RADOSLAV ŠTEFÍK

Kybernetické útoky počas prezidentskej kampane v Spojených štátoch amerických v roku 2016

The rapid growing informatization by the end of 90s in last century became crucial to society development. This new situation became new challenges regarding personal and national security. Internet as a global network create cyberspace, which is becoming increasingly a domain for cyber confrontation. The aim of this article is to review cyber-attacks which took place during US president election in 2016. These cyber-attacks have brought fundamental change in perception of cyber threats and impact of cyber-attacks to political functions and legitimacy.

Key words: Advanced Persistent Threat; Attribution; Cyberspace; Elections; Non-states actors; States actors

1. Úvod

Pojmy ako kybernetický priestor, kybernetické hrozby, prípadne kybernetické zbrane sa čoraz častejšie stávajú témami nielen bezpečnostných odborníkov, vojenských analytikov, ale aj politikov. Termín kybernetický priestor zrejme po prvý raz použil už v roku 1982 Gibson vo svojom vedecko-fantastickom románe *Neuromanacer* a charakterizoval ho ako konsenzuálne halucinácie, ktoré denne pociťujú miliardy oprávnených operátorov i detí všetkých národov, učiace sa matematické koncepty.[1] V modernom ponímaní kybernetický priestor chápeme ako systém vzájomne poprepájaných informačných systémov a každý informačný systém pripojený do celosvetovej siete, internetu, sa automaticky stáva časťou kybernetického priestoru. Podľa Clarka a Choucriho je kybernetický priestor tvorený fyzickými zariadeniami, logickými vrstvami, informačnými vrstvami a používateľmi.[2] Spojené štáty americké vo svojej stratégii definujú kybernetický priestor ako nervový systém, ktorý sa skladá z jednotlivých informačných systé-

[1] GIBSON, W.: *Neuromanacer*, 1984, s. 5.
[2] CLARK, D., CHOUCRI, N.: *Integrating Cyberspace and International Relations: The Co-Evolution Dilema*, 2012.

mov, zariadení a dovoľuje kritickej infraštruktúre plniť jej úlohy.[3] Slovenská republika rovnako ako Česká republika toto chápanie kybernetického priestoru rozširuje o pojem informácie. Informácie sú v digitálnom svete vytvárané, ukladané a prostredníctvom elektronických komunikácií a služieb prebieha ich aktívna výmena.[4]

V roku 1995 bolo k internetu pripojených 0,4 % svetovej populácie, čo v tom čase predstavovalo približne 16 miliónov používateľov. Internetovým pripojením v tom čase disponovali predovšetkým vládne inštitúcie, vedecké pracoviská a medzinárodné organizácie. Ako príklad možno uviesť svetové štatistiky, podľa ktorých bol v období rokov 2000 až 2016 nárast používateľov internetu o 918,3 %[5], čo v celkových číslach predstavovalo 3,675 miliardy používateľov[6]. Za takýmto rastom treba vidieť prudký technologický rozvoj v oblasti informačných a telekomunikačných technológií, pokles cien telekomunikačných služieb a veľký dopyt používateľov po nových technológiách.

Z pohľadu bezpečnosti nám rozvoj informačných technológií a ich penetrácia prakticky do každodenných činností priniesla aj nové hrozby, na ktoré musia jednotlivci, súkromné spoločnosti a štátne inštitúcie reagovať v dostatočnej miere. Pre štátne orgány sa kybernetický priestor stáva čoraz častejšie otázkou národnej bezpečnosti. Krajiny ako Spojené štáty americké, Rusko, Čína, Francúzsko, Nemecko, Irán či severná Kórea chápu kybernetický priestor ako novú operačnú doménu, porovnateľnú so zemou, vodou, vzduchom a vesmírom. Slovenská republika aplikovala tento princíp vo svojej *Koncepcii kybernetickej bezpečnosti na roky 2015 až 2020*.[7] Severoatlantickou alianciou bol kybernetický priestor uznaný na Varšavskom samite v roku 2016. Táto dohoda pre alianciu zadefinovala kybernetický priestor ako integrálnu súčasť kolektívnej obrany.[8] Význam kybernetického priestoru z pohľadu strategickej vojenskej sily môžeme nájsť aj vo vyhlásení najvyšších predstaviteľov krajín združených v Šanghajskom pakte, v ktorom sa uvádza, že použitie informačných technológií v negatívnom význame môže viesť k podobnej katastrofe ako použitie zbraní hromadného ničenia.[9] Podľa čínskych stratégov Qiaoa a Wanga kybernetický priestor predstavuje možnosť vedenia vojny bez priameho fyzického dosahu na ľudí a mení strategický prístup vedenia vojny, kde v budúcnosti bude paralelne koexistovať konvenčné a kybernetické vedenie vojenských operácií. Postupne sa budú stierať rozdiely medzi vojenskými a civilnými technológiami, profesionálnymi vojakmi, nie profesionálnymi bojovníkmi, a pohľad, čo vlastne je priestor vedenia operácie, sa stane čoraz viacej nečitateľ-

[3] THE WHITE HOUSE, *The National Strategy to Secure Cyberspace*, 2003, s. 6.
[4] KONCEPCIA KYBERNETICKEJ BEZPEČNOSTI SLOVENSKEJ REPUBLIKY NA ROKY 2015 – 2020, 2015; JIRÁSEK, P. et al.: *Výkladový slovník kybernetickej bezpečnosti*, 2015, s. 59.
[5] INTERNET WORLD STATS, 2016.
[6] Ibid.
[7] KONCEPCIA KYBERNETICKEJ BEZPEČNOSTI SLOVENSKEJ REPUBLIKY NA ROKY 2015 – 2020, 2015.
[8] NORTH ATLANTIC TREATY ORGANIZATION, *Warsaw Summit Communiqué*, 2016.
[9] SHANGHAI COOPERATIVE ORGANIZATION, *SCO members sign statement on international information security,* 2006.

ný.[10] Ruská federácia vo svojom *Koncepčnom pohľade na aktivity v kybernetickom priestore* opisuje pojem informačnej vojny, ktorá znamená konfrontáciu dvoch alebo viacerých štátov v informačnom priestore s cieľom poškodenia informačných systémov, procesov a zdrojov. Tieto škody podkopávajú dôveru v politický, ekonomický a sociálny systém a za použitia masívnej dezinformačnej kampane dochádza k destabilizácii spoločnosti, čo môže viesť k zmene politických rozhodnutí na konfrontáciu.[11]

Z politologického pohľadu sme iba na začiatku chápania dosahu kybernetických hrozieb na fungovanie domácej politiky a ich vplyvu na medzinárodné vzťahy. V slovenskej vedeckej a odbornej literatúre sa téme kybernetickej bezpečnosti autori venujú prevažne v technickej rovine. Pre súčasnú politiku predstavujú moderné komunikačné technológie najmä nové komunikačné kanály, ktoré umožňujú priamu interakciu medzi politickými stranami a ich voličmi. No napríklad podľa Šmihulu každá zmena politickej komunikácie znamená aj zmenu fungovania politiky, a to predovšetkým z pohľadu nárokov na politické elity a ich politickú prácu. Rýchla adaptácia na nové komunikačné prostredie môže znamenať náskok pred politickými súpermi.[12]

Hlavným cieľom tohto článku je prostredníctvom analýzy otvorených zdrojov potvrdiť alebo vyvrátiť hypotézu, či vhodné použitie kybernetických nástrojov ponúka možnosti ovplyvnenia volebného procesu štátu. S cieľom spresnenia hlavného cieľa boli stanovené nasledujúce oblasti analýzy:

Prvá oblasť sa týka *aktérov* v kybernetickom priestore. Predpokladom je, že hlavným aktívom v kybernetickom priestore je informácia. Z tohto dôvodu predstavuje kybernetický priestor platformu na uplatnenie sa štátnych, ako aj neštátnych aktérov.

