Západočeská univerzita v Plzni

Fakulta filozofická

Bakalářská práce

Wikileaks a USA

Klára Hanušová

Plzeň 2013

Západočeská univerzita v Plzni

Fakulta filozofická

Katedra filozofie

Studijní program Humanitní studia

Studijní obor Humanistika

Bakalářská práce

Wikileaks a Spojené státy americké

Klára Hanušová

Vedoucí práce:

PhDr. Přemysl Rosůlek Ph.D.

Katedra politologie

Fakulta filozofická Západočeské univerzity v Plzni

Plzeň 2013

Prohlašuji, že jsem práci zpracovala samostatně a použila jen uvedených pramenů a literatury.

Plzeň, duben 2013 ……

OBSAH

1 ÚVOD

Tato práce se zabývá činností webové stránky Wikileaks, konkrétně materiály, které přímo souvisejí se zahraniční politikou prosazovanou Spojenými státy americkými. Hledá odpověď na otázku, zda se Wikileaks podařilo přiblížit k naplnění jejího cíle, tedy zvýšení transparentnosti ve vedení politiky.

Jedná se o aktuální téma, neboť stránka jako taková funguje teprve necelých 7 let a její největší počin, uveřejnění rozsáhlého souboru diplomatické korespondence, se datuje k roku 2010. Stránce Wikileaks se podařilo, díky své činnosti, přitáhnout značnou mediální pozornost. Ideologie Wikileaks si získala mnoho příznivců, ale také mnoho odpůrců.

Její, až možná utopická, snaha o svět bez tajemství a bez jednání za zavřenými dveřmi naráží na odpor jak ze strany vládních organizací, tak i ze strany části společnosti. Wikileaks se musela s těmito útoky vyrovnat a byla nucena čelit veškerým následkům, které její činnost přinesla.

Na druhou stranu také Spojené státy americké musely čelit důsledkům, které únik jejich interních informací přinesl. Bylo nutné zaujmout jasný postoj a podniknout konkrétní kroky pro vyrovnání se s tímto novým fenoménem. Wikileaks nejen Spojeným státům americkým, ale i celému světu ukázaly, jak velké jsou nedostatky nejenom státních informačních systémů.

V první kapitole se zaměříme na definici kyberprostoru, v rámci kterého Wikileaks působí. Současně se zaměříme na možná rizika, která s sebou kyberprostor přináší. Konkrétněji zhodnotíme možná rizika z pohledu USA.

Ve druhé kapitole této práce si představíme organizaci Wikileaks, její krátkou historii a cíle, kterými se prezentuje na veřejnosti. Ve stručnosti si představíme materiály, které doposud uveřejnila a o něco podrobněji se zaměříme na její asi nejvýraznější počin. Tím bylo uveřejnění rozsáhlého souboru diplomatických depeší v roce 2010. Díky těmto únikům se dostaly Wikileaks do pozornosti široké veřejnosti a Spojené státy musely veřejně přiznat své selhání v rámci zabezpečení svých informačních toků.

Poslední kapitola této práce se snaží zjistit, zda zveřejněné materiály svou povahou a obsahem mohou znamenat zásadní ohrožení, případně změnit způsob prosazování zahraniční politiky Spojených států. Pokusí se zhodnotit důsledky jak pro Spojené státy, tak i pro samotnou stránku Wikileaks.

2 KYBERPROSTOR A JEHO RIZIKA

2.1 Kyberprostor

Do styku s kyberprostorem se lidé ve vyspělých zemích dostávají prakticky neustále. Do přímé interakce s kyberprostorem se dostáváme například skrze naše mobilní telefony nebo naše počítače. Jako kyberprostor můžeme označit i informační systémy, které používá stát pro své fungování, ale neznámějším kyberprostorem je Internet. Kyberprostor můžeme definovat jako „*infrastrukturu provázaných sítí informačních technologií, která zahrnuje Internet, telekomunikační sítě, počítačové systémy a vložené procesory a řídící jednotky důležitých odvětví.“*[1] (Přeloženo autorem)

Kterýkoli kyberprostor, tedy například Internet, je prostředí vytvořené člověkem. Toto prostředí mu umožňuje rychlý přístup k velkému množství informací. Skládá se za prvé z globálně propojených sítí, hardwaru, softwaru a dat, za druhé se skládá z lidí, kteří vstupují do interakce s těmito sítěmi. Při vývoji byly hlavními požadavky především snadná přístupnost, rozšiřitelnost, vnitřní operativnost a možnost další inovace. Bezpečnost nepatřila mezi hlavní priority. V současné době můžeme pozorovat zvýšenou snahu o zlepšení právě v oblasti zabezpečení. Tento obrat k většímu důrazu na bezpečnost zapříčinil zvyšující se počet útoků v rámci kyberprostoru. Dalšími charakteristickými vlastnostmi kyberprostoru, tedy i Internetu, je jeho dynamičnost, rychlost, relativně neomezené hranice, vnitřní operativnost, přístupnost a rozšiřitelnost. [2] Jedná se o neustále rozvíjející se mechanismus, do kterého každý den vstupuje více a více jednotlivců, a

---

[1] US Executive Office of the President. *Cyberspace Policy Review* [online]. 2009, s. 1 [cit. 15.4.2013]. Dostupné z: http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf

[2] NIELSE, S.C. Pursuing Security in Cyberspace: Strategic and Organizational Challenges. *Orbis,* 2012, 56 (3), s. 337.

také prudce narůstá množství informací, se kterými je možné v rámci Internetu pracovat.

Ovšem i Internet má své hranice. K zajištění přístupu k Internetu potřebujeme vybudovanou infrastrukturu pokrytí, jako jsou kabely nebo síť bezdrátového připojení. Povaha Internetu je sice nadnárodní, ovšem stát může svými zákony fungování Internetu na svém území korigovat. Takovým příkladem může být například cenzura v rámci Internetu v Číně. Internetové prostředí je dynamickým prostředím, které neustále narůstá. Díky již zmíněné dynamičnosti a stále většímu množství uživatelů vzrůstají možnosti jeho využití a případně i zneužití. K tomu, aby došlo k nějaké relativně význačné změně, mnohdy stačí pouze malá skupina uživatelů nebo i pouze zdatný jednotlivec. Díky vzájemné propojenosti a relativně žádným hranicím je možné pracovat velmi rychle. *„Ve srovnání s ostatními, na čase závisejícími systémy, mohou v kyberprostoru nastat dramatické změny v extrémně krátkém čase.“*[3](Přeloženo autorem) Náklady, které jsou s aktivitou na Internetu spojené, jsou relativně malé. Co se dá považovat za asi největší výhodu oproti fungování v reálném světě je, že je zde možné vystupovat anonymně.[4]

Stejně tak jako mají možnost využít všech možností kyberprostoru jednotlivci nebo společnosti, využívají jich také ve značné míře i státy. Ty jich využívají hlavně pro zajištění efektivního a rychlého přístupu k jejich vnitřním databázím a dalším informacím. Tím se značně zvyšuje efektivita jejich fungování. Z toho tedy vyplývá, že existují oblasti kyberprostoru, které, pokud jsou narušené, mohou způsobit závažné riziko pro národní bezpečnost, ekonomiku nebo veřejné zdraví. Mezi hlavní rizikové oblasti patří například voda, elektrická energie, přeprava,

---

[3] OTTIS, R. LORENTS, P. Cyberspace: Definition and Implications. *Proceedings of the International Conference on Information Warfa,* 2010, s. 370.

