3. PRÍPADY ZNEUŽITIA KYBERNETICKÉHO PRIESTORU

Čoraz častejšie sme svedkami udalostí, počas ktorých sa kybernetický priestor stáva dejiskom negatívnych operácií zameraných aj voči štátom. Ani zďaleka však nejde o prvé a žiaľ zrejme ani o posledné takéto aktivity. Obavy spájané s kybernetickým priestorom a kybernetickou bezpečnosťou sú totiž staré ako internet sám. Uviesť možno napríklad rok 1998 a útoky 3000 čínskych hackerov na indonézske vládne stránky. Známe sú tiež desiatky tisíce pokusov o preniknutie do počítačových sietí spadajúcich pod ministerstvá obrany, banky, médiá a pod.[362] a ich počet neustále rastie.[363]

V ďalšom texte približujeme azda najznámejšie prípady zneužitia kybernetického priestoru, ktoré spolu s konfliktom na Ukrajine poskytujú reálny obraz o sile a možnostiach tohto typu priestoru. Všetky uvedené prípady potvrdzujú, že kybernetická bezpečnosť je neoddeliteľnou súčasťou národnej bezpečnosti.

3.1 Estónsko (2007)

Ako prvý možno spomenúť prípad z apríla 2007, keď Estónsko čelilo asi tri týždne trvajúcim DDoS útokom, ktoré predstavujú tzv. distribuované odmietnutie služby. Estónsko je pritom krajina s mimoriadne rozvinutými internetovými službami, často označovaná ako jeden z národov najviac závislých od internetu na svete. Táto malá krajina s počtom približne 1,3 milióna obyvateľov sa považuje za jednu z najviac technicky prepojených oblastí planéty. Takmer všetko v tomto štáte v ktorom sa zrodil Skype, sa deje cez počítačové siete a mobilné zariadenia.[364]

Estónci využívajú internet a internetové služby pre množstvo činností v rámci svojho každodenného života. Prostredníctvom internetu spravujú svoje osobné bankovníctvo a môžu, dokonca, voliť v národných voľbách online. Pre vládu je totiž zavádzanie technológií vysokou prioritou. Aj preto sa dostalo Estónsko z postkomunistickej ekonomiky na úroveň priekopníka v zavádzaní týchto

[362] O'CONNELL, M., E. ARIMATSU, L., WILMSHURST, E.: Cyber Security and International Law ... cit. dielo, s. 3.

[363] Z posledných kybernetických operácií takéhoto typu možno spomenúť tie z októbra 2018, zamerané na siete Ministerstva zahraničných vecí a európskych záležitostí Slovenskej republiky.

[364] Bližšie pozri: LAASME, H.: Estonia: Cyber Window into the Future of NATO. In: Журнальный клуб Интелрос; Joint Force Quarterly, 2011, č. 63; dostupné na: http://www.intelros.ru/readroom/jfq/jfq-63-october-2011/11378-estonia-cyber-window-into-the-future-of-nato.html (navštívené dňa 10. 8. 2018).

technológií.[365] V číselnom vyjadrení asi 40 % populácie číta denníky online, viac ako 90 % bankových transakcií sa realizuje cez internet. Krajina je pretkaná bezplatnou wi-fi, mobilné telefóny môžu byť použité na zaplatenie za parkovanie alebo obed a Skype preberá medzinárodné telefónne služby zo svojho ústredia na okraji mesta Tallinn. Podľa mnohých je Estónsko oknom do budúcnosti s tým, že raz bude aj zvyšok sveta rovnako prepojený ako tento malý pobaltský národ.[366] Toto masívne spoliehanie sa na internet pri každodenných činnostiach, dokonca, viedlo niektorých k tomu, aby Estónsko označovali ako „E-stónsko".[367]

Podnetom k vykonaniu DDoS útokov malo byť rozhodnutie estónskych úradov premiestniť sovietsky vojnový pamätník z centra hlavného mesta Tallinn na vojenský cintorín. Tento čin vyvolal nepokoje ruskej menšiny, ktorej príslušníci vnímali tento pamätník ako pamiatku na vojnové obete a viedlo to až k blokáde estónskeho veľvyslanectva v Moskve. Na druhej strane Estónci vnímajú tento pamätník ako symbol cudzej okupácie.[368] Sovieti postavili tento pamätník v roku 1947, aby si pripomenuli svoje vojnové obete, po vyhnaní nacistov z tohto regiónu na konci druhej svetovej vojny. Keď sa však krajina zbavila nemeckej okupácie, Rusi sa rozhodli usadiť sa. Následne si tu Sovietska tajná polícia zriadila pracovisko a čoskoro boli masy Estóncov deportované na Sibír. Z toho dôvodu bola táto socha pre mnohých občanov symbolom ich ťažkej okupácie. A tak, po šestnástich rokoch nezávislosti, nabrali Estónci odvahu ignorovať protesty ruskej vlády (ktorá zlovestne varovala, že odstránenie sochy by malo „neblahé" následky) a sochu odstránili. O tri dni neskôr bola umiestnená na vojenskom cintoríne na predmestí. Ešte pred samotným odstránením vypuklo násilie v uliciach Tallinnu. Demonštranti rozbili výklady, prevrátili autá a vrhali kamene na policajné jednotky. Väčšinu z nich tvorili etnickí Rusi, ktorí predstavujú asi štvrtinu obyvateľstva. Tieto však rýchlo utíchli, stovky ľudí bolo zatknutých a škody napravené.[369] V skutočnosti sa však nepokoje premiestnili do inej sféry – do kybernetického priestoru.

---

[365] Bližšie pozri: MEAGHER, S.: When Personal Computers are Transformed into Ballot Boxes: How Internet Elections in Estonia Comply with the United Nations International Covenant on Civil and Political Rights. In: American University International Law Review, 2009, Vol. 23, issue 2, s. 355 – 356; dostupné na: https://digitalcommons.wcl.american.edu/cgi/viewcontent.cgi?referer=https://www.google.sk/&httpsredir=1&article=1023&context=auilr (navštívené dňa 10. 8. 2018).

[366] DAVIS, J.: Hackers Take Down the Most Wired Country in Europe. In: Wired Mag., 2007; dostupné na: https://www.wired.com/2007/08/ff-estonia/ (navštívené dňa 12. 8. 2018).

[367] Bližšie pozri: BASU, I.: Estonia Becomes E-stonia. In: Government Technology, April 9, 2008, dostupné na: http://www.govtech.com/e-government/Estonia-Becomes-E-stonia.html?topic=117673 (navštívené dňa 10. 8. 2018).

[368] The Economist: A Cyber-riot. May 10th 2007, dostupné na: http://www.economist.com/node/9163598, (navštívené dňa 1. 10. 2015).

[369] DAVIS, J.: Hackers Take Down the Most Wired Country in Europe ... cit. dielo, dostupné na: https://www.wired.com/2007/08/ff-estonia/.

Namietala aj ruská vláda, ktorá to považovala za urážku a marginalizovanie ruského historického dedičstva v Estónsku, pričom nazvala tento čin za „rúhavý".[370] Následne nastali DDoS útoky. Bežný človek si to mohol všimnúť tak, že viaceré internetové stránky boli zrazu nedostupné a nedostal sa tak ani k online denníkom. To bol aj prípad estónskeho ministra obrany. Až následne sa k nemu dostala správa, že niekto narúša a napáda desiatky cieľov po celej krajine. Nešlo len o noviny, ale aj najvýznamnejšiu banku a postupne zlyhávali aj vládne komunikačné prostriedky. Nebol však vyhlásený žiadny poplach, hraničná stráž neoznamovala žiadne zásahy a ani estónsky vzdušný priestor nebol narušený. Išlo totiž o operácie v kybernetickom priestore.

Kybernetické operácie boli zamerané na základnú elektronickú infraštruktúru Estónska. Aj telekomunikačné spoločnosti a médiá pocítili ich dopad a ovplyvnilo to väčšinu obyvateľov.[371] Internetové stránky najvýznamnejších bánk v Estónsku, novín a hlavných vládnych agentúr sa zrútili, čím sa národ presunul do izolácie v kybernetickom priestore. Celkovo DDoS útoky ochromili najkritickejšie estónske webové stránky a boli zamerané najmä na webové stránky prezidenta, parlamentu, ministerstiev a politických strán, hlavných spravodajských oddelení a dvoch hlavných bánk v Estónsku.[372]

Viaceré z napadnutých internetových stránok boli nahradené stránkami s ruskou propagandou alebo falošným ospravedlnením, no väčšina útokov bola zameraná na ich vypnutie. Hovorca estónskeho Ministerstva obrany prirovnal tieto útoky, dokonca, k tým proti Spojeným štátom americkým z 11. septembra 2001.[373]

DDoS útoky fungovali na základe preťaženia estónskych webových stránok s toľkými požiadavkami na informácie, že servery doviedli až do úplného vypnutia. Podľa estónskeho ministra obrany zažívali stránky, ktoré sú zvyčajne navštívené približne 1000 krát za deň, pod kybernetickým „bombardovaním" takmer 2 000 návštev a žiadostí za sekundu. Samotný DDoS útok bol v skutočnosti kombináciou niekoľkých súčasne sa vyskytujúcich DDoS útokov, pričom v čase útoku bolo takmer 130 identifikovateľne odlišných DDoS útokov zameraných a narušujúcich estónske internetové infraštruktúry.

Internetový prenos počas útoku dramaticky vzrástol a množstvo skutočných dát prenášaných na estónskych serveroch sa v priebehu útokov DDoS zvýšilo

[370] Bližšie pozri: RABOIN, B.: Corresponding Evolution: International Law and the Emergence of Cyber Warfare. In: Journal of the National Association of Administrative Law Judiciary, 2011, Volume 31, Issue 2, s. 617; dostupné na: http://digitalcommons.pepperdine.edu/naalj/vol31/iss2/5 (navštívené dňa 8. 8. 2018).

[371] DAVIS, J.: Hackers Take Down the Most Wired Country in Europe ... cit. dielo, dostupné na: https://www.wired.com/2007/08/ff-estonia/.

[372] RABOIN, B.: Corresponding Evolution: International Law and the Emergence of Cyber Warfare ... cit. dielo, s. 616 – 617.

[373] The Economist: A Cyber-riot ... cit. dielo, dostupné na: http://www.economist.com/node/9163598.

z 20 000 na viac ako 4 milióny za sekundu.[374] Situáciu komplikovala aj skutočnosť, že útočníci neustále vylepšovali svoje škodlivé zásahy s cieľom vyhýbania sa filtrom. To len potvrdzovalo presvedčenie, že ten kto bol za tým, bol sofistikovaný, rýchly a inteligentný. Týždeň po premiestnení sochy stovky príspevkov na internete volali po koordinovanom útoku, ktorý sa mal realizovať o polnoci 9. mája, v deň, keď Rusko oslavuje víťazstvo v druhej svetovej vojne. Objavovali sa príspevky v duchu „*Nesúhlasíte s politikou eSStónska ???*" (používateľ s názvom Victoris na ruskom online fóre). „*Možno si myslíte, že nemáte žiadny vplyv na situáciu? Môžete ho mať na internete!*" Príspevok potom obsahoval presné pokyny na spustenie kybernetickej operácie na konkrétne estónske stránky. V reálnom svete to možno prirovnať vojenskému náborovému stredisku s následnými rozkazmi.

Hackeri používali súkromné chatovacie miestnosti na komunikáciu medzi sebou, ale aj na verejných fórach naznačovali svoje zámery: „*DDoS sa vyskytuje aj teraz, ale niečo silnejšie je na ceste :)*", napísal hacker s názvom S1B. „*Dňa 9. mája sa plánuje útok, ktorý bude masívny - plánuje sa, že Estonnet skočí :)*". Následne bolo Estónsko zablokované prevádzkou, ktorá predstavovala viac ako 4 milióny paketov za sekundu, čo je 200 násobný nárast. Celosvetovo sa takmer 1 milión počítačov náhle dostal do mnohých estónskych lokalít, od ministerstva zahraničných vecí až po najvýznamnejšie banky.[375]

Po tom, čo Estónsko požiadalo NATO o kybernetickú pomoc a krátko po príchode expertov NATO do Estónska, sa útoky zastavili.

Niektorí sa domnievajú a Estónsko verejne vyjadrilo svoje presvedčenie, že za kybernetické operácie je zodpovedné Rusko. Samotná povaha DDoS útokov však znemožňuje vysledovať konečný zdroj a vieme len, že servery zodpovedné za útoky pochádzali z niekoľkých lokalít vrátane Spojených štátov, Egypta, Južnej Ameriky a Ruska,[376] pričom väčšina z nich prichádzala z mnoho tisíc obyčajných počítačov. Viaceré boli prevádzkované súkromnými osobami nahnevanými na Estónsko. Mnoho ďalších pochádzalo z počítačov napadnutých vírusom s cieľom zapojiť ich do týchto útokov bez vedomia ich majiteľov.[377]

Niektoré zdroje hovoria o tom, že v druhej fáze týchto útokov sa na nich podieľalo viac ako milión počítačov z viac ako sto krajín. Celkovo však tieto útoky

[374] RABOIN, B.: Corresponding Evolution: International Law and the Emergence of Cyber Warfare ... cit. dielo, s. 617; porovnaj: KERNER, S. M.: Estonia Under Russian Cyber Attack? In: InternetNews, May 18, 2007, dostupné na: http://www.internetnews.com/security/article.php/3678606/Estonia+Under+Russian+Cyber+Attack.htm (navštívené dňa 8. 8. 2018).

[375] DAVIS, J.: Hackers Take Down the Most Wired Country in Europe ... cit. dielo, dostupné na: https://www.wired.com/2007/08/ff-estonia/.

[376] RABOIN, B.: Corresponding Evolution: International Law and the Emergence of Cyber Warfare ... cit. dielo, s. 617 – 618.

[377] The Economist: A Cyber-riot ... cit. dielo, dostupné na: http://www.economist.com/node/9163598.

spôsobili obmedzené ekonomické a komunikačné narušenia, no žiadne výrazné materiálne škody, zranenia, či straty na životoch.[378]

Existuje viacero indícií, ktoré naznačujú, že na kybernetických operáciách mala podiel ruská strana: bulletiny v ruskom jazyku povzbudzovali užívateľov, aby obhajovali vlasť a na prinajmenšom jednej estónskej stránke útočníci nahradili domovskú stránku frázou „*Hacked from Russian hackers*".

V rámci FSB (nástupcu KGB) údajne existuje špecifické oddelenie, ktoré sa špecializuje na koordináciu kybernetických kampaní proti tým, ktorých považujú za hrozbu. V tomto prípade však mala Ruská vláda malý záujem vystopovať vinníkov[379] a bližšie sa týmto prípadom zaoberať.

Rusko poprelo a naďalej popiera akúkoľvek účasť na uvedených kybernetických operáciách. Akékoľvek závery z pohľadu zodpovednosti zostávajú preto v rovine úvah a teórií.

Niektorí sú presvedčení, že DDoS útoky boli odplatou zo strany Ruska za premiestnenie sovietskeho vojnového pamätníka z centra hlavného mesta Tallinn na vojenský cintorín. Iní zastávajú názor, že uvedené aktivity boli pokusom Ruska otestovať pripravenosť Západu na takéto kybernetické operácie, ako aj záväzok NATO voči svojim najnovším a najmenším členom (Estónsko sa stalo členom NATO v roku 2004).[380]

Za zmienku stojí aj vyjadrenie ruského hackera E. Azizova, ktorí tvrdí, že uvedené kybernetické operácie majú na svedomí jednoducho hackeri, ktorých otcovia a starí otcovia urobili obrovské obety pre Rusko počas druhej svetovej vojny. Zdôraznil, že títo neboli koordinovaní vládou. Zapojené botnety - ktoré sú zvyčajne prenajímané na trestné účely - boli v tomto prípade odoslané zadarmo. Nešlo totiž v tomto prípade o peniaze, bolo to o ruskej hrdosti. Ak by to bola pravda, mohlo by to byť ešte viac znepokojujúce. Predpokladalo by to existenciu skupiny ruských hackerov, ktorí samy osebe môžu narušiť rutinné fungovanie obchodu, médií a vlády, kedykoľvek chcú. Ak by to tak bolo, títo hackeri by predstavovali značnú silu bez štátnej príslušnosti - akúsi súkromnú milíciu.[381]

Z hľadiska bezpečnosti je podstatnou aj skutočnosť, že Estónsko je členom NATO. Táto medzinárodná organizácia vojensko-politickej povahy na uvedenú akciu nereagovala protiútokom, no následkom bolo zriadenie Centra výnimočnosti

---

[378] ROSCINI, M.: Cyber Operations and the Use of Force in International Law ... cit. dielo, s. 4 - 5.

[379] DAVIS, J.: Hackers Take Down the Most Wired Country in Europe ... cit. dielo, dostupné na: https://www.wired.com/2007/08/ff-estonia/.

[380] RABOIN, B.: Corresponding Evolution: International Law and the Emergence of Cyber Warfare ... cit. dielo, s. 617; porovnaj: APPLEBAUM, A.: For Estonia and NATO, A New Kind of War, Washington Post, May 22, 2007, s. Al5.

[381] DAVIS, J.: Hackers Take Down the Most Wired Country in Europe ... cit. dielo, dostupné na: https://www.wired.com/2007/08/ff-estonia/.

pre oblasť spoločnej kybernetickej obrany [Cooperative Cyber Defense Center of Excellence (CCDCOE)][382] so sídlom v Estónskom Tallinne.

3.2 Rusko – Gruzínsky konflikt (2008)

Kybernetické operácie zamerané proti Gruzínsku sa uskutočnili na prelome júla a augusta 2008, pred a počas ozbrojeného konfliktu s Ruskou Federáciou. Išlo o konflikt medzi Gruzínskom na jednej strane a Ruskom, Južným Osetskom a Abcházskom na druhej strane, pričom primárnym predmetom sporu bola snaha o secesiu Južného Osetska.[383] Ozbrojený konflikt začal v noci zo 7. na 8. augusta 2008, keď gruzínska armáda začala vojenskú operáciu s cieľom dobyť hlavné mesto Južného Osetska, Cchinvali. Po ostreľovaní osetských osád došlo k ťažkým bojom medzi gruzínskymi armádnymi silami a juhoosetskými jednotkami (ktoré sa snažia o odtrhnutie gruzínskej autonómnej republiky Južné Osetsko). Išlo však len o vyvrcholenie dlhé obdobie zvyšujúceho sa napätia, provokácií a incidentov.

Konflikt má skutočne hlboké korene v histórii regiónu, v národných tradíciách a ašpiráciách národov, ako aj v často nesprávnom vnímaní a predstavách aktérov, ktoré boli občas zneužívané. Podľa niektorých informácií došlo pri útoku aj k zasiahnutiu základne ruských mierových síl. Následkom uvedeného postupu bolo, že Rusko obvinilo Gruzínsko z agresie proti Južnému Osetsku a zahájilo pozemnú, leteckú a námornú inváziu do Gruzínska.[384] Boje, ktoré sa čoskoro rozšírili aj do iných častí Gruzínska, trvali len 5 dní, no straty na ľudských životoch a škody na majetkoch boli značné. Gruzínska strana uviedla, že na jej strane bolo 170 vojakov, 14 policajtov a 228 civilistov zabitých a 1 747 osôb zranených. Ruská strana tvrdila, že na jej strane zahynulo 67 vojakov a 283 bolo zranených. Na strane Južného Osetska bolo 365 zabitých, pričom toto číslo pravdepodobne zahŕňa vojakov aj civilistov. Celkovo približne 850 ľudí prišlo o život, nehovoriac o tých, ktorí boli zranení, ktorí zmizli, alebo o viac ako 100 000 civilistoch, ktorí utiekli z domovov.[385]

Jednou z osobitných čŕt tohto konfliktu boli súčasne prebiehajúce kybernetické operácie. Tieto spôsobili, že vládne webové stránky sa dostali do režimu offline

[382] O'CONNELL, M. E., ARIMATSU, L., WILMSHURST, E.: Cyber Security and International Law ... cit. dielo, s. 4; Estónsko pritom navrhlo koncept Centra kybernetickej obrany už v roku 2004 po svojom vstupe so Aliancie. Bližšie pozri: NATO Cooperative Cyber Defence Centre of Excellence, History; dostupné na: https://ccdcoe.org/history.html (navštívené dňa 5. 8. 2018).

[383] MELKOVÁ, M., SOKOL, T.: Kybernetický priestor ako nová dimenzia národnej bezpečnosti ... cit. dielo, s. 59.

[384] Bližšie pozri: Independent International Fact-Finding Mission on the Conflict in Georgia, September 2009, Volume I, s. 10 - 11; dostupné na: http://www.mpil.de/files/pdf4/IIFFMCG_Volume_I2.pdf (navštívené dňa 12. 12. 2018).

[385] Bližšie pozri: Tamtiež, s. 5.

a spomalili internetové služby. Najmä bezprostredne pred tým a po tom ako ruské jednotky vstúpili do Gruzínskej provincie Južné Osetsko, niekoľko vládnych webových stránok bolo znefunkčnených a ich obsah bol nahradený anti - Gruzínskou propagandou, zatiaľ čo DDoS útoky znemožnili schopnosť kaukazskej krajiny šíriť informácie.

Týmto kybernetickým operáciám bola venovaná pozornosť v Správe Nezávislej vyšetrovacej misie o konflikte v Gruzínsku z roku 2009,[386] ktorá však nedospela k záveru o ich pripísateľnosti alebo legalite, ale uvádza, že „*ak boli tieto útoky riadené vládou alebo vládami, je pravdepodobné, že táto forma vojny bola po prvýkrát použitá v medzištátnom ozbrojenom konflikte*".[387] Aj iní autori uvádzajú, že Ruský kombinovaný kybernetický a kinetický útok na Gruzínsko v roku 2008 bol prvým praktickým testom tejto doktríny. Mnohé z tých istých techník a počítačov zapojených proti Estónsku pred rokom sa opäť objavili aj v tomto prípade proti Gruzínsku.[388]

Medzi najvýznamnejšie udalosti spôsobené kybernetickými operáciami možno zaradiť nasledujúce:

- už dňa 20. júla bola internetová stránka prezidenta Saakašviliho vypnutá počas 24 hodín;
- dňa 7. augusta došlo k zmocneniu sa niekoľkých gruzínskych serverov a internetovej prevádzky, ktoré boli následne umiestnené pod externú kontrolu;
- o deň neskôr, 8. augusta začali rozsiahle kybernetické útoky proti lokalitám v Gruzínsku. Zdroj kybernetických útokov bol pritom neistý. Niektoré správy ich pripísali organizácii s názvom „*Russian Business Network*" (známej aj ako zločinecký syndikát RBN[389]);
- v tomto čase bolo oznámené, že všetky webové stránky gruzínskej vlády boli nedosiahnuteľné z amerického, britského a európskeho kybernetického priestoru. Turecký server AS9121 TTNet, jeden zo smerovacích bodov pre prevádzku na Kaukaz, bol zablokovaný;

---

386 *Report of the Independent Fact-Finding Mission on the Conflict in Georgia.*

387 ROSCINI, M.: Cyber Operations and the Use of Force in International Law ... cit. dielo, s. 7 - 8, porovnaj: *Report of the Independent Fact-Finding Mission on the Conflict in Georgia*, September 2009, Vol II, s. 217 – 19, dostupné na: http://www.mpil.de/en/pub/publications/archive/independent_international_fact.cfm, (stránka navštívená dňa 10. 10. 2015).

388 SMITH, J. D.: Russian Cyber Strategy and the War Against Georgia. In: NATOSource|Daily News of the World's Most Powerful Alliance, January 17, 2014, dostupné na: http://www.atlanticcouncil.org/blogs/natosource/russian-cyber-policy-and-the-war-against-georgia (stránka navštívená dňa 3. 10. 2015).

389 *The Russian Business Network* je ruskou kybernetickou kriminálnou organizáciou špecializujúcou sa predovšetkým na krádeže identít s cieľom ich ďalšieho predaja. RBN vznikla ako poskytovateľ internetových služieb pre detskú pornografiu, phishing, spam a malware s fyzickým sídlom v meste Petrohrad. MELKOVÁ, M., SOKOL, T.: Kybernetický priestor ako nová dimenzia národnej bezpečnosti ... cit. dielo, s. 59.