Druhou je oblasť použitia *kybernetických techník*. Všeobecne možno konštatovať, že sofistikovanosť a rozsah kybernetických útokov je bezprostredne závislá od technickej vyspelosti útočníka.

Verifikácia a falzifikácia hlavného cieľa a pracovných hypotéz budú overované za pomoci prípadovej štúdie predvolebnej prezidentskej kampane, ktorá v Spojených štátoch amerických vrcholila v roku 2016. Na dosiahnutie tohto cieľa je štúdia rozdelená do nasledujúcich častí: Prvá časť je venovaná vymedzeniu a definovaniu hlavných aktérov, pre ktorých sa kybernetický priestor stal novou operačnou doménou na vedenie kybernetických operácií. Druhá časť bude opisovať priebeh kybernetických útokov počas prezidentskej kampane v Spojených štátoch amerických v roku 2016. Záver je venovaný problému motivácie k uskutočneniu takýchto kybernetických útokov a problému atribúcie ako jedného z kľúčových faktorov na určenie adekvátnych protiopatrení.

[10] QIAO, L., WANG X.: *Un-Restricted Warfare*, 1999, s. 31.

[11] THE NATO COOPERATIVE CYBER DEFENCE CENTRE OF EXCELENCE, *Conceptual Views Regarding the Activities of the Armed Forces of the Russian Federation in Cyber Space,* 2011.

[12] ŠMIHULA, D.: *Médiá ako determinant politiky*, 2006, s. 65.

2. Vymedzenie a definovanie hlavných aktérov v kybernetickom priestore

V rámci geopolitického pôsobenia aktérov je jedným zo základných predpokladov definovanie, vymedzenie a medzinárodná legalizácia hraníc. Ako uvádza Volner, pojem hranice možno chápať viacvýznamovo, a môže znamenať nielen geografickú hranicu daného štátu, ale napríklad aj hranice geopolitického pôsobenia aktérov, hranice strategických síl či mocensko-politickej rovnováhy.[13] V kybernetickom svete sa tieto pravidlá strácajú. Štát hrá síce naďalej vedúcu úlohu, no vďaka rastúcemu počtu neštátnych aktérov je s nimi nútený o svoj vplyv súperiť. Neštátnych aktérov v kybernetickom svete predstavujú jednotlivci, korporácie, zločinecké organizácie alebo aj štátom sponzorovaní aktéri. Pre štáty je kybernetický priestor novým priestorom, doménou, na použitie „ofenzívnych a defenzívnych kybernetických techník k útoku, obrane a špionáži, typický pre politické a iné ciele národnej bezpečnosti".[14] V tejto súvislosti sa prevažne v anglosaskej terminológii spomína pojem kybernetická moc (angl. Cyber-power). Metodologickým východiskom tohto konceptu je teória moci, ako bola koncipovaná Maxom Weberom či Robertom Dahlom.[15] Tento koncept sa neskôr rozvinul a čoraz častejšie sa spomína v súvislosti so strategickým vnímaním kybernetického priestoru ako miesta bojiska budúcnosti. Tieto teórie majú základ v Clausewitzovom diele *O vojne*. Vojna je podľa Clausewitza sociálnym javom, ktorej protikladom je mier. Boj je vo vojne zjavný, no v mieri je utajený, ale v oboch stavoch trvá ako zápas o kultúrne a hmotné hodnoty.[16] Istú analógiu možno nájsť aj v komparácii so vzdušnou mocou tak, ako bola formulovaná Williamom „Billom" Mitchelom, ktorý vzdušnú moc definoval ako „schopnosť niečo vo vzduchu spraviť".[17] Štát je všeobecne považovaný za kľúčového aktéra. Preto by malo byť jednou z jeho priorít vytváranie takého koncepčného inštitucionálneho a právneho rámca, ktorý mu zabezpečí v novej doméne komparatívnu výhodu.

Informácia je nepochybne jedno z hlavných aktív kybernetického priestoru. Už podľa Sun Tzua zohrávala informácia v stratégii kľúčovú rolu. „Poznaj nepriateľa a poznaj seba. Tak vyhráš sto bitiek a nebudeš porazený. Ak nepoznáš nepriateľa, ale poznáš seba, raz vyhráš a raz budeš porazený. Ak nepoznáš ani nepriateľa, ani seba, určite prehráš každú bitku."[18] Špionáž je preto považovaná za tradičnú aktivitu štátu, a to aj v prípade, že samotný akt špionáže sa všeobecne považuje za trestný čin vo vnútroštátnych právnych systémoch. Spravodajské služby bežne využívajú všetky dostupné prostriedky a metódy na získanie požadovaných informácií.[19] Hlavnou motiváciou štátnych aktérov je z takto získaných informácií profitovať politicky, eko-

[13] VOLNER, Š.: *K teoretickým a metodologickým aspektom skúmania geopolitického pôsobenia*, 2004, s. 28.
[14] HEALEY, J.: *A Fierce Domain: Conflict in Cyberspace 1986 to 2012*, 2013, s. 14.
[15] NYE, S. J.: *Cyber Power,* 2010, s. 2; JORDAN, T.: *Cyber Power. The culture and politics of cyberspace and the Internet*, 1999, s. 8; BETZ, J. D a STEVENS, T.: *Cyberspace and the States: Toward a Strategy for Cyber-power, 2011,* s. 42.
[16] VOJENSKÝ HISTORICKÝ SBORNÍK. *Druhá přednáška kruhu pro studium čs. dějin vojenských,* 1932, s. 238.
[17] BETZ, J. D a STEVENS, T.: *Cyberspace and the States: Toward a Strategy for Cyber-power,* 2011, s. 43.
[18] SUN TZU. *Art of War*, 1996.
[19] ZIOLKOWSKI, K.: *Peacetime Regime for State Activities in Cyberspace*, 2013, s. 14.

nomicky či vojensky. V niektorých pohľadoch kybernetickú špionáž považujeme za nevyhnutnú súčasť globálnej hospodárskej súťaže a monitorovanie kybernetických schopností protivníkov ako nevyhnutnosť pre národnú bezpečnosť.

Kybernetické nástroje, často používané štátnymi aktérmi, sa postupne stávajú voľne dostupné na čiernom trhu aj pre ostatných aktérov, a to najmä na páchanie kybernetickej kriminality.[20] Portfólio neštátnych aktérov pôsobiacich v kybernetickom priestore je veľmi pestré a zahŕňa rôzne skupiny od jednotlivcov cez organizované hackerské skupiny, teroristické a zločinecké organizácie, ale taktiež aj nadnárodné korporácie. Cieľom neštátnych aktérov je prostredníctvom kybernetických zručností získať ekonomickú a bezpečnostnú prevahu nad svojimi obeťami. Kybernetický priestor pre tieto skupiny poskytuje vysoký stupeň anonymity, čo pri relatívne nízkych ekonomických nákladoch vedie k uskutočňovaniu sofistikovaných kybernetických útokov. Prehľad neštátnych aktérov, ich motivácie, ciele a hlavné metódy kybernetických útokov poskytuje nasledujúca tabuľka.

Tabuľka č.1: Hlavné skupiny neštátnych aktérov.[21]

Druh	Motivácia	Cieľ	Metóda
Jednotlivec	žiadna, testovanie vlastných schopností	všetky	priame
Script kiddies – neskúsený hacker	zvedavosť, ego	jednotlivci, spoločnosti, organizácie	používanie cudzích scriptov a nástrojov
Haktivizmus	politická a sociálna ideológia	veľké spoločnosti, vládne inštitúcie	protest vyjadrený zmenou webových stránok alebo DDoS útokov
Hackerské skupiny **- Black hat** **- Grey hat**	ego, osobné animozity, ekonomické záujmy,	všetky	malware, vírus, prekonanie zraniteľností, DDos útoky,
Hackerské skupiny **- White hat**	idealizmus, rešpektovanie právneho systému	všetky	penetračné testovanie, odhaľovanie a upozorňovanie na zraniteľností
Teroristické skupiny	politická a sociálna zmena	nevinné obete, vládne a medzinárodné inštitúcie,	šírenie násilných až brutálnych činov prostredníctvom sociálnych sietí, propaganda, verbovanie nových stúpencov
Organizovaný zločin	ekonomické záujmy	jednotlivci, spoločnosti	všetky dostupné techniky
Kybernetická špionáž	finančné a politické záujmy	jednotlivci, spoločnosti, vládne inštitúcie	všetky dostupné techniky

[20] NATIONAL CYBER SECURITY CENTER. *Cyber Security Assessment Netherlands,* 2015, s. 28.

[21] SINGHOLM, J.: *Non-State Actors in Cyberspace operation*. 2013.

Pre potreby tohto článku je potrebné samostatne pripomenúť skupinu takzvaných aktérov, ktorých v odborných publikáciách nazývajú ako „pokročilá a trvalá hrozba“[22] (angl. Advanced Persistent Threats, APT). Cieľom APT je podľa *Českého výkladového slovníka kybernetickej bezpečnosti* dlhodobé a vytrvalé infiltrovanie sa do cieľových systémov, a to pomocou pokročilých a adaptívnych techník.[23] Tieto skupiny sú často, no nie vždy, napojené na vládne inštitúcie, s cieľom kapacitami a potrebnými zdrojmi efektívne a konzistentne sa zamerať na špecifickú entitu.[24] Čo robí z APT doslova kybernetickú zbraň? Je to vysoká miera profesionalizácie kybernetických útokov a priame zameranie sa na konkrétny cieľ. Na rozdiel od hackerských útokov, ktoré využívajú slabiny, prípadne zle zabezpečené informačné systémy, APT postupujú strategicky, často svoj kybernetický útok modifikujú a prispôsobujú vzniknutej situácii, využívajú rozličné vektory útokov, a preto sú veľmi často úspešní. Obrana proti takémuto druhu nepriateľa si vyžaduje veľmi dobrú organizáciu bezpečnosti po materiálnej, ľudskej a ekonomickej stránke. V nasledujúcej tabuľke sú uvedené najznámejšie APT skupiny spolu s ich realizovanými kybernetickými útokmi.[25]

Tabuľka č. 2: Najznámejšie APT skupiny.[26]

Primárny názov	Iné označenie	Krajina pôvodu	Známe realizované kybernetické útoky
Sofacy	APT 28, Sednit, Fancy Bear, Pawn Storm	Ruská federácia	Bundestag, TV5 Monde
APT 29	Dukes, CozyDuke, Cozy Bear,	Ruská federácia	americké korporácie
Cyber Berkut		Ruská federácia	ukrajinská revolúcia, ukrajinsko-ruský konflikt
APT 2,	Unit 61486, TG-6952, Group 36	Čínska ľudová republika	prevažne angl. hovoriace krajiny, IT spoločnosti, finančné inštitúcie
APT 1	Unit 61398, TG-8223, Group 3	Čínska ľudová republika	
Flying Kitten	Saffron Rose, Ajax Security Team, Group 26	Iránska islamská republika	iránski aktivisti a disidenti
Rocket Kitten		Iránska islamská republika	Izrael, Saudská Arábia, vysoko postavení vojenskí funkcionári, aktivisti, žurnalisti, vedci

[22] JIRÁSEK, P. et al.: *Výkladový slovník kybernetickej bezpečnosti*. 2015, s. 87.

[23] Ibid, s. 87.

[24] HEALEY, J.: *A Fierce Domain: Conflict in Cyberspace 1986 to 2012*. 2013, s. 279.

[25] Poznámka autora: zoznam uvádzaných APT skupín vychádza zo zdrojov prevažne amerických technologických a bezpečnostných spoločností, a preto neodráža celkový stav, pôsobenie a zameranie týchto aktérov v kybernetickom priestore.

[26] OPEN SOURCE DATABÁZA APT SKUPÍN (pozn. autora: údaje do tejto databázy sú poskytované prevažne americkými bezpečnostnými a technologickými spoločnosťami).

Dark Seoul	Bureau 121, Unit 121, Lazarus Group	Kórejská ľudovodemokratická republika	vládne, vojenské, finančné inštitúcie a kritická infraštruktúra najmä v USA a Kórejskej republike

V kybernetickom priestore však všetci vyššie spomenutí aktéri koexistujú paralelne s rozličnými cieľmi, potrebami či motiváciami. Pri neštátnych aktéroch však treba spomenúť, že relatívna anonymita kybernetického priestoru im umožňuje v závislosti od situácie a konkrétneho záujmu prechádzať medzi jednotlivými kategóriami.

3. Prípadová štúdia: kybernetické útoky počas prezidentských volieb v Spojených štátoch amerických

Prezidentské voľby v Spojených štátoch amerických sú v celosvetovom meradle považované za politickú a mediálnu udalosť roka. Z tohto dôvodu je preto potrebné predpokladať zvýšený záujem štátnych aj neštátnych aktérov o „zapojenie sa“ do politického boja. Takéto konanie nie je ničím nezvyčajným, a ako hovorí Ryan, „zahraničné vlády majú záujem podporovať priateľského kandidáta“ rovnako ako „Spojené štáty otvorene podporujú takých kandidátov v iných krajinách, ktorí by mohli predstavovať benefit pre záujmy Spojených štátov“.[27]

Prezidentské voľby v roku 1992 boli vôbec prvými, keď prezidentskí kandidáti William J. Clinton a George H. W. Bush použili vo svojej kampani internet ako jeden z nástrojov na komunikáciu so svojimi voličmi.[28] Významnú úlohu v politickej komunikácii a politickom marketingu začal internet zohrávať až s nástupom nových technológií založených na platforme Web 2.0. Tieto nové technológie zahŕňajú rôzne on-line aplikácie, ktorých obsah je definovaný samotnými používateľmi, ako napr. blogy, sociálne siete, web stránky.[29]

3.1 Kybernetická špionáž

Už vo voľbách v roku 2008 bola zaznamenaná kybernetická kampaň cielená na oba súperiace tábory prezidentských kandidátov. Zo zverejneného materiálu Federálneho vyšetrovacieho úradu (FBI) vyplýva, že informačné systémy Demokratickej, ako aj Republikánskej strany boli infiltrované a odcudzili sa z nich veľké množstvá dát.[30] Za touto kybernetickou kampaňou boli

[27] PAZZANESE, C.: *Inside the hacked U.S. election,* 2016
[28] DAVIS, R. et al.: *The internet in U.S. election campaigns*, 2009, s. 14.
[29] ANDUIZA, E.: *The Internet, election campaigns and citizens: state of affairs,* 2009, s. 6.
[30] GLENDINNING, L.: *Obama, McCain computer hacked during election campaign*, 2008.

pravdepodobne APT organizované čínskou vládou a cieľmi útokov bola súkromná a oficiálna emailová korešpondencia, kľúčové postoje a interné stanoviská. Z tábora republikánskeho kandidáta Johna McCaina bol odcudzený návrh listu adresovaného taiwanskému prezidentovi Ma Ying-jeou, kde McCain vyjadril podporu vojenskej sily Taiwanu. Ako uviedol Schriver[31] po dôvernom rozhovore s vysokopostaveným čínskym diplomatom: „...bolo mi oznámené, že vedia, čo sa deje."[32]

Podobne ako v roku 2008, aj v roku 2016 bola na predvolebnú kampaň zacielená kybernetická špionážna kampaň do oboch hlavných súperiacich táborov. O kompromitácii systémov Národného demokratického výboru a odcudzení bližšie nešpecifikovaného množstva dát z obdobia január 2015 až máj 2016, ktoré patrili siedmim kľúčovým postavám Národného demokratického výboru, informoval denník *Washington Post* 14. júla 2016. Tento kybernetický útok potvrdila v rovnaký deň taktiež bezpečnostná a konzultačná spoločnosť CrowdStrike, ktorá participovala na jeho vyšetrovaní. Podľa CrowdStrike boli za touto kybernetickou kampaňou hackerské skupiny známe ako COZY BEAR a FANCY BEAR.[33] Tieto skupiny, pravdepodobne v spolupráci, monitorovali emailovú a internú digitálnu komunikáciu viac ako rok. Medzi odcudzenými dokumentmi bola aj interná analýza protikandidáta Donalda Trumpa, interná správa o slabinách Hilary Clintonovej a taktiež informácie o sponzoroch jej prezidentskej kampane.[34] O tom, že tento kybernetický útok bol starostlivo pripravovaný a útočníkom záležalo na tom, aby neboli odhalení, svedčí aj fakt, že sa „neustále vracali do napadnutých systémov a modifikovali svoje prístupové metódy".[35] Prvá séria uniknutých dokumentov bola zverejnená na blogu hackera menom Glucifer 2.0, ktorý tvrdil, že stál za kompromitáciou sietí Národného demokratického výboru. Neskôr boli na jeho blogu zverejnené ďalšie série dokumentov, aktívne vystupoval na sociálnych sieťach a na internetovom kanáli VICE.com bolo s ním dokonca uverejnené interview. V tomto interview Glucifer 2.0 potvrdil informácie, že vystupoval ako „samostatný bojovník, ktorý nemá rád Rusov a ich zahraničnú politiku"[36]. Uniknuté dokumenty Národného demokratického výboru boli neskôr uverejňované aj prostredníctvom domény DCLeaks.

Cieľom kybernetických špionážnych aktivít sa stala aj kampaň samotnej prezidentskej kandidátky Hilary Clintonovej. Na základe zverejnenej správy bezpečnostnej a konzultačnej spoločnosti SecureWorks[37] v období marec až apríl 2016 rovnaké skupiny ako v prípade Národného demokratického výboru monitorovali emailovú komunikáciu v rámci internetovej domény hila-

[31] Randal Schriver zastával funkciu politického poradcu pre Áziu republikánskeho kandidáta Johna McCaina v prezidentských voľbách v roku 2008.

[32] LARSON, L.: *Chinese government hackers infiltrated computer networks of Obama, McCain presidential capaigns in 2008: report,* 2013.

[33] ALPEROVITCH, D.: *Bears in the Midst: Inrusion inte the Democratic National Committee*, 2016.

[34] BENNETT, C. a GELLER, E.: *Why Russia is top suspect in the DNC hack*, 2016.

[35] ALPEROVITCH, D.: *Bears in the Midst: Inrusion inte the Democratic National Committee*, 2016.

[36] BICCHIERAI, F. L.: *Full Transcript of Our Interview With DNC Hacker 'Guccifer 2.0'*, 2016.

[37] SECUREWORKS COUNTER THREAT UNIT. *Threat Group – 4127 Targets Hilary Clinton Presidential Campaign*, 2016.

ryclinton.com, ktorú využívali členovia jej kampaňového výboru. „Cieľovými osobami boli vedúci pracovníci v oblasti mediálnej komunikácie vrátane prípravy mediálnych výstupov, financií a koordinácie pracovných stretnutí. Zoznam cieľov zahŕňal:

- politického riaditeľa,
- finančného riaditeľa,
- riaditeľa pre strategickú komunikáciu,
- riaditeľa pre plánovanie pracovných aktivít,
- koordinátora pracovných stretnutí".[38]

Rovnako ako v prípade Národného demokratického výboru bola takto získaná emailová komunikácia zverejnená prostredníctvom domény WikiLeaks. Začiatkom októbra 2016 bola, taktiež na WikiLeakse, zverejnená prvá séria 50 000 emailov Johna Podestu, predsedu kampaňového výboru Hilary Clintonovej.

Národný výbor Republikánskej strany či kampaňový výbor republikánskeho kandidáta Donalda Trumpa tiež potvrdili nezákonné kybernetické aktivity, no žiadne dokumenty z vnútra strany či kampane neboli zverejnené. Ako neskôr uviedol Donald Trump vo svojom prvom januárovom prejave, „oslovili sme množstvo firiem a objednali sme silnú ochranu proti takémuto zasahovaniu proti hackerom, a nik sa k nám nedostal".[39] Odborníci zo spoločnosti SecureWorks vo svojej správe taktiež konštatujú, že nezaznamenali použitie rovnakých techník namierených na Republikánsku stranu alebo na ich prezidentských kandidátov, ktorých kampaň aktívne prebiehala v období marca a mája 2016.[40]

3.2 Kybernetické útoky na voličské databázy

Kybernetická špionáž hlavných politických súperov bola pravdepodobne iba jedným z vektorov celej kybernetickej kampane. FBI, ako aj Úrad pre vnútornú bezpečnosť (ďalej len „DHS") vo svojich vyhláseniach potvrdili kybernetické útoky na voličské registračné systémy vo viac ako 20 štátoch.[41] V štáte Arizona bol za asistencie FBI volebný registračný systém vypnutý niekoľko dní z dôvodov možnej kompromitácie. V štáte Illinois federálne úrady potvrdili neoprávnené oboznámenie sa s osobnými údajmi o približne 700 voličoch. Podozrenie o neoprávnenom oboznámení sa s osobnými údajmi bolo približne pri 86 000 osobných údajoch a podozrenie o oboznámení sa pri približne 3 533 záznamoch nepodarilo identifikovať.[42] Hackeri sa dostali

[38] Ibid.

[39] TRUMP, D.: *Tlačová konferencia D. Trumpa o vedení Spojených štátov,* 11. január 2017.

[40] SECUREWORKS COUNTER THREAT UNIT. *Threat Group – 4127 Targets Hilary Clinton Presidential Campaign*, 2016.

[41] LEVINE, M. a THOMAS, P.: *Russian hackers targeted nearly half of states voters registration systems, Successfully infiltrated 4*, 2016.

[42] STATE BOARD OF ELECTION. *Illinois Voter Registration System Records Breached*, 2016.

k menám, adresám, číslam vodičských oprávnení, minimálne k štyrom číslam z čísla sociálneho poistenia a dátumom narodenia oprávnených voličov[43]. DHS informoval o systematickej snahe útočníkov využiť zraniteľnosť informačných systémov a pre časopis *Politico* potvrdil, že hackeri všetkého druhu konštantne každý deň testujú kybernetickú obranu.[44] Federálna vláda poskytla dotknutým štátom pomoc vo forme nepretržitého dohľadu a vykonávala potrebné testy zraniteľností jednotlivých databáz.

3.3 Zraniteľnosti elektronických voličských zariadení

Elektronizácia odovzdávania voličských hlasov bola v Spojených štátoch amerických spustená v roku 2002, keď prezident George W. Bush podpísal tzv. „Help America Vote Act". Spolu s týmto programom federálna vláda prispela dvoma miliardami dolárov na nákup nových hlasovacích zariadení a vytvorila štandardy pre tieto nové elektronické hlasovacie zariadenia.[45] Aj napriek tomu sa systém nezjednotil a každý štát, a v niektorých prípadoch každý kraj, používa iné elektronické hlasovacie zariadenia.

Vo všeobecnosti sa však používajú štyri typy voličských systémov:

Optické skenovanie papierových volebných lístkov.

Priame zaznamenávanie odovzdaných hlasov – používa so vo viacerých verziách a elektronické zariadenie zaznamená odovzdané hlasy priamo vo svojej pamäti. Niektoré štáty určujú taktiež podmienku, aby takéto zariadenie umožňovalo voličovi vytlačenie jeho volebného lístku pred zaznamenaním do pamäte zariadenia, a tieto lístky slúžia ako poistka pre prípadný audit volebných výsledkov.

Zariadenia a systémy označovania volebných lístkov slúžia pre hendikepovaných na označovanie papierových volebných lístkov, ktoré sú skenované alebo spočítavané manuálne.

Elektronické zariadenie na čítanie kariet s diernymi štítkami.

Papierové volebné hlasovacie lístky – tento systém sa využíva v značnom množstve štátov.[46]

Po medializovaní udalostí kybernetickej špionáže, úniku a nefunkčnosti elektronických voličských databáz, federálne úrady zisťovali možnosti ovplyvnenia volebného procesu prostredníctvom kompromitácie práve elektronických volebných zariadení. Testom možných zraniteľností sa venovali aj súkromné bezpečnostné spoločnosti. Výsledky testov tímu bezpečnostných expertov spoločnosti Cylance, uverejnených časopisom *Fortune*, upozorňujú, že na elektronických voličských zariadeniach používaných v štátoch Louisiana, Virgínia Pensylvánia, Kalifornia, Florida a New Jersey možno zmeniť výsledný počet hlasov pre jednotlivých kandidátov jed-

[43] Ibid.
[44] GELLER, E. a SAMUELSON, D.: *More than 20 states have faced major election hacking attempts, DHS says*, 2016.
[45] NORDEN, L. a FAMIGHETTI, CH.: *America's Voting Machines at risk,* 2015, s. 8.
[46] VERIFIED VOTING. *Voting Equipment*, 2012.

noduchou výmenou predprogramovanej pamäťovej karty.[47] Časopis *Politico* uverejnil reportáž z testu na jednom type elektronického hlasovacieho zariadenia, ktorý vykonal tím pod vedením profesora Appela z Prinstonskej univerzity. Na základe udalostí týkajúcich sa úniku informácií z prostredia Demokratickej strany pracovali s hypotézou či „by motivovaný programátor mohol manipulovať s novembrovými výsledkami prostredníctvom zariadení, ktoré používame na hlasovanie?" Výsledná odpoveď bola jednoduchá: „Tieto zariadenia, ktoré Američania používajú počas volebného procesu, sú menej bezpečné ako iPhone."[48]

Tieto všetky mediálne výstupy však iba kopírovali výsledky štúdie Brennanovho centra pri New York Univesity of Law, ktorá identifikovala nasledujúce problémové oblasti:

Vek elektronických volebných zariadení – až 43 štátov používa zariadenia staršie ako 10 rokov a 14 štátov používa niektoré zariadenia staršie ako 15 rokov.

Zraniteľnosti a chyby spôsobené vekom zariadení – prevažná väčšina zariadení využíva technológiu deväťdesiatych rokov a operačné systémy, ktoré už nie sú podporované, a preto aplikácia nových bezpečnostných štandardov už nie je možná.

Chýba podpora zo strany dodávateľov technológie – iba šesť štátov používa zariadenia, ktoré sú stále podporované, no až 43 štátov používa viacej ako jeden typ zariadenia, ktorý už nie je podporovaný. Tento faktor spôsobuje problémy predovšetkým s náhradnými dielmi a technickou podporou.

Chýbajúce financovanie nových zariadení alebo novej technológie.[49]

4. Záver

Cieľom tejto štúdie bolo formou analýzy otvorených zdrojov odpovedať na otázku, či správne zvolené kybernetické nástroje dokážu ovplyvniť volebný proces. Ako prípadová štúdia bola zvolená prezidentská predvolebná kampaň v Spojených štátoch amerických z roku 2016. Práve táto predvolebná kampaň nám ukázala veľkosť a závažnosť kybernetických hrozieb v kontexte volebného procesu ako jedného zo základných kameňov demokratického systému. Napriek skutočnosti, že k uvedeným prípadom kybernetických incidentov stále nie sú dostupné všetky informácie, a v prípade únikov informácií ešte stále prebieha vyšetrovanie v pôsobnosti federálnych bezpečnostných zložiek, možno konštatovať, že volebný proces nie je imúnny voči kybernetickým hrozbám.

Vo vzťahu k čiastkovej oblasti analýzy viažucej sa k aktérom v kybernetickom priestore a ich záujmu o narušenie či ovplyvnenie volebného procesu sa dá konštatovať, že vedenie takýchto kybernetických operácií je možné prevažne vysoko skúsenými a vysoko organizovanými

[47] HACKETT, R.: *Watch This Security Researcher Hack a Voting Machine*, 2016.
[48] WOFFORD, B.: *How to Hack an Election in 7 Minutes*, 2016.
[49] NORDEN, L. a FAMIGHETTI, CH.: *America's Voting Machines at risk*, 2015.

skupinami. Kybernetické útoky smerované na Národný demokratický výbor a prezidentskú kandidátku Demokratickej strany Hilary Clintonovú boli, podľa súkromnej bezpečnostnej spoločnosti ESET, cielenými útokmi hackerských skupín známych ako Sednit, APT 28, Fancy Bear, Pawn Storm alebo Sofacy. ESET tieto kybernetické skupiny charakterizovala ako vysoko skúsené a zameriavajúce sa predovšetkým na kybernetickú špionáž s cieľom krádeže citlivých informácií.[50] Bezpečnostná komunita ich dlhodobo zaraďuje k takzvaným štátom sponzorovaným aktérom (APT) s podporou vládnych agentúr Ruskej federácie.[51] V januári bola taktiež publikovaná spoločná správa spravodajských a bezpečnostných služieb, podľa ktorej stáli za kybernetickými útokmi na Národný demokratický výbor, prezidentskú kandidátku Hilary Clintonovú a databázy s voličskými zoznamami v niektorých štátoch ruské spravodajské služby, riadené priamo prezidentom Putinom. Rusko už vo vojne v Gruzínsku a neskôr počas anexie Krymu uplatňovalo tzv. Gerasimovu[52] doktrínu hybridného boja. Táto doktrína chápe hybridnú vojnu ako vojnu novej generácie, v ktorej tradičné vojenské metódy a postupy sú nahradené hybridnými, to znamená širokou škálou politických, ekonomických, informačných, medzinárodných a humanitárnych postupov. Ako uvádza Ivančík, „budúce vojny sa nebudú viesť klasickým spôsobom na bojisku, ale najmä v ľudských mysliach".[53]

Druhá čiastková oblasť analýzy sa týkala kybernetických techník použitých na dosiahnutie požadovaného cieľa. Prevažná väčšina autorov, odborníkov a analytikov sa zhodla na tom, že táto kybernetická kampaň, zamierená na Národný demokratický výbor a kandidátku Demokratickej strany Hilary Clintonovú, bola cielená kybernetická špionáž, ktorá bola dobre koordinovaná a nebola aktom náhodnej hackerskej skupiny. Kybernetickú špionáž z pohľadu medzinárodného práva *Tallinský manuál* definuje ako nie nezákonný akt, ktorý však môže vyvolať nezákonné konanie, a to podľa práva štátu, na ktorého území je špionáž vykonávaná.[54] Z tohto pohľadu je dôležité, akými metódami sa táto kybernetická špionáž vykonáva a či nevyvolá ekonomické a materiálne škody, či dokonca straty na ľudských životoch. V tomto prípade by z pohľadu medzinárodného práva mohol napadnutý štát postupovať rovnako ako v prípade kinetického útoku.[55] Ako však upozorňuje Koh, „pri posudzovaní použitia kinetických jednotiek alebo ofenzívnych nástrojov prostredníctvom kybernetického priestoru je potrebné vyhodnotiť faktory vrátane kontextu, určiť konkrétneho aktéra (atribúcia je kľúčovým faktorom), cieľ a okrem iného aj možné dôsledky".[56] Medzinárodná kybernetická stratégia Spojených štátov z roku 2011 explicitne uvádza, že v prípade „oprávnenosti budú Spojené štáty reagovať na nepriateľské aktivity

[50] CLULEY, G.: *New ESET research paper puts Sednit under the microscope*, 2016.
[51] FIREEYE, *APT28: A window into Russia`s cyber espionage operation?*, 2015, s. 5.
[52] Generál Valerij Vasilievič Gerasimov, náčelník Generálneho štábu Ozbrojených síl Ruskej federácie a prvý námestník ministra obrany, sa považuje za „otca" ruskej koncepcie hybridnej vojny.
[53] IVANČÍK, R.: *Teoretické východiská skúmania problematiky hybridnej vojny – Vojny 21. storočia*, 2016, s. 138.
[54] SCHMITT, M. et al.: *Tallin manual on the International Law Applicable To Cyber Warfare,* 2013, s. 194.
[55] Čl. 2 ods. 4 Charty OSN.
[56] KOH, H. H.: *International Law in Cyberspace,* 2012, s. 4.

v kybernetickom priestore ako v ktoromkoľvek inom".[57] Ako už bolo v úvode spomenuté, Spojené štáty chápu kybernetický priestor ako doménu vojenskej konfrontácie, rovnako ako vodu, vzduch, Zem a vesmír.[58] Rozhodnutie o vykonaní takéhoto odvetného opatrenia je plne v rukách prezidenta. Kybernetický priestor pre skúsených aktérov umožňuje vystupovať anonymne, preto posilňovanie kapacít na odhaľovanie a redukciu anonymity predstavuje rozhodujúcu časť aktivít pri budovaní efektívnej kybernetickej obrany.

Zverejnením získaných dokumentov dostala predvolebná kampaň nové témy, týkajúce sa predovšetkým národnej bezpečnosti. Administratíva prezidenta B. Obamu z tejto kybernetickej kampane obvinila štátom sponzorované skupiny, napojené priamo na bezpečnostné zložky Ruskej federácie, riadené prezidentom Putinom.[59] Motívom týchto kybernetických útokov mala byť podpora neskoršieho víťaza prezidentských volieb, republikánskeho kandidáta Donalda Trumpa. Odpoveď na otázku, či táto kybernetická kampaň D. Trumpovi pomohla, môže byť sporná, pretože v počte odovzdaných hlasov zvíťazila H. Clintonová s rozdielom viacej ako 2,8 milióna hlasov[60] a Donald Trump sa stal prezidentom iba vďaka americkému volebnému systému, keď o víťazovi rozhoduje získaný počet tzv. voliteľov za jednotlivý štát. Naproti tomu kybernetické útoky mierené na jednotlivé štátne volebné komisie a ich databázy s osobnými údajmi oprávnených voličov, ako aj útoky priamo na elektronické voličské zariadenia mohli seriózne narušiť priebeh samotných volieb, legitimitu zvolených kandidátov a štátnej moci.

Budovanie kybernetických spôsobilostí v súčasnosti predstavuje jeden z kľúčových aspektov národnej bezpečnostnej architektúry. Úloha štátu spočíva v zabezpečení odolnosti kritickej infraštruktúry, ktorej súčasťou by sa mali stať aj časti volebného systému spojené s národným kybernetickým priestorom. Bezpečnostné zložky musia disponovať prostriedkami na zastavenie kybernetického útoku a v prípade straty na ľudských životoch, ohrození ekonomických, politických a medzinárodných záujmov vedieť odpovedať na takýto kybernetický útok. K tomu je potrebné budovanie vnútroštátnych právnych mechanizmov a dodržiavanie medzinárodného práva, ľudských práv a Charty Spojených národov. Dôležitosť pochopenia technologického vývoja v teoretickom politologickom myslení spočíva v unikátnosti kybernetického priestoru ako nového mocenského nástroja. Táto unikátnosť spočíva v schopnosti manipulovať strategické prostredie nielen v čase vojny, ale predovšetkým v čase mieru. Nie je náhoda, že väčšina jadrových mocností[61] buduje alebo už má vybudované nielen defenzívne, ale aj ofenzívne kybernetické spôsobilosti, ktoré napríklad v prípade Spojených štátov amerických tvoria aj integrálnu súčasť politiky odstrašenia.

---

[57] White House. *International strategy for Cyber Space, 2011,* s. 14.

[58] Na Varšavskom samite Severoatlantickej aliancie bol kybernetický priestor uznaný ako nová operačná doména NATO a začlenený do kolektívnej obrany aliancie.

[59] INTELLIGENCE COMMUNITY ASSESSMENT. *Assessing Russian Activities and Intentions in Recent US Elections, 2017.*

[60] THE NEW YORK TIMES. *Presidential Election Results: Donald J. Trump Wins*, 2017.

[61] KREJCI, O.: *Válka*, 2014, s. 41.

Literatúra

ALPEROVITCH, D. (2016). *Bears in the Midst: Inrusion inte the Democratic National Committee* [online]. 15/06 2016. [cit. 2017-01-01]. Dostupné na internete: http://sdu.sk/ia0ulj

ANDUIZA, E**.** (2009). *The Internet, election campaigns and citizens: state of affairs.* In: The internet and the electoral communication, vol. 33, str. 5 – 12 , 2009, ISBN 1138-9761, [online]. 12/2009. [cit. 2017-30-03]. Dostupné na internete: http://sdu.sk/KEGTHWH

BEHAR, R. (2016). *Inside Israel's Secret Startup Machine* [online]. 11/05 2016. [cit. 2017-12-01]. Dostupné na internete: http://sdu.sk/UckaPagcQ

BENNETT, C. a GELLER, E. (2016). *Why Russia is top suspect in the DNC hack.* In: *Politico* [online]. 26/07 2016. [cit. 2016-29-12]. Dostupné na internete: http://sdu.sk/4niDh3

BETZ, J. D a STEVENS, T. (2011). *Cyberspace and the States: Toward a Strategy for Cyber-power*. International Institute for Strategic Studies, 2011, s. 158, ISBN 978-0-415-52530-5

BICCHIERAI, F. L. (2016). *Full Transcript of Our Interview With DNC Hacker 'Guccifer 2.0'*. [online]. 21/06 2016. [cit. 201-06-01]. Dostupné na internete: http://sdu.sk/f3BfXZXEn

CLARK, D. CHOUCRI, N. (2012). *Integrating Cyberspace and International Relations: The Co-Evolution Dielma*. In: Massachusetts Institute of Technology. Harvard University [cit. 2017-28-03]. Dostupné na internete: http://ecir.mit.edu/images/stories/Clark_WORKSHOP.pdf

CLULEY, G. (2016). *New ESET research paper puts Sednit under the microscope* [online]. 20/10 2016. [cit. 2016-30-12]. Dostupné na internete: http://sdu.sk/0iaP4BXhc

CNA. (2013). *McCain's letter to Ma stolen by Chinese cyberspies: report*. In: The China Post [onlline]. 08/06 2013. [cit. 2016-29-12]. Dostupné na internete: http://sdu.sk/i0VMaq3A

DEPATRMENT OF HOMELAND SECURITY PRESS OFFICE. (2016). *Joint Statement from the Department Of Homeland Security and Office of the Director of National Intelligence on Election Security* [online]. 07/10 2016. [cit. 2017-01-01]. Dostupné na internete: http://sdu.sk/ODgBs

FIREEYE (2015). *APT28: A window into Russia`s cyber espionage operation?* [online]. 19/08 2015. [cit. 2017-15-01]. Dostupné na internete: http://sdu.sk/vRfqBMz6A

GARRIDO, G. A. (2014). *Cyber Conflict in International relations: Framework and Case Studies*. In: Massachusetts Institute of Technology [online]. 01/04 2014. [cit. 2017-28-03]. Dostupné na internete: http://sdu.sk/g40nGJ

GELLER, E. a SAMUELSON, D. (2016). *More than 20 states have faced major election hacking attempts, DHS says*. In: *Politico* [online]. 30/09 2016. [cit. 2017-03-01]. Dostupné na internete: http://sdu.sk/wYGKV8

GIBSON, W. (1984): *Neuromanacer*, 1. vyd. Londýn : Ace edition, 1984, 271 s. ISBN-0-441-56959.

GLENDINNING, L. (2008). *Obama, McCain computer hacked during election campaign.* In: *The Guardian* [online]. 7/11 2008.[cit. 2016-29-12]. Dostupné na internete: https://www.theguardian.com/global/2008/nov/07/obama-white-house-usa

HACKETT, R. (2016): *Watch This Security Researcher Hack a Voting Machine*. In: *Fortune* [online]. 05/11 2016. [cit. 2017-10-01]. Dostupné na internete: http://fortune.com/2016/11/04/voting-machine-hack-watch-video-cylance/

HEALEY, J. et al., *A Fierce Domain: Conflict in Cyberspace 1986 to 2012*. Arlington, VA: Cyber Conflict Studies Associations, 2013, 352 s. ISBN 0989327418

CHADWICK, A. HOWARD, P. N. (2009). *Routledge Handbook of Internet Politics*. New York : Routledge Taylor&Francis Group. 2009, 511 s. ISBN 978-0-203-96254-1

INTELLIGENCE COMMUNITY ASSESSMENT. (2017). *Assessing Russian Activities and Intentions in Recent US Elections* [online]. 6/01 2017. [cit.2017-15-01]. Dostupné na internete: https://www.dni.gov/files/documents/ICA_2017_01.pdf

INTERNET WORLD STATS. (2016). [online]. www.internetworldstats.com. 9.december 2016 [cit 15.01. 2017]. Dostupné na: http://www.internetworldstats.com/emarketing.htm

IVANČÍK, R. (2016). Teoretické východiská skúmania problematiky hybridnej vojny – Vojny 21. storočia. In: *MEDZINÁRODNÉ VZŤAHY / JOURNAL OF INTERNATIONAL RELATIONS, vol. 14, nr. 2,* s. 130 – 156. ISSN 1339-2751

JIRÁSEK, P. et al. (2015). *Výkladový slovník kybernetickej bezpečnosti*. Praha : Policejní akademie ČR, 2015, s. 240 ISBN 978-80-7251-436-6

JORDAN, T. (1999). *Cyber Power. The culture and politics of cyberspace and the Internet*. Routlenge, London, 1999, s. 250, ISBN 0-415-17078-8

KONCEPCIA KYBERNETICKEJ BEZPEČNOSTI SLOVENSKEJ REPUBLIKY NA ROKY 2015 – 2020 (2015), [online]. 7/2015. [cit. 2017-30-03]. Dostupné na internete: http://sdu.sk/6AYF3EDf3

KOH, H. H. (2012). International Law in Cyberspace. In: Faculty Scholarship Series. Paper 4854 [online]. 12/2012. [cit. 2017-15-01]. Dostupné na internete: http://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=5858&context=fss_papers

KREJCI, O. (2014). Válka. *Britské listy*. Praha, 2014, s. 176, ISBN 978-80-7431-063-8

VOJENSKÝ HISTORICKÝ SBORNÍK (1932). *Druhá přednáška kruhu pro studium čs. dějin vojenských*. Praha, 1932, s. 250, ISSN 1803-7925

LARSON, L. (2013). Chinese government hackers infiltrated computer networks of Obama, McCain presidential capaigns in 2008: report. In: Daily News. [online]. 7/6 2013. [cit. 2016-27-12]. Dostupné na internete: http://sdu.sk/OQ657a5u

LEVINE, M. a THOMAS, P. (2016). Russian hackers targeted nearly half of states voter's registration systems, successfully infiltrated 4. In: *ABS News* [online]. 29/09 2016. [cit. 2017-14-01]. Dostupné na internete: http://sdu.sk/OPVc8ytbK

NATIONAL CYBER SECURITY CENTER (2015). *Cyber Security Assessment Netherlands*. [online]. 11/2015. [cit. 2016-15-12]. Dostupné na internete: https://english.nctv.nl/binaries/25760-csan-5-v3.2-web-uk_tcm32-83562.pdf

NORDEN, L. a FAMIGHETTI, CH. (2015). *America's Voting Machines at risk.* [online]. Brennan Center for Justice at New York University School of Law. 2015. [cit. 2017-10-01]. Dostupné na internete: http://sdu.sk/MtNP42N

NORTH ATLANTIC TREATY ORGANIZATION (2016). *Warsaw Summit Communiqué*, [online]. 09/07 2016. [cit:2017-30-03]. Dostupné na internete: http://www.nato.int/cps/en/natohq/official_texts_133169.htm

NYE, S. J. (2010). *Cyber Power*, Harvard Kennedy School, 2010, s. 24, [cit. 2017-30-03]. Dostupné na internete: http://sdu.sk/foAtmlL

OPEN SOURCE DATABÁZA APT SKUPÍN [online]. 26/12 2015. [cit. 2017-15-01]. Dostupné na internete: http://sdu.sk/0srRs

PAZZANESE, C. (2016). Inside the hacked U. S. election. In: *Harvard gazette*. [online]. 14/12 2016. [cit:2017-05-01]. Dostupné na internete: http://news.harvard.edu/gazette/story/2016/12/inside-the-hacked-u-s-election/

QIAO, L., WANG X. (1999). *Un-Restricted Warfare*. Echo Point Books, 1999, 197 s, ISBN 978-1-62654-306-5

SECUREWORKS COUNTER THREAT UNIT (2016). *Threat Group – 4127 Targets Hilary Clinton Presidential Campaign*. [online]. Secureworks Counter Threat Unit Threat Intelligence 16/06 2016. [Cit.2016-30-12]. Dostupné na internete: http://sdu.sk/P0Uidr

SHANGHAI COOPERATIVE ORGANIZATION (2006). *SCO members sign statement on international information security*. [online]. 15/06 2006. [cit. 2017-30-03]. Dostupné na internete: http://www.gov.cn/misc/2006-06/15/content_311225.htm

SINGHOLM, J. (2013). Non-State Actors in Cyberspace operation. In: *Journal of Military Studies*, vol.4, nr. 1. [online]. 14/04 2013. [cit. 2017-15-01]. 37 s. ISSN 1799-3350, Dostupné na internete: http://journal.fi/jms/article/view/7609

SCHMITT, M. et al. *Tallin manual on the International Law Applicable To Cyber Warfare.* Cambridge : Cambridge University Press, 2013, 304 s. ISBN 9781107024434

STATE BOARD OF ELECTION (2016). *Illinois Voter Registration System Records Breached.* [online]. 31/08 2016. [cit. 2017-15-01]. Dostupné na internete: https://www.elections.il.gov/Downloads/AboutTheBoard/PDF/08_31_16PressRelease.pdf

SUN TZU. (1996). Art of War. *Westview Press*, USA, 1996, ISBN 83- 7361-821-X

ŠMIHULA, D. (2006). Médiá ako determinant politiky. In: *Parlamentný kuriér*. Vol. XIV, 2006, ISSN 1335-0307 s. 65

TRUMP, D. (2017). *Tlačová konferencia D. Trumpa o vedení Spojených štátov*. [online]. 11/01 2017. [cit. 2017-11-01]. Dostupné na internete: http://www.ta3.com/clanok/1097791/tb-d--trumpa-o-vedeni-spojenych-statov-americkych.html

THE NATO COOPERATIVE CYBER DEFENCE CENTRE OF EXCELENCE (2011). *Conceptual Views Regarding the Activities of the Armed Forces of the Russian Federation in Cyber Space***,** [online], 2011. [cit. 2017-30-03]. Dostupné na internete: https://ccdcoe.org/strategies/Russian_Federation_unofficial_translation.pdf

THE NEW YORK TIMES (2017). *Presidential Election Results: Donald J. Trump Wins.* [online]. 04/01 2017. [cit. 2017-15-01]. Dostupné na internete: http://www.nytimes.com/elections/results/president

UDOH, T. V. (2016). *Online Extremism in Nigeria*. In Journal of European Security and Defense Issues, vol. 7, nr. 2, s. 29 – 33. ISSN 2166-322X

VERIFIED VOTING (2012). *Voting Equipment.* [online]. 9/01 2012. [cit. 2016-10.01]. Dostupné na internete: https://www.verifiedvoting.org/resources/voting-equipment

VOLNER, Š. (2004). K teoretickým a metodologickým aspektom skúmania geopolitického pôsobenia. In: *Medzinárodné vzťahy*, vol. 1, Bratislava, 2004, ISSN 1336-1562

WHITE HOUSE (2011). *International strategy for Cyber Space.* In: Obama White House Archive [online]. 05.2011. [cit. 2017-15-01]. Dostupné na internete: http://sdu.sk/U605cvW1l

WOFFORD, B. (2016). How to Hack an Election in 7 Minutes. In: *Politico* [online]. 05/08 2016. [cit. 2017-16-01]. Dostupné na internete: http://sdu.sk/Ubd201

ZIOLKOWSKI, K. (2013). *Peacetime Regime for State Activities in Cyberspace*. *International Law, International Relations and Diplomacy*, Tallin : NATO CCD COE Publication, 746 s. ISBN 978-9949-9211-8-8