[4] NIELSE, S.C. Pursuing Security in Cyberspace: Strategic and Organizational Challenges. *Orbis,* 2012, 56 (3), s. 339.

komunikace, bezpečnostní složky nebo bankovnictví. V současné době je totiž téměř veškeré řízení těchto oblastí ovládáno v rámci počítačových systémů. Pokud dojde k jejich ohrožení nebo narušení, dají se očekávat závažné důsledky pro celou společnost. Navíc velké množství z těchto oblastí patří soukromým vlastníkům a záleží tedy hlavně na nich, jakou pozornost věnují zabezpečení svých dat a systémů před možným útokem.[5]

2.2 Možná rizika kyberprostoru z pohledu USA

Vše má ale také svou odvrácenou stránku. Jak se Internet postupně rozrůstal a přibývalo množství připojených uživatelů, začaly se objevovat snahy o zneužití celého systému k nelegálním účelům. Kriminalita si začala z reálného světa hledat cestu do světa kybernetického. Tento problém se stává více a více závažnějším, jak přibývá množství operací, které dříve probíhaly pouze v rámci fyzického světa, ale dnes se dají provést elektronicky prostřednictvím počítače. Jako příklad uveďme placení přes Internet a celkově manipulace s finančními prostředky.

V případě útoků v rámci kyberprostoru je největším problémem čas a včasné zjištění, že k útoku vůbec došlo. Pokud by někdo přišel a násilím se fyzicky vloupal například do kanceláře prezidenta, odkud by odnesl citlivé informace, ihned se zalarmují obranné složky a pachatelé budou rychle dopadeni. Ovšem v případě útoků v rámci kyberprostoru se sofistikovanost a promyšlenost útoků neustále zvyšuje, a tak je dokonce možné, že při nedostatečném zabezpečení informačních systémů si vniknutí do systému nemusí nikdo všimnout.[6] Například v případě zveřejnění diplomatických depeší stránkou Wikileaks v roce 2010

[5] LYNN III, W.F. Defending a New Domain: The Pentagon's Cyberstrategy. *Foreign Affairs*, 2010, 89 (5), s. 98.

[6] NIELSE, S.C. Pursuing Security in Cyberspace: Strategic and Organizational Challenges, *Orbis,* 2012, 56 (3), s. 342.

Spojené státy do poslední chvíle přesně nevěděly, jaké konkrétní dokumenty se Wikileaks podařilo získat a které konkrétní údaje se tedy chystají uveřejnit.

Pokud se zaměříme konkrétně na Spojené státy americké, pak by v případě ohrožení národní bezpečnosti Spojených států za použití útoků skrze kyberprostor mohly reálné důsledky ovlivnit celou řadu dalších zemí. Spojené státy mají sice velice silnou vojenskou sílu, ovšem celý tento systém je závislý ve všech ohledech na informačních systémech.[7] Systém národní digitální infrastruktury ve Spojených státech je z větší části založen na internetovém prostředí. Tento systém není zase tak odolný ani zcela bezpečný, jak by se mohlo zdát.[8] Narušení tohoto systému by mohlo způsobit v nejhorším případě destabilizaci obranných systémů Spojených států.

Jak poukazuje například dokument *Cyberspace Policy Review*, tohoto problému si však odborníci jsou již delší dobu dobře vědomi. Bohužel vzhledem k nedostatečné pozornosti ze strany vlády se tento problém potýkal s nedostatečnou podporou i nedostatečným množstvím poskytnutých finančních prostředků.[9] Spojené státy v současné době nemají jednotlivce nebo subjekt, který by byl plně odpovědný za koordinaci vládních aktivit spojených s bezpečností kyberprostoru. Ovšem právě existence jednoho centrálního mechanismu je v tomto případě základ. Tento subjekt by měl mít podporu prezidenta a dostatečné množství zdrojů, aby mohl efektivně fungovat. Představitelé takového subjektu by pak měli být odpovědni za přípravu návrhů týkajících se národní strategie pro zabezpečení informačních a

---

[7] LYNN III, W.F. Defending a New Domain: The Pentagon's Cyberstrategy. *Foreign Affairs*, 2010, 89 (5), s. 98.

[8] US Executive Office of the President. Cyberspace Policy Review [online]. 2009, s. 1 [cit. 15.4.2013]. Dostupné z: http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf

[9] Tamtéž, s. i.

komunikačních infrastruktur. Tyto návrhy by pak měly být předloženy prezidentovi k posouzení.[10]

Pokud se tedy díváme na kyberprostor jako na nedokonalý systém, který má mezery v zabezpečení, jaká skupina lidí je pro jeho fungování, v rámci možnosti zneužití jeho dat, tou největší hrozbou? Pro běžného uživatele Internetu to jsou převážně lidé tvořící malware, spyware, celkově tedy lidé, kteří se snaží získat naše citlivá data a ta buď zneužít, nebo je prodat. V případě státu a jeho orgánů budou hrozby poněkud odlišné. Pro stát, jako jsou Spojené státy, tvoří hlavní oponenty dobře organizované a financované vojenské nebo výzvědné složky. Proti takto vyvinuté a pokročilé kybernetické síle by v případě jejich útoku neměly Spojené státy vypracovanou dostatečnou obranu svých informačních systémů. V případě vzniku tzv. kyberválky by se tedy systémy Spojených států potýkaly se značnými problémy. Je ovšem nepravděpodobné, že by některé státy vstoupily do takovéto války proti Spojeným státům, neboť rizika jsou příliš veliká a také by bylo nutné počítat s velmi razantním odvetným protiútokem, který by následně Spojené státy proti takovému útočníkovi zahájily.[11]

Když tedy odhlédneme od relativně nepravděpodobné možnosti kyberválky mezi státy v rámci kyberprostoru, zůstávají nám pouze útoky ze strany méně silných a technicky vybavených jednotlivců nebo hackerských skupin. V posledních letech se stal velmi častým způsobem útoku na webové stránky útok typu DDoS.[12] V rámci těchto útoků je vysíláno velké množství požadavků na DNS.[13] Server, ve snaze zodpovědět veškeré tyto požadavky, pod jejich návalem zkolabuje, a

[10] US Executive Office of the President. *Cyberspace Policy Review* [online]. 2009, s. 7 -9. [cit. 15.4.2013]. Dostupné z: http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf,

[11] CSSI. *Cybersecurity two years later* [online]. 2011, s. 2 [cit. 15.4.2013]. Dostupné z: http://csis.org/files/publication/110128_Lewis_CybersecurityTwoYearsLater_Web.pdf

[12] Distributed Denial of Service

[13] Domain Name Server, například: ff.zcu.cz

webová stránka se tak stane pro uživatele Internetu dočasně nedostupná. Takový způsob útoku použila například skupina aktivistů známa jako Anonymous jako odpověď na předchozí DDoS útok proti stránce Wikileaks. Útok byl veden nejen proti původním útočníkům na stránky Wikileaks, ale také proti společnostem jako MasterCard nebo PayPal, které v té době znepřístupnily své služby pro Wikileaks, a ty se tak ocitly bez finančních prostředků.[14]

Ovšem ani útoky DDoS ani činnost stránky Wikileaks nejsou z pohledu Spojených států válečným aktem. Pro Spojené státy tu existují daleko větší a závažnější hrozby jako špionáž a kyberkriminalita. Špionáž v rámci kyberprostoru mohou páchat lidé zaměstnaní výzvědnou službou jiného státu, ale také to mohou být jednotlivci, dělající to pro svůj vlastní profit. Ani tyto hrozby se ale nedají označit jako akty války, přesto ovšem dokáží napáchat velké škody. [15]

Nejenom Spojené státy, ale stejně tak i všechny ostatní státy musí v době moderních počítačových technologií čelit více a více sofistikovaným útokům na jejich interní počítačové systémy. Je to oblast neustálého dynamického vývoje, která si bude do budoucna vyžadovat daleko více pozornosti. Politika Spojených států nebyla schopná udržet krok s vývojem technologií. Důvodem, proč implementace nových pohledů na kyberprostor je tak pomalá, je převládající přístup k samotnému Internetu. Internet je vnímán jako svobodný prostor, poskytující možnosti ke vzniku inovací a spolupráce. Zásahy se strany států by měly být minimální, neboť se předpokládá, že Internet je schopen se s problémy vypořádat sám. Tento přístup ale spíš než nové inovace podpořil vznik aktivit, které se snaží využít nedostatečné

[14] GIRALTE, L.C. et al., Detecting denial of service by modelling web-server behaviour. *Computers and Electrical Engineering*, 2012, s. 2.

[15] CSSI. *Cybersecurity two years later* [online]. 2011, s. 2 [cit. 15.4.2013]. Dostupné z: http://csis.org/files/publication/110128_Lewis_CybersecurityTwoYearsLater_Web.pdf

ochrany Internetu ve svůj prospěch.[16] Nejenom Spojené státy se musí přizpůsobit nastalé situaci a změnit svůj dosavadní přístup. Je třeba zvýšit informovanost a vzdělanost občanů a společnosti, aby si byla vědoma rizik online aktivit. Je třeba podporovat klíčové vzdělávací programy, výzkum a vývoj, aby bylo možné efektivně čelit dynamicky se vyvíjejícím možnostem Internetu.[17]

Tato kapitola se snažila ukázat, že i přes veškerou mediální pozornost, kterou Wikileaks vzbudila, není jejich činnost ve skutečnosti tak závažným bezpečnostním problémem, jako spíše problémem politickým. Spojené státy jsou si vědomy svých nedostatků v zabezpečení svých elektronických databází a snaží se na tomto problému pracovat. Je pravděpodobné, že díky Wikileaks bude tomuto problému věnována ještě větší pozornost než v minulosti, ale skutečnou hrozbou jsou daleko propracovanější skupiny.

[16] *Cybersecurity two years later,* Center for Strategic and International Studies, 2011, s. 3-4.

[17] US Executive Office of the President. *Cyberspace Policy Review* [online]. 2009, s. 13-14. [cit. 15.4.2013]. Dostupné z: http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf,

3 MASOVÁ MÉDIA A WIKILEAKS

3.1 Masová média v prostředí Internetu

V současné moderní společnosti se do kontaktu s masovými médii dostáváme prakticky každý den. Posloucháme rádio při snídani, čteme noviny na cestě autobusem do práce a po návratu z práce si sedneme k našim počítačům nebo televizorům. Vliv masových médií na současnou společnost i politiku je tak nepopiratelný. Mezi masová média řadíme *„periodický tisk (…) a rozhlasové a televizní vysílání, ale stále častěji také veřejně dostupná sdělení na Internetu, ať již mají povahu výstupu výrobní organizace (např. zpravodajské portály), akumulace uživatelských příspěvků (servery typu YouTube), individuálních počinů (např. autorské blogy), popř. kontaktních sebeprezentačních nástěnek (Facebook). Přes velkou tvarovou rozmanitost mají masová média společné to, že jsou obsahově univerzální, mají velkou popularitu a jsou v zásadě veřejné povahy."*[18]

Díky médiím zprostředkujícím nám informace o dění ve světě si utváříme své názory a postoje. Z tohoto důvodu jsme do jisté míry ovlivňováni tím, co a jak nám média prezentují. Míra a způsob ovlivnění záleží na formě, kterou nám je zpráva prezentována, neboť každá forma, ať už se jedná o tisk nebo televizní zpravodajství, má svá specifika.[19]

Současná masová média nebo jinak masmédia zprostředkovávají nepřeberné množství zpráv a informací, které nejsou omezeny pouze na zemi, v rámci které dané masmédium pracuje. Zprávy o událostech mohou být odvysílány chvíli po tom, co se skutečně odehrály, ať už se

[18] JIRÁK, J., KÖPPLOVÁ, B. *Masová média,* 2009*,* s. 21.

[19] BIRSEN, H. Internet Journalism and Journalistic Ethics: Working Conditions and Qualifications of Journalists in the New Media. *Journal of US-China Public Administration,* 2011, 8(2), s. 230.

staly na domácí půdě nebo třeba v Austrálii. Vzhledem k souboji o co nejaktuálnější zprávy musí být proto výsledné sdělení krátké a stručné. Už zde není čas na důkladné vysvětlení a případné zhodnocení události a možných důsledků. Na čtenáře či diváka se tak ze všech stran neustále valí nové a nové útržkovité zprávy, které mu ve výsledku toho ale příliš neřeknou a zanechají ho více zmateného než informovaného.[20]

K již tradičním médiím, poskytujícím informace pro širokou veřejnost, jako tisk, televize a rozhlas přibyl v současné době Internet. Internet umožňuje rychlý přenos informací a okamžité zobrazení kdekoliv, kde mají lidé necenzurovaný přístup k internetovému připojení. Neexistuje zde žádné omezení, co se týče rozsahu nebo tématu. Také způsob uchování dat je zde daleko jednodušší a není spojen s tak vysokými finančními náklady. V rámci jednoho serveru si můžou lidé přečíst zprávy rok i pět let zpětně a nemusí přitom opustit pohodlí svého domova. Neustále se také pracuje na digitalizaci starších dokumentů a jejich online zpřístupňování široké veřejnosti. Internet disponuje velkou mírou interaktivity, která se projevuje například možností pohybování se mezi jednotlivými webovými stránkami za použití hypertextových odkazů. Hypertext umožňuje přiblížit kontext nebo rozvést další témata, skrze odkazování na jiné stránky nebo místa v textu. Takovou možnost tištěná média nikdy mít nebudou.

Na druhou stranu je v případě online masmédií potřeba pracovat daleko rychleji než v případě ostatních médií. Článek je potřeba publikovat dříve než konkurence, nehledě na denní nebo noční dobu. To s sebou přináší i rizika, neboť není dostatek času na úpravy, korekce, ověřování. *„Kontrola obsahu a kvality zpráv se, jak se zdá, vymyká*

[20] NEWTON, K. Mass Media Effects: Mobilization or Media Malaise?. *British Journal of Political Science*, 1999, 29(4), s. 578.

editorům z rukou.“[21] Internet je prostředí, kde může každý přispívat a zároveň zůstat anonymní, nebo se vydávat za někoho úplně jiného. Zásady používané v dosud známé žurnalistice se mění.[22]

Ovšem i přes odlišné podmínky, které Internet poskytuje, stále tu musí být nějaká pravidla, kterými by se měl žurnalista při své práci řídit. Měl by být schopen využít možností, které Internet poskytuje pro zlepšení své práce. Možnost rychlého ověřování informací a větší množství použitelných zdrojů, to vše by mohlo vést ke zlepšení informovanosti široké veřejnosti a větší míře transparentnosti.

Právě vyšší transparentnosti se snaží dosáhnout internetová stránka Wikileaks. *„Transparentnost v žurnalistice se často spojuje s důvěryhodností a demokratičností.“* [23] (Přeloženo autorem) Pojem transparentnost je poměrně rozsáhlý, ovšem jako velmi obecnou definici můžeme použít tu, která transparentnost definuje jako snahu o ukázání, kdo udělal co a proč. V rámci celého procesu utváření zpráv je ovšem důležité najít rovnováhu mezi naprostou transparentností, žurnalistickou etikou a zároveň je nutné nést odpovědnost za výsledné sdělení.[24]

Vedle transparentnosti se v souvislosti s masovými médii také často mluví o tzv. funkci „watchdog“ u nás překládané jako „hlídací pes demokracie“. „‚*Watchdog‘ proces nejčastěji obsahuje kombinaci veřejných a neveřejných informací společně s analýzou, která se snaží*

[21] DEMIR, M. Importance of Ethic, Credibility and Reliability in Online Journalism. *European Journal of Social Sciences*, 2011, 24(4), s. 540.

[22] DEMIR, M. Importance of Ethic, Credibility and Reliability in Online Journalism. *European Journal of Social Sciences*, 2011, 24(4), s. 540.

[23] GROENHARTA, H.P., BARDOELB, J.L.H. Conceiving the transparency of journalism: Moving towards a new media accountability currency. *Studies in Communication Sciences,* 2012, 12(1), s. 6.

[24] GROENHARTA, H.P., BARDOELB, J.L.H. Conceiving the transparency of journalism: Moving towards a new media accountability currency. *Studies in Communication Sciences,* 2012, 12(1), s. 7.

*zdůraznit potencionální problémy.“ (*Přeloženo autorem)[25] K lidem se tak dostanou i informace, jejichž zveřejnění nemusí být některým subjektům zcela příjemné.

Oba tyto prvky skutečně můžeme v práci Wikileaks najít. Jak na svých stránkách uvádějí, je jejich práce založena na obraně práva svobodného projevu, práva na vlastní názor a jeho vyjadřování.[26]

3.2 Wikileaks

Wikileaks je internetová doména, která byla založena v roce 2006. Julian Assange, zastávající pozici mluvčího, je pro veřejnost hlavní osobou spojenou se jménem Wikileaks, ale na provozu této internetové stránky se vedle něj podílí úzká skupina nadšenců a počítačových expertů, kteří mají na starosti běžný chod stránky a hlavní práci na přijatých materiálech. Jména těchto lidí ale nejsou většinou známa. Jednu z výjimek tvoří Daniel Domscheit-Berg, který dříve působil jako mluvčí Wikileaks v Evropě, zvláště pak v Německu.[27] Správu stránek má tedy na starosti omezená skupina lidí, ale současně s nimi se na celém projektu Wikileaks podílí mnoho jiných nadšenců a otevřených podporovatelů projektu. Podílet se mohou například tak, že na svých vlastních webových stránkách provozují tzv. „mirrors“, tedy úplné kopie původního obsahu stránky wikileaks.com. Tyto kopie byly zvláště důležité v období, kdy byly kompletně znepřístupněny oficiální stránky Wikileaks. K tomu došlo krátce po zveřejnění souboru diplomatických depeší Spojených státu, a v této době byly také zmraženy účty Wikileaks, na které mohli lidé přispívat na běžný provoz stránek.[28]

---

[25] MILLER, G.S. The Press as a Watchdog for Accounting Fraud. *Journal of Accounting Research,* 2006, 44(5), s. 1006.

[26] About. *What is Wikileaks?* [online]. Wikileaks. [cit. 15.4.2013]. Dostupné z: http://wikileaks.org/About.html

[27] ROSENTHAL, J. Dear Julian. *World Affairs*, 2011,174(4), s. 86-87.

[28] LAST, J. V. Can You Plug a WikiLeak?. *The Weekly Standard*, 2010, 16(15), s. 13-14.

V současné době je již ovšem znovu možné na provoz stránek přispívat. Mezi společnostmi umožňující online platbu je i společnost PayPal, která v prosinci 2010 odmítla nadále s Wikileaks spolupracovat, a tím znemožnila lidem využít služby PayPal k posílání příspěvků na účty Wikileaks. [29]

Wikileaks samotná se definuje jako nezisková organizace s cílem přinášet důležité informace veřejnosti. Společnost má dle ní právo na informace o činnosti její vlády, aby si tak mohla utvořit svůj vlastní názor a věděla, co její volení zástupci dělají jejím jménem. Za základní prvek fungování Wikileaks je považována možnost poskytnutí anonymního způsobu, jak informace o podezřelém jednání dát k dispozici ke zveřejnění. Informace se k pracovníkům Wikileaks mají možnost dostat skrze zaslání do tzv. drop boxu, který funguje zcela anonymně.

Za další základní premisu svého fungování je pro Wikileaks to, že získané materiály důkladně ověří a podrobí analýze. Je nezbytné, aby bylo možné ověřit pravost obdrženého dokumentu a informací v něm obsažených. Po obdržení materiálu a jeho ověření se ke slovu dostávají pracovníci Wikileaks. Žurnalisté Wikileaks sice napíší článek o daném dokumentu, přesto ale považují za nejdůležitější dát na své webové stránky k dispozici originální neupravený dokument, aby si každý mohl udělat vlastní názor na daný problém. [30]

Vzhledem k velkému rozsahu některých obdržených dokumentů Wikileaks časem přistoupila ke spolupráci s několika zpravodajskými deníky. Díky této spolupráci mohou využít jejich prestiž, mediální vliv a hlavně jejich personální kapacity pro zpracování velkých datových souborů. Tyto deníky tedy Wikileaks pomáhají se zpracováním dat,

[29] ROBERTS, A. Wikileaks: The Illusion Of Transparency. *International Review of Administrative Sciences*, 2012, 78(2), s. 7.

[30] About. *What is Wikileaks?* [online]. Wikileaks. [cit. 15.4.2013]. Dostupné z: http://wikileaks.org/About.html

neboť samotná Wikileaks by toho nebyla tak efektivně schopna. Tuto mediální síť tvoří především *Der Spiegel, Guardian, el País a New York Times*.[31] Nejvíce znatelná byla tato spolupráce při přípravě na uveřejnění diplomatických depeší v roce 2010. Deníky poskytly jak technickou asistenci, tak i odborné znalosti svých žurnalistů při zpracování a interpretaci materiálů. Také se staly jakýmsi pojítkem mezi Wikileaks a vládními představiteli.[32]

3.2.1 Dosud zveřejněné materiály

Do pozornosti široké veřejnosti se Wikileaks dostala poměrně nedávno. V dubnu roku 2010 bylo na stránkách Wikileaks uveřejněno video nazvané „*Collateral murder*". Jedná se o videozáznam z vrtulníku Apache spadající pod vojenské jednotky Spojených států. Dokument byl pořízen roku 2007 v Bagdádu. Záznam zachycuje pohled střelce z vrtulníku a jeho radiový rozhovor. Během této akce zahynulo dvanáct lidí včetně dvou zaměstnanců zpravodajské agentury Reuters.[33] Mnoho dalších lidí bylo zraněno a mezi nimi bylo i několik dětí. Na webu Wikileaks je původní verze, která má přibližně čtyřicet minut, a také zkrácená, přibližně osmnáctiminutová, verze. Na videu je patrný kameraman, jehož kamera byla vojáky identifikovaná jako zbraň RPG, což je ruční protitankový granát. Po rozhovoru několika vojáků dojdou k názoru, že je potřeba zasáhnout. Začnou střílet do skupinky lidí před nimi, mezi nimiž je i kameraman identifikovaný pracovníky Wikileaks ve zkrácené nahrávce jako Namir Noor-Edeen. Ten se po prvním zásahu snaží uniknout, ale je na něj znovu střílено. V této chvíli je z vrtulníku hlášeno, že se na ulici nachází přibližně 8 těl. Po chvíli se ukáže, že jeden ze zaměstnanců Reuters je naživu a snaží se zraněný dostat

[31] CULL, N.J. WikiLeaks, public diplomacy 2.0 and the state of digital public diplomacy. *Place Branding & Public Diplomacy,* 2011, 7(1), s. 2.

[32] ROBERTS, A. Wikileaks: The Illusion Of Transparency. *Forthcoming in International Review of Administrative Sciences*, 2012, 78(2), s. 13.

[33] ROBERTS, A. The Wikileaks Illusion. *The Wilson Quarterly*, 2011, 35(3), s. 16.

z ulice. Vojáci nyní řeší, zda mají znovu střílet. Po nějaké době se objeví dodávka, která se snaží naložit zraněného reportéra a dostat ho do bezpečí. Ovšem vojáci se rozhodnou zasáhnout a začnou do dodávky střílet. Další střih ukazuje příjezd tanků na místo zásahu. Ze záběru je patrné, že minimálně jeden z tanků přejel přes mrtvé tělo.[34] Krátce po zveřejnění videa vojenského zásahu v Bagdádu byly publikovány materiály vztahující se k válce v Iráku a v Afghánistánu.

Mezi dříve zveřejněné informace se řadí seznam členů krajně pravicové Britské národní rady včetně jmen, adres a věku v roce 2008.

Takzvané *Gitmo files* se zabývají úniky o věznici Guantánamo, která byla zřízena v roce 2002 na námořní základně na Kubě jako speciální zajatecký tábor. Tento zajatecký tábor byl původně určen pro zajatce z Afghánistánu. Vězni neměli statut válečného zajatce a díky umístění se na ně nevztahovalo ani vnitrostátní právo USA.[35] Záznamy zveřejněné Wikileaks se vztahují k období mezi lety 2002 až 2008.

V nedávné době se na stránkách Wikileaks začaly objevovat informace označené jako „*The Global Intelligence Files*“. Tyto soubory obsahují emailovou korespondenci, která by měla obsahovat důkazy o krocích, které Spojené státy vedou proti Julianovi Assangeovi a celkově proti celé organizaci Wikileaks. Jedná se o informace uniklé ze zpravodajské agentury Stratfor. Informace se měly k Wikileaks dostat díky útoku hnutí Anonymous na počítače agentury. Agentura Statfor již dopředu zdůraznila, že se k uniklým emailovým korespondencím nebude vyjadřovat.[36]

---

[34] Obě videa jsou přístupná online na collateralmurder.com.

[35] KREJČÍ, O. *Zahraniční politika USA*, 2009, s. 307.

[36] BBC News US & Canada. *Wikileaks publishes confidential emails from Stratfor* [online]. BBC, 2013. Poslední změna 27.2.2012 20:50. [cit. 15.4.2013]. Dostupné z: http://www.bbc.co.uk/news/world-us-canada-17176602

Rok 2010 se stal pro Wikileaks rokem velkého úspěchu, ale i rokem velkých ztrát. Asi nejzásadnější ránou pro Wikileaks byla skutečnost, že krátce po zveřejnění diplomatických depeší Spojených států v roce 2010 společnosti jako Amazon.com nebo PayPal znepřístupnily pro Wikileaks své služby. Následně byl společností EveryDNS.net smazán DNS záznam Wikileaks, což mělo za následek nepřístupnost oficiálních webových stránek.[37]

Tento pokus o umlčení Wikileaks ovšem velmi silně rozbouřil vody Internetu, neboť snaha cokoliv cenzurovat jen zvýšila zájem o cenzurované informace. Během několika dní uživatelé začali šířit obsah Wikileaks prostřednictvím klonů původní stránky již zmíněných „mirrors“. Wikileaks byly ale stále zmraženy její bankovní účty. Wikileaks tedy chyběly finanční prostředky k zajištění byť jen základního provozu domény a bez finančních prostředků se ocitl i sám Assange.

Reakcí na tyto skutečnosti byla série masivních útoků na stránky Mastercard či Paypal. Aktivně se zde projevila skupina aktivistů známá pod názvem Anonymous, která v současné době platí za synonymum hackerských útoků a celkově boji v rámci Internetu. Ovšem tato skupina je spíše označení různorodé skupiny lidí, fungujících v internetovém prostoru. Anonymous, nemají žádnou pevnou strukturu ani organizaci. Je to název zastřešující ty, kteří se chtějí anonymně projevit.

---

[37] BBC News US & Canada. *PayPal cuts Wikileaks access for donations* [online]. BBC, 2013. Poslední změna 4.12.2010 09:33. [cit. 15.4.2013]. Dostupné z: http://www.bbc.co.uk/news/world-us-canada-11917891

3.2.2 Diplomatické depeše

Na konci listopadu roku 2010 se na stránkách Wikileaks začaly postupně objevovat diplomatické depeše Spojených států. Tyto informace měla Wikileaks, dle současného vyšetřování, získat pravděpodobně od analytika americké armády Bradley Manninga. Bradley Manning čelí v současné době obvinění z neoprávněného nakládání s utajovanými informacemi.[38]

Podle oficiálních stránek Wikileaks jde celkem o soubor 251 287 diplomatických depeší rozdělených podle označení na tajné, důvěrné a neklasifikované. Depeší klasifikovaných jako tajné je ale z celkového počtu pouze necelých 16 tisíc.[39] Před samotným zveřejněním depeší na oficiálních stránkách Wikileaks byly diplomatické depeše poskytnuty spřízněným deníkům jako *The New York Times, Guardian* nebo *Der Spiegel*. Důležité je ovšem poznamenat, že celkové množství uniklých informací příliš neznamená. I tak velký rozsah informací je jen zlomkem dat, které si jednotlivé složky Spojených států posílají denně skrze jiné informační kanály.[40]

Zásadním problémem celého uniklého materiálu je fakt, že je celý soubor natolik obsáhlý, že aby ho širší veřejnost byla vůbec schopná pochopit, je zapotřebí odbornějšího a komplexnější zpracování. Surové informace v tak velkém rozsahu toho příliš neřeknou a není možné je proto jednoduše číst. Bez znalosti kontextu nebo politické situace dané země nejsou tyto informace příliš užitečné. Navíc se zde často vyskytují

[38] HQ, USD-Center. *Soldier faces criminal charges* [online]. 2010. [cit. 24.4.2012]. Dostupné z: http://www.cbsnews.com/htdocs/pdf/ManningPreferralofCharges.pdf?tag=contentMain;contentBody

[39] Secret US Embassy Cables [online].*Wikileaks* [cit. 2012-04-24]. Dostupné z: http://wikileaks.org/cablegate.html#

[40] ROBERTS, A. The Wikileaks Illusion. *The Wilson Quarterly*, 2011, 35(3), s. 18.

zkratky, které nejsou často vůbec vysvětleny, jelikož se počítá s tím, že je adresát dobře zná. Rozsah jednotlivých zpráv se pohybuje od několika odstavců až ke kompletním zápisům jednotlivých rozhovorů při jednáních. Každá depeše má přidělené své identifikační číslo, zařazení, autora klasifikace, důvody pro přidělení dané klasifikace, určení místa odeslání a seznam institucí, na které byla daná zpráva zaslána.

Nejstarší depeší je depeše z ambasády v Buenos Aires z roku 1966 a jedná se o zprávu o rozšíření zón pro rybolov. Poslední informace se váží k datu 28. února roku 2010.

Pro účely této práce je z celkového souboru informací vybrán pouze segment depeší označených jako tajné a odeslaných přímo orgány Spojených států svým zahraničním zastupitelstvím po teroristickém útoku 11. září 2001. Datum bylo vybráno vzhledem k významnému vlivu této události na zahraniční politiku Spojených států za vlády prezidenta George Bushe. Zpráva vztahující se k této tragické události byla odeslána hned následující den, tedy 12. září, a varovala před možnými dalšími útoky, neboť čtyři útoky z 11. září měly být podle informací Spojených států pouze prvními z řady až třiceti možných útoků na zájmy USA. Dále zpráva shrnuje reakce ze strany zahraničních partnerů a informuje o dočasném omezování působení některých ambasád v důsledku hrozících útoků.[41]

Téměř většina všech následujících depeší se týká otázky boje proti terorismu. Jedna z nich byla přímo adresována vybraným ambasádám a obsahovala několik hlavních bodů, na které se bude USA snažit v rámci svého tažení proti terorismu zaměřit. Jedná se hlavně o zničení sítě teroristické organizace al-Kájda, zajištění situace v Afghánistánu a jeho následná stabilizace po zlikvidování sítě Taliban. V

[41] Cablegate. *Tf United States September Attack Situation Report* [online databáze]. Wikileaks, 2011. Poslední změna 8.9.2011. [cit. 29.52012]. Dostupné z: http://www.cablegatesearch.net/cable.php?id=01STATE157224

rámci stabilizace USA nastiňuje svou představu, do jaké míry je ochotná zasahovat či naopak nezasahovat do ustanovování nového systému ve státě. Dále také stanovuje, do jaké míry jsou Spojené státy ochotny se podílet na ekonomické rekonstrukci a humanitární pomoci v rámci země. V závěru také prosí adresáty, aby vyjádřili svůj názor na danou problematiku, a vyzývá k dialogu na dané téma. [42]

Mezi dalšími tématy depeší se objevuje i zájem o jednání Evropské unie, které se zabývalo teroristickými skupinami, jako je Hamas a Hizballáh. Tyto zprávy jsou ve své zásadě informační a vedle informací o jednání obsahovaly také základní informace o těchto teroristických skupinách.

Vedle zpráv týkajících se Afghánistánu věnovala USA značnou pozornost aktu o nešíření nukleárních zbraní mezi Sýrií a Iránem (ISNA). V souladu s ustanovením tohoto aktu USA stanovuje sankce pro určené skupiny či jednotlivce, pakliže dojde k vypomáhání či poskytování materiálu na vývoj nukleárních zbraní ze strany jedinců či skupin působících v rámci jiného státu. Podle uvedených zpráv USA v roce 2006 informovala státy o celkem sedmi případech uvalení sankcí. Další rok se pak jednalo celkem o pět dalších případů. Tyto sankce se vztahovaly pouze na danou osobu či skupinu a netýkaly se tedy žádné z vlád států, v rámci které jedinec či skupina působili.

V roce 2007 se převážná většina diplomatických depeší označených jako tajné týkala právě prošetřování a zkoumání aktivit, které by mohly směřovat k podpoře íránského nebo syrského raketového programu. Pozornost Spojené státy vedle toho také věnovaly finančním

[42] Cablegate. *Afghanistan's Future - Next Steps* [online databáze]. Wikileaks, 2011. Poslední změna 8.9.2011. [cit. 29.52012]. Dostupné z: http://www.cablegatesearch.net/cable.php?id=01STATE192153

transakcím Iránu, jež by mohly sloužit jako podpora financování v oblasti zbrojení.[43]

Asi nejdůležitější zemí, skrze kterou se podle informací získaných Spojenými státy mohl do Iránu dostávat potřebný materiál pro výrobu zbraní, byla Čína. Spojené státy se domnívaly, že skrze území Číny putoval materiál z Jižní Koreje do Iránu. Vzhledem k závažnosti tohoto problému tedy Spojené státy prováděly intenzivní jednání s Čínou. Jak vypovídá zpráva z listopadu 2007, prezident Bush tuto problematiku projednával s čínským prezidentem v rámci summitu APEC a žádal o prošetření této, pro Spojené státy zvláště závažné, problematiky ze strany Číny.[44]

V roce 2008 se kromě všech předchozích témat depeše věnují válce v Jižní Osetii, v rámci které proti sobě stála gruzínská armáda a armádní jednotky Jižní Osetie. Tyto jednotky Jižní Osetie se snažily o odtržení svého území od Gruzie. Zvláštní pozornost pak Spojené státy věnovaly informacím vztahujícím se k zásahům ze strany Ruska do tohoto konfliktu. Ruské armádní jednotky operovaly na území Gruzie a právě jejich aktivitou a pohybem se diplomatické depeše zabývají nejvíce.

V souvislosti s Českou republikou se objevuje pouze několik málo depeší, z nichž se většina týká monitorovacího programu BlueLantern,

[43] Cablegate. *Ongoing Proliferation Finance Activities By Iran And North Korea* [online databáze]. Wikileaks, 2011. Poslední změna 8.9.2011. [cit. 29.5.2012]. Dostupné z: http://www.cablegatesearch.net/cable.php?id=07STATE114443.

[44] Cablegate. *Post Requested To Follow Up On Ongoing Matters Of Proliferation Concern Raised At Apec By President Bush* [online databáze]. Wikileaks, 2011. Poslední změna 8.9.2011. [cit. 29.5.2012]. Dostupné z: http://www.cablegatesearch.net/cable.php?id=07STATE152317.

jehož úkolem je sledování prodeje a ověřování konečného uživatele materiálu vyskytujícího se na tzv. muničním listu (USML).[45]

Kromě depeší označených jako tajné, které se vztahují ke sledování zbrojního programu zemí jako je Pákistán, Irán nebo Sýrie, jsou dále veřejnosti k dispozici i zprávy o dalších nepříliš závažných skutečnostech. Pokud není zpráva čistě informativní, často v ní bývá část označená jako „ACTION REQUEST“. V této části zprávy je jasně specifikováno, jakých ambasád se tento požadavek týká a co se po nich požaduje. Z převážné většiny jde o informování vládních autorit přijímajícího státu a někdy také o vyjádření jejich stanoviska k danému problému. V jiných případech chce USA informovat své zahraniční partnery o výsledcích jednání, jako je tomu například ve zprávě z prosince 2008.[46] Tato zpráva požaduje předání informací z jednání mezi USA a Ruskem v rámci dohody CFE.[47]

V roce 2009 se kromě témat vztahujících se k zásobování rizikových zemí materiálem na výrobu zbraní, objevuje problematika Severní Koreje. 5. dubna 2009 totiž Severní Korea vypálila raketu TD-2, která přešla přes území Japonska a poté přistála v Japonském moři. V této depeši Spojené státy jasně deklarují, že tento akt považují za porušení rozhodnutí Rady bezpečnosti OSN 1718. Spojené státy byly jednáním Severní Koreje zneklidněny, přestože to bylo ze strany Severní Koreje prezentováno jako pouhé vypuštění satelitu. Důvodem k tomuto zneklidnění je fakt, že vybavení nutné k takovému vypuštění je prakticky totožné s vybavením potřebným k vypuštění raketových zbraní. USA

[45] US Department of State. Blue Lantern Program. [online]. US Department of State, 2012. [cit. 29.5.2012]. Dostupné z: http://exportcontrol.org/library/conferences/1379/STITZIEL_--_Blue_Lantern_PPT_for_Bucharest_Conference_Mar_06.pdf

[46] Cablegate. *Action Request: Readout Of Fried-antonov Discussion On Cfe* [online databáze]. Wikileaks, 2011. Poslední změna 8.9.2011. [cit. 25.6.2012]. Dostupné z: http://www.cablegatesearch.net/cable.php?id=08STATE133419

[47] Conventional Armed Forces in Europe.

vznáší požadavek na Severní Koreu, aby se v budoucnu zdržela podobných provokativních akcí. Od adresátů této depeše Spojené státy požadují jasné stanovisko přijímajícího státu k této otázce. Jako příklad slouží přiložené stanovisko prezidenta České republiky z 5. dubna 2009, ve kterém prezident vyjadřuje souhlas s tím, že akt Severní Koreje byl jasným porušením stanoviska Rady bezpečnosti OSN 1718. Severní Korea je vyzývána k opuštění své snahy o sestavení zbraní hromadného ničení a dodržování svých mezinárodních závazků a povinností.[48]

V další části této zprávy se USA obrací jen na své vybrané zastupitelské orgány ve městech Tokio, Moskva, Soul a Peking. Pro ně stanovuje základní body, které se mají objevit v jejich případných veřejných prohlášeních, a odpovědi na možné otázky ze strany tisku.

Zároveň se v roce 2009 věnuje USA intenzivním jednáním s Ruskem ohledně podepsání nové dohody START.[49] Rozsáhlé datové zprávy obsahují informace o základních termínech užitých ve smlouvě, průběh jednání obou stran, programy plánovaných setkání a také různé návrhy verzí putujících mezi USA a Ruskem.

Za jednu ze zásadních informací z roku 2009 můžeme považovat depeše ukazující snahu Spojených států amerických o špionáž v rámci Organizace spojených národů. V této zprávě se vyzývá ke shromažďování informací o strategických osobách.[50]

Celá databáze uniklých materiálů končí datem 28. únor 2010, tedy více jak půl rok před uveřejněním materiálů. Převážná část z nich se týká sledování možných hrozeb ze stran států jako je Irán, Pákistán,

[48] Cablegate. *Response To North Korean Taepo-dong 2 Launch* [online databáze]. Wikileaks, 2011. Poslední změna 8.9.2011. [cit. 25.6.2012]. Dostupné z: http://www.cablegatesearch.net/cable.php?id=09STATE33031

[49] Strategic Arms Reduction Treaty.

[50] Cablegate. *Reporting and collection needs: the United Nations* [online databáze]. Wikileaks, 2011. Poslední změna 8.9.2011. [cit. 25.6.2012]. Dostupné z: http://cablegate.wikileaks.org/cable/2009/07/09STATE80163.html

Severní Korea nebo Sýrie. Podle uvedených informací je patrné, jak velkou energii věnují Spojené státy sledování pohybu nebezpečného materiálu a látek, které by mohly sloužit k vývoji a výrobě zbraní hromadného ničení. USA ve zprávách žádají státy, v rámci kterých se rizikový obchod nebo pohyb materiálu uskutečňuje, aby danou situaci prošetřily a poté informovaly o zjištěných skutečnostech. S tím souvisí také v depeších často opakovaný termín ‚*Blue Lantern.* ‚*Blue Lantern* je projekt, v rámci kterého Spojené státy dohlížejí na vojenský materiál prodaný Spojenými státy. U prodaného vojenského materiálu zkoumají, zda neskončil v nepovolaných rukou a nemůže být využit proti Spojeným státům nebo jejich zájmům v zahraničí.

Mimo těchto témat se objevuje celá řada jiných, která ale bez kontextu nemají velký význam. Veřejnost sice bude rozumět zprávě informující o nastalé kolizi mezi soukromým komunikačním satelitem *Iridium – 33* a tzv. „mrtvým“ ruským vojenským komunikačním satelitem *Cosmos 2251*[51], ale žádné velké závěry z této zprávy není možné vyvodit.

Není zde ani žádný znatelný předěl mezi obdobím vlády prezidenta Bushe a jeho nástupcem Barackem Obamou. Stále se tu velká pozornost věnuje problematice vývoje zbraní ve státech jako Irán nebo Sýrie. Rozdílem oproti dřívější administrativě prezidenta Bushe můžeme zaznamenat ale v tom, že probíhají daleko častější jednání ze strany ministryně zahraničních věcí Spojených států Hillary Clintonové s jejími zahraničními protějšky. Zprávy o proběhnutých jednáních jsou daleko častější, než tomu bylo za působení předchozích dvou ministrů Colina Powella a Condoleezy Riceové. Tuto změnu můžeme přisuzovat

[51] Cablegate. *U.s. And Russian Comm Satellite Collision*. [online databáze]. Wikileaks, 2011. Poslední změna 8.9.2011. [cit. 25.6.2012]. Dostupné z: http://www.cablegatesearch.net/cable.php?id=09STATE12945.

rozdílnému přístupu Baracka Obamy a jeho administrativy vůči svým zahraničním partnerům a většímu důrazu na dialog.

4 USA A WIKILEAKS

4.1 Výsledek pro USA

Nedá se říci, že veškeré činnosti a veškeré dokumenty, které Wikileaks na svých stránkách zveřejňují, se týkají výhradně Spojených států amerických. Pravdou ale zůstává, že většina pro Wikileaks nejzásadnějších úniků, díky kterým se dostaly do širokého povědomí společnosti, je spojována právě s informacemi souvisejícími s činností Spojených států v zahraničí, ať už se jedná o zveřejněné informace o válce v Iráku nebo soubor diplomatických depeší. Mohou tedy vyvstat pochybnosti o nestrannosti nebo případné zaujatosti ze strany Wikileaks vůči tak silnému hráči na poli mezinárodní politiky, jakým jsou Spojené státy americké. Na druhou stranu ovšem je třeba si připomenout, že i světová zpravodajství se často zaměřují na události spojené se Spojenými státy nebo jinými významnými světovými hráči na poli mezinárodní politiky.

Brzo po nástupu do funkce nového prezidenta Spojených států amerických oznámil Barack Obama, že se bude v rámci svého politického působení v čele státu snažit zvýšit otevřenost vlády vůči občanům Spojených států. Impulzem k tomuto kroku byla myšlenka, že by americká veřejnost měla získat větší přístup k informacím o činnosti své vlády. Lepší míra informovanosti by pak měla vést k větší důvěře občanů ve vládu a její rozhodnutí. Tento program nesl název *Freedom and Information Act*, zkráceně FOIA. Tento program měl za úkol využít pro svůj cíl moderní technologie, jako jsou například online databáze vládních výdajů. Díky tomu bude občanům stačit pouze připojení k internetové síti a nebudou tedy muset dokumenty fyzicky získat.[52] Tento krok souvisí se změnou přístupu k vedení politiky, kterou nově nastupující prezident Barack Obama přinesl. Snažil se co nejvíce profilovat jako opak svého předchůce George W. Bushe.

[52] CUILLIER, D., PIOTROWSKI, S.J. Internet information-seeking and its relation to support for access to government records. *Government Information Quarterly,* 2009, 26(3), s. 442.

„Charakteristickými znaky Bushovy zahraniční politiky byly nacionalismus, sebevědomí až arogance, unilateralismus a nedůvěra v mezinárodní organizace, včetně OSN. Přístup v duchu hesla, kdo není s námi je proