zákon v této oblasti. Proto je potřeba, aby se příští Kongres věnoval i tomuto problému a pokusil se přijmout potřebný legislativní akt.

2. Kybernetická bezpečnost

2.1 Představení problematiky

Kybernetický prostor je virtuální oblast, kde nastává prostřednictvím elektronických komunikací interakce informačních systémů, jednotlivých počítačů i počítačových sítí. V kybernetickém prostoru jsou zpracovávány a vyměňovány informace a ukládána, sdílena či přenášena data v elektronické podobě.[1] Kybernetický prostor čelí mnoha potenciálním hrozbám, které se s jeho růstem zvětšují. Souhrnně můžeme tyto hrozby označit pojmem *počítačová kriminalita*, což je jakýkoliv trestný čin zahrnující počítače a síť. Prováděna je kybernetickými útoky, které mají mnoho forem. Ty se odvíjí od cíle, kterých má útok dosáhnout, a také od velikosti útoku. Častým motivem je snaha o vyřazení stránek a serverů cíle či bránění v přístupu k informacím a jiným službám. Provádí se útoky DoS a DDoS[2], při nichž je informační kanál přehlcen požadavky a zkolabuje. Dalším cílem je únik informací – za jakýmkoliv účelem (krádež, neautorizované zveřejnění apod.). Setkat se můžeme i s útoky, které se snaží o narušení integrity, to znamená poškodit, změnit, či vymazat data napadeného subjektu. Počítačovou kriminalitu můžeme rozdělit i podle jiných kritérií – podvody a finanční kriminalita, vydírání, kybernetické válčení, krádeže informací či terorismus. Takových rozdělení můžeme najít mnoho, nicméně tohle nám pro účely tohoto backgroundu postačí, zájemci si mohou sami nastudovat více.

2.2 Nástroje na podporu bezpečnosti

Nástroje na podporu bezpečnosti jsou opatření, kterými se dá bránit proti kybernetickým útokům. Kyberobranu můžeme rozdělit na aktivní a pasivní. *„Aktivní kyberobranu je možné definovat jako přímou obrannou akci, která způsobí zneškodnění nebo snížení potenciálu*

[1] Kybernetický zákon, vysvětlení pojmů. Dostupný z: http://www.kybernetickyzakon.cz/
[2] Denial of Service a Distributed Denial of Service. Při DoS napadení je k útoku použit jeden počítač a jedno internetové připojení, zatímco při DDoS útoku je použito mnoho zařízení a připojení, proto je obrana proti tomuto typu útoku těžší.

útočníka." [3] Pasivní obrana je potom téměř cokoliv jiného, co snižuje účinnost útoku. Kyberobrana se dá dělit i jinými způsoby (např. interní a externí), nicméně my se zde budeme věnovat hlavně její nejvýznamnější části – prevenci, tedy opatřením, které mají co nejvíce znesnadnit primární proniknutí do sítě. Nejčastějšími nástroji jsou autentizace osob, kryptografie, monitorovací systémy a mnoho dalších nástrojů a prostředků. Autentizace osob je základním ochranným prvkem, který používá naprostá většina uživatelů komunikačních technologií. Jde o tzv. ověření identity, tedy hesla a piny, využití biometrických údajů (otisky prstů, vzor sítnice apod.) či různé tokeny, což jsou např. magnetické a čipové karty. Kryptografie se zabývá šifrováním komunikace, používá se proto pro zajištění důvěrnosti, integrity a autenticity dat. Z ostatních nástrojů bych ještě zmínil například antivirové softwary, firewall či třeba jen aktualizace softwaru.[4]

2.3 Kybernetická bezpečnost ve Výboru pro národní bezpečnost

Kybernetická kriminalita je obrovský pojem, zahrnující aktivity s velkou spoustou cílů – od menších útoků až po samotnou teroristickou činnost. Účelem navrhovaného zákona bude však hlavně bezpečnost Spojených států amerických, a proto budeme řešit převážně útoky ohrožující stabilitu země, útoky s větším finančním dopadem (jak na soukromé podniky, tak na stát) či útoky zaměřující se na krádeže citlivých a tajných informací. Abychom těmto hrozbám lépe porozuměli, je třeba si ještě představit jednotlivé agresory, proti kterým bude navrhovaný zákon bojovat. [5]

Kybernetičtí teroristé (Cyberterrorists) se podílí na útocích formou terorismu. Nejčastěji používají internet k plánování útoků, rekrutování a propagandě či jako prostředek ke komunikaci. Tato skupina může být sponzorovaná jak národními vládami, tak i soukromými subjekty.

Kybernetičtí špioni (Cyberspies) jsou jednotlivci, kteří většinou kradou utajené či cenné informace vládě a soukromým podnikům s cílem získat bezpečnostní, strategickou, finanční nebo politickou výhodu. Nejčastěji pracují pro cizí vlády a jejich rozvědky s cílem získat tyto výhody.

Kybernetičtí zloději (Cyberthieves) jsou jednotlivci, kteří provádí ilegální kybernetické útoky z peněžních důvodů. Jde často o útoky s cílem získat přístupy k bankovním účtům, kreditním kartám a podobně citlivým informacím s cílem je použít či prodat.

---

[3] BALÁŽIK, Milan. Reakce a obrana proti kybernetickým útokům v prostředí SCADA. In: *System OnLine* [online]. [cit. 2015-03-16]. Dostupné z: http://www.systemonline.cz/rizeni-vyroby/reakce-a-obrana-proti-kybernetickym-utokum-v-prostredi-scada.htm

[4] STODOLA, Petr. Kybernetická a informační válka: Ochrana a obrana proti kybernetickým útokům. In: [online]. [cit. 2015-03-16]. Dostupné z: https://moodle.unob.cz/pluginfile.php/20733/mod_resource/content/2/KIV%20T-9.pdf

[5] Issues in Homeland Security Policy for the 113th Congress. [online]. s. 11, 09-23-2013 [cit. 2015-03-16]. Dostupné z: http://fas.org/sgp/crs/homesec/R42985.pdf

Kybernetičtí válečníci (Cyberwarriors) jsou agenti či kvazi-agenti jednotlivých států, kteří podnikají akce, ať už jménem daného státu, či tajně, na podporu strategických cílů dané země. Když napadená země zjistí, odkud byl útok proveden, často se pak vláda agresora zříká zodpovědnosti a tvrdí, že útočníci jednali sami na vlastní pěst.

Kybernetičtí aktivisté (Cyberactivists) jsou jednotlivci, kteří neprovádí útoky pro peníze, ale pro radost či nějaké politické, filozofické a jiné přesvědčení. Často je pro ně útok pouze osobní výzvou a jejich cíl může být jakýkoliv. Nejznámějším příkladem je určitě skupina Anonymous, jejichž útoky jsou často z nějakého přesvědčení, či pouze pro radost.

3. Stávající zákonná úprava

Jak jsem již zmínil v úvodu, problematiku kybernetické bezpečnosti upravuje přes 50 federální zákonů. Většina z nich byla v posledních letech dokonce revidována, nicméně žádný větší zákon o kybernetické bezpečnosti v poslední době přijat nebyl, což je potřeba v tak rychle se vyvíjejícím odvětví změnit. V roce 2009 Obamova administrativa zřídila post koordinátora kybernetické bezpečnosti pro Bílý dům. V roce 2012 pak Obama podle The Washington Post podepsal pokyn, který umožňuje armádě reagovat agresivněji proti hrozbám kybernetického útoku na národní web vlády a soukromé počítačové sítě.[6]

Při současné zákonné úpravě mají všechny federální agentury své aktivity v oblasti kybernetické bezpečnosti v rámci vlastních systémů. Některé další agentury je mají přímo svěřené ze zákona. Nicméně často se jejich činnosti překrývají či si konkurují, proto je třeba tyto agentury usměrnit a poskytnout jim zákonný rámec, aby mohly zajišťovat větší bezpečnost pro národ.[7] Navíc zodpovědnost za kybernetickou bezpečnost je rozdělena mezi několik institucí – NSA, ministerstvo vnitřní bezpečnosti (Department of Homeland Security), FBI a americké velitelství kybernetické obrany (U. S. Cyber Command). Prezident Obama se nechal na začátku roku 2015 slyšet, že chce zřídit novou agenturou, která by analyzovala a posuzovala jednotlivé hrozby. Podle Bílého domu tady taková instituce ještě není, tudíž by nově vzniklé *Zpravodajské centrum pro kybernetické hrozby* (Cyber Threat Intelligence Integration Center) mělo tuto díru vyplnit.[8]

Obama si je vědom i jednoho z nejpalčivějších problémů kyberbezpečnostních návrhů – přístup a zasahování do soukromých údajů a informací. Toto se snaží řešit i jeden z bodů nařízení Bílého domu z února 2013, ve kterém stojí, že všechny agentury mají koordinovat

[6] NAKASHIMA, Ellen. National Security: Obama signs secret directive to help thwart cyberattacks. In: *The Washington Post* [online]. 11-14-2012 [cit. 2015-03-16]. Dostupné z: http://www.washingtonpost.com/world/national-security/obama-signs-secret-cybersecurity-directive-allowing-more-aggressive-military-role/2012/11/14/7bf51512-2cde-11e2-9ac2-1c61452669c3_story.html

[7] Issues in Homeland Security Policy for the 113th Congress. [online]. s. 13, 09-23-2013 [cit. 2015-03-16]. Dostupné z: http://fas.org/sgp/crs/homesec/R42985.pdf

[8] STROBEL, Warren. U.S. To Create New Cybersecurity Agency: Official. In: *Huffington Post* [online]. 02-10-2015 [cit. 2015-03-16]. Dostupné z: http://www.huffingtonpost.com/2015/02/10/us-cybersecurity-agency_n_6651688.html

své aktivity s agenturami pro ochranu soukromí a občanských svobod a mají tato bezpečnostní opatření zahrnout do svých aktivit.[9]

4. CISPA a CISA

4.1 Současná situace

CISPA (Cyber Intelligence Sharing and Protection Act) je návrh zákona, který dovoluje sdílet internetová data mezi vládou a technologickými a výrobními společnostmi. Cílem návrhu je zabránit hrozbám kybernetických útoků a zajistit bezpečnost sítě. Návrh zákona byl představen v roce 2011 ve Sněmovně reprezentantů, kde i prošel, nicméně Senát jej odmítl a i Bílý dům pohrozil vetem z důvodu ohrožení občanských svobod a důvěrnosti.[10] Návrh zákona byl přepracován a znovu představen ve Sněmovně v únoru 2013, kde opět prošel. V Senátu se však zastavil a nebylo o něm hlasováno, jelikož senátoři řekli, že místo opětovného hlasování raději napíší jejich vlastní verzi zákona o kybernetické bezpečnosti.[11] V lednu 2015 se zatím naposledy opět mírně přepracovaný návrh zákona představil ve Sněmovně, ale zatím o něm hlasováno nebylo.

V Senátu byl mezitím v létě 2014 představen návrh zákona CISA (Cybersecurity Information Sharing Act), který je již zmíněnou senátní verzí návrhu CISPA. O tom ale zatím nijak hlasováno nebylo. Je však otázkou, jak moc se tyto dva návrhy od sebe liší. Mnoho odpůrců tvrdí, že jsou oba de facto stejné a oba by měly být zamítnuty. Mnoho expertů však varuje, že Kongres musí přijmout zákon o kybernetické bezpečnosti, jelikož jsou americké počítačové systémy čím dál více zranitelné před kybernetickými útoky.[12]

4.2 Pro a proti

Základem obou legislativ je víceméně to stejné – sdílení kybernetických hrozeb mezi vládou a soukromými společnostmi (i mezi společnostmi navzájem). V praxi to znamená, že komunikace mezi vládou a společnostmi je mnohem volnější. V backgroundu k zákonu CISPA jeho tvůrci uvádějí, že sdílení těchto hrozeb pomůže společnostem navzájem i vládě rychleji a efektivněji reagovat na kybernetické útoky. Například když hacker napadne nějakou společnost a ta tyto údaje sdílí s ostatními, další společnosti mají mnohem větší šanci se

[9] The White House, Office of the Press Secretary. Executive Order -- Improving Critical Infrastructure Cybersecurity. In: [online]. 02-12-2013 [cit. 2015-03-16]. Dostupné z: https://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

[10] BBC News US & CANADA: Cyber-security bill Cispa passes US House. In: *BBC* [online]. 04-27-2012 [cit. 2015-03-16]. Dostupné z: http://www.bbc.com/news/world-us-canada-17864539

[11] SMITH, Gerry. Senate Won't Vote On CISPA, Deals Blow To Controversial Cyber Bill. In: *Huffington Post* [online]. 04-25-2013 [cit. 2015-03-16]. Dostupné z: http://www.huffingtonpost.com/2013/04/25/cispa-cyber-bill_n_3158221.html

[12] SMITH, Gerry. Senate Won't Vote On CISPA, Deals Blow To Controversial Cyber Bill. In: *Huffington Post* [online]. 04-25-2013 [cit. 2015-03-16]. Dostupné z: http://www.huffingtonpost.com/2013/04/25/cispa-cyber-bill_n_3158221.html

dalším potenciálním útokům ubránit. Tvůrci také uvádějí, že poskytování informací je čistě dobrovolné a nesmí být žádným způsobem zneužito. Vláda může informace použít pouze pro obranu proti kybernetickým útokům. Zdůrazňují také to, že zákon nepotřebuje žádné další federální výdaje, neprohlubuje výrazně byrokracii a nezavádí žádné nové regulace, na rozdíl od většiny jiných zákonů. V backgroundu tvůrci argumentují právě i obecně kybernetickými hrozbami. Představují prý obrovské nebezpečí a zdůrazňují potřebu spolupráce mezi vládou a jednotlivými společnostmi proto, že americké podniky jsou často terčem právě národních agresorů, převážně Ruska a Číny, jejichž podniky pak získávají nespravedlivou výhodu na trhu.[13]

Za zákony stojí také více než 800 společností, v čele s předními internetovými giganty jako je Facebook, Intel či Microsoft a americké asociace sdružující softwarové a technologické podniky. Viceprezident Facebooku vydal prohlášení, ve kterém se staví na obranu CISPA s tím, že čím rychleji budou moci podniky a vláda mezi sebou sdílet kybernetické hrozby, tím rychleji a lépe se pak mohou bránit. Navíc když jedna společnost čelí útoku a sdílí tyto informace, ostatní společnosti mohou tomu samému útoku předejít.[14] Ostatní asociace se přidávají s podobnými tvrzeními.

Zákony mají však i spoustu odpůrců. Jde často o organizace hájící lidská práva, základní svobody apod. Nejvýraznějšími jsou neziskové organizace American Civil Liberties Union (ACLU) či Electronic Frontier Foundation (EFF). EFF se zabývá lidskými právy v digitálním světě a vadí jí třeba, že jazyk, kterým jsou zákony psány, je příliš vágní a široký, dá se proto snadno zneužívat. Společnosti by tak mohly zákon používat k monitorování elektronických konverzací, blokování přístupu k internetovým stránkám apod.[15] Podle ACLU zase zákony dostatečně nevymezují a nelimitují, o jaký typ informací při sdílení půjde, a chtějí tudíž upozornit obyvatelstvo, že se Kongres chystá dát vládě obrovskou vlnu nových pravomocí ke sbírání osobních internetových dat a informací.[16]

4.3 Podpora napříč stranami

CISPA má ve sněmovně podporu relativně napříč politickými stranami. Předkladateli jsou dva politici – jeden za republikánskou a jeden za demokratickou stranu. Pozice republikánů je poměrně jasná. Až na libertariánské křídlo, které je velkým a hlasitým odpůrcem návrhů, je republikánská strana vesměs jednotná a snaží se zákon prosadit. U demokratů je to

[13] Backgrounder on the Rogers-Ruppersberger Cybersecurity Bill. In: *U.S. House of Representatives: Permanent Select Committee on Intelligence* [online]. [cit. 2015-03-16]. Dostupné z: http://intelligence.house.gov/backgrounder-rogers-ruppersberger-cybersecurity-bill
[14] TSUKAYAMA, Hayley. Technology: CISPA: Who's for it, who's against it and how it could affect you. In: *The Washington Post* [online]. 04-27-2012 [cit. 2015-03-16]. Dostupné z: http://www.washingtonpost.com/business/technology/cispa-whos-for-it-whos-against-it-and-how-it-could-affect-you/2012/04/27/gIQA5ur0lT_story.html
[15] NEWMAN, Jared. Security: CISPA Monitoring Bill: Just the Facts. In: *TechHive* [online]. 04-13-2012 [cit. 2015-03-16]. Dostupné z: http://www.techhive.com/article/253800/cispa_just_the_facts.html?null
[16] tamtéž

složitější, během prvního hlasování byla pro pouze necelá třetina demokratických poslanců, při druhém hlasování to však byla již téměř polovina. Nyní se poslanci snaží o úpravu návrhu, aby byl přijatelnější. Snaha je například v zúžení definic a nastavení jasných pravidel pro sdílení informací, nicméně kritici jsou skeptičtí. Klíčový proto bude senátní návrh – ve sněmovně je podpora již velká, ovšem nadále hrozí veto prezidenta, který nechce ohrozit soukromí amerických občanů.

5.SOPA

Stop Online Piracy Act (SOPA) byl americký zákon navrhnutý v roce 2011, který měl bránit duševní práva a omezit počítačové pirátství. Zákon podporovaly společnosti a organizace zabývající ochranou duševního vlastnictví či instituce spojené s tímto tématem, včetně předních amerických televizí. Problém je, že by tento zákon zvýšil pravomoci amerických institucí a mimo jiné by umožňoval na základně rozhodnutí federálního soudu zakročení proti každému webu, který by byl nějakým způsobem podezřelý a uchovával by obsah porušující autorská práva. Proto se vůči tomuto návrhu zvedla vlna kritiky a zákon si našel opravdu mnoho odpůrců. A právě kvůli rozepřím v Kongresu byl tento zákon odložen s tím, že se o něm nebude hlasovat do doby, než se najde konsenzus.[17] Mnoho odpůrců zákonu CISPA se jej právě snaží připodobnit k zákonu SOPA a tvrdí, že je to víceméně to stejné, že oba zákony hrubě porušují základní lidské svobody nebo svobodu projevu a že by měly být oba staženy.

6. Nedávný vývoj

Jedním z důvodů, proč je téma kybernetické bezpečnosti v poslední době tolik populární a proč jej i prezident Obama zařadil mezi své nejvyšší priority, je i třeba kybernetický útok na společnost Sony Pictures a následná krádež citlivých dat. Tento útok se odehrál v listopadu roku 2014. Spojené státy tehdy obvinily z útoku Severní Koreu, která měla skrze útok společnost Sony vydírat, aby nepustila do kin svůj nový film *The Interview*, který si dělá legraci z vůdce Severní Korei, Kim Čong-Una. Tato nařčení se však nepotvrdila, nicméně hackerský útok se stal a opět rozvířil debaty ohledně kybernetické bezpečnosti a potřeby její koordinace.

Nicméně argumenty se objevují i na druhé straně. Podle dokumentů, které zveřejnil Edward Snowden,[18] měla v roce 2010 americká NSA spolu s britskou GCHQ (britská zpravodajská agentura) napadnout největšího výrobce SIM karet, společnost Gemalto. Firma přiznala, že se pravděpodobně stala terčem útoku, nicméně krádež bezpečnostních klíčů k dešifrování

[17] WORTHAM, Jenna a Somini SENGUPTA. Technology: Bills to Stop Web Piracy Invite a Protracted Battle. In: *The New York Times* [online]. 01-15-2012 [cit. 2015-03-16]. Dostupné z: http://www.nytimes.com/2012/01/16/technology/web-piracy-bills-invite-a-protracted-battle.html?_r=0

[18] Bývalý pracovník amerických tajných služeb, který vynesl do tisku přísně tajné informace.

komunikace nepotvrdila.[19] Tato událost hraje do karet všem oponentům amerických tajných složek, kteří tvrdí, že NSA a jí podobné instituce zneužívají své postavení a porušují základní lidská práva a svobody.

7. Závěr

Kybernetická bezpečnost se stává čím dál důležitějším aspektem národní bezpečnosti. S rychlým rozvojem IT sektoru roste i nebezpečí kybernetických útoků, které mohou narušit integritu i chod celé země. Proto je toto téma pro Výbor pro národní bezpečnost prioritní. Kybernetické útoky jsou vedeny za účelem získání citlivých informací, porušení jejich integrity, nebo vyřazení služeb z činnosti. Jejich nejčastějšími formami jsou neautorizovaný přístup do systému (za účelem získání citlivých informací), implementace škodlivého softwaru (virů apod.) nebo útoky na potlačení služeb systému (Dos a DDoS útoky). O sjednocení legislativy se nejprve snažil zákon CISPA, který však doposud nebyl přijat. Senátní verze CISA se zatím vytváří, nicméně kritici považují oba zákony za obrovský zásah do lidských svobod a soukromí. Sdílení informací prý dává federální vládě obrovské pravomoci, které může jednoduše zneužít. I když je podpora návrhů mezi politiky velká, bude potřeba ještě mnoho práce a úprav, aby byl výsledný dokument opravdu kvalitní a přijatelný všemi stranami.

[19] VALÁŠEK, Michal. Tech: NSA napadla výrobce SIM karet, bezpečnost SIM masivně neohrozila. In: *Hospodářské noviny* [online]. 02-26-2015 [cit. 2015-03-16]. Dostupné z: http://tech.ihned.cz/c1-63594580-bezpecnostni-svodka-nsa-napadla-vyrobce-sim-lenoco-superfish

8. Zdroje

8.1 Webové stránky

Committee on Homeland Security, http://homeland.house.gov/issue/cybersecurity

Department of Homeland Security, http://www.dhs.gov/topic/cybersecurity

The White House Foreign Policy, Cybersecurity, https://www.whitehouse.gov/issues/foreign-policy/cybersecurity

U. S. House of Representatives: Permanent Select Committee on Intelligence, http://intelligence.house.gov/cispa

GamePolitics, Cybersecurity, http://www.gamepolitics.com/category/topics/cyber-intelligence-sharing-and-protection-act

Kybernetický zákon, http://www.kybernetickyzakon.cz/

Cispa is back, http://www.cispaisback.org/

Cyber Security Legislation. In: *Electronic Frontier Foundation* [online]. [cit. 2015-03-16]. Dostupné z: https://www.eff.org/issues/cyber-security-legislation

8.2 Dokumenty

H.R.624. Cyber Intelligence Sharing and Protection Act. Dostupné z: http://www.lawfareblog.com/wp-content/uploads/2013/05/BILLS-113hr624eh-as-passed-4-2013.pdf

Issues in Homeland Security Policy for the 113th Congress. [online]. s. 79, 09-23-2013 [cit. 2015-03-16]. Dostupné z: http://fas.org/sgp/crs/homesec/R42985.pdf

KOLOUCH, Jan. Kybernetické útoky. In: [online]. [cit. 2015-03-16]. Dostupné z: https://csirt.cesnet.cz/Dokumenty?action=AttachFile&do=get&target=Kyberneticke+utoky.pdf

STODOLA, Petr. Kybernetická a informační válka: Ochrana a obrana proti kybernetickým útokům. In: [online]. [cit. 2015-03-16]. Dostupné z: https://moodle.unob.cz/pluginfile.php/20733/mod_resource/content/2/KIV%20T-9.pdf

8.3 Ostatní

ROSENZWEIG, Paul. HARD NATIONAL SECURITY CHOICES: CISPA – An Assessment. In: *Lawfare* [online]. 05-07-2013 [cit. 2015-03-16]. Dostupné z: http://www.lawfareblog.com/2013/05/cispa-an-assessment/

SCHWARZ, Mathew. Cybersecurity: CISPA Cybersecurity Bill, Reborn: 6 Key Facts. In: *InternationWeek Government* [online]. 02-14-2013 [cit. 2015-03-16]. Dostupné z: http://www.informationweek.com/government/cybersecurity/cispa-cybersecurity-bill-reborn-6-key-facts/d/d-id/1108675?

BALÁŽIK, Milan. Reakce a obrana proti kybernetickým útokům v prostředí SCADA. In: *System OnLine* [online]. [cit. 2015-03-16]. Dostupné z: http://www.systemonline.cz/rizeni-vyroby/reakce-a-obrana-proti-kybernetickym-utokum-v-prostredi-scada.htm

NAKASHIMA, Ellen. National Security: Obama signs secret directive to help thwart cyberattacks. In: *The Washington Post* [online]. 11-14-2012 [cit. 2015-03-16]. Dostupné z: http://www.washingtonpost.com/world/national-security/obama-signs-secret-cybersecurity-directive-allowing-more-aggressive-military-role/2012/11/14/7bf51512-2cde-11e2-9ac2-1c61452669c3_story.html

STROBEL, Warren. U.S. To Create New Cybersecurity Agency: Official. In: *Huffington Post* [online]. 02-10-2015 [cit. 2015-03-16]. Dostupné z: http://www.huffingtonpost.com/2015/02/10/us-cybersecurity-agency_n_6651688.html

BBC News US & CANADA: Cyber-security bill Cispa passes US House. In: BBC [online]. 04-27-2012 [cit. 2015-03-16]. Dostupné z: http://www.bbc.com/news/world-us-canada-17864539

SMITH, Gerry. Senate Won't Vote On CISPA, Deals Blow To Controversial Cyber Bill. In: Huffington Post [online]. 04-25-2013 [cit. 2015-03-16]. Dostupné z: http://www.huffingtonpost.com/2013/04/25/cispa-cyber-bill_n_3158221.html

TSUKAYAMA, Hayley. Technology: CISPA: Who's for it, who's against it and how it could affect you. In: *The Washington Post* [online]. 04-27-2012 [cit. 2015-03-16]. Dostupné z: http://www.washingtonpost.com/business/technology/cispa-whos-for-it-whos-against-it-and-how-it-could-affect-you/2012/04/27/gIQA5ur0lT_story.html

NEWMAN, Jared. Security: CISPA Monitoring Bill: Just the Facts. In: *TechHive* [online]. 04-13-2012 [cit. 2015-03-16]. Dostupné z: http://www.techhive.com/article/253800/cispa_just_the_facts.html?null

WORTHAM, Jenna a Somini SENGUPTA. Technology: Bills to Stop Web Piracy Invite a Protracted Battle. In: *The New York Times* [online]. 01-15-2012 [cit. 2015-03-16]. Dostupné z: http://www.nytimes.com/2012/01/16/technology/web-piracy-bills-invite-a-protracted-battle.html?_r=0

Denial of Service Attacks. In: [online]. [cit. 2015-03-16]. Dostupné z: http://www.incapsula.com/ddos/ddos-attacks/denial-of-service.html

VALÁŠEK, Michal. Tech: NSA napadla výrobce SIM karet, bezpečnost SIM masivně neohrozila. In: *Hospodářské noviny* [online]. 02-26-2015 [cit. 2015-03-16]. Dostupné z:

http://tech.ihned.cz/c1-63594580-bezpecnostni-svodka-nsa-napadla-vyrobce-sim-lenoco-superfish

LITTLE, Morgan. CISPA legislation seen by many as SOPA 2.0. In: *Los Angeles Times* [online]. 04-02-2012 [cit. 2015-03-16]. Dostupné z: http://articles.latimes.com/2012/apr/09/news/la-pn-cispa-legislation-seen-by-many-as-sopa-20-20120409

MCNEAL, Gregory. Controversial Cybersecurity Bill Known As CISA Advances Out Of Senate Committee. In: *Forbes* [online]. 07-09-2014 [cit. 2015-03-16]. Dostupné z: http://www.forbes.com/sites/gregorymcneal/2014/07/09/controversial-cybersecurity-bill-known-as-cisa-advances-out-of-senate-committee/

Cloud Monitoring: Controversial cybersecurity bill CISA advances in the Senate. In: *Copperegg* [online]. 07-14-2014 [cit. 2015-03-16]. Dostupné z: http://copperegg.com/controversial-cybersecurity-bill-cisa-advances-in-the-senate/

Senate committee passes CISA cybersecurity bill that could broaden NSA powers. In: *RT* [online]. 08-08-2014 [cit. 2015-03-16]. Dostupné z: http://rt.com/usa/171368-senate-committee-adopts-cybersecuirty-bill/

US House of Representatives passes CISPA cybersecurity bill. In: *RT* [online]. 04-20-2013 [cit. 2015-03-16]. Dostupné z: http://rt.com/usa/congress-house-bill-cispa-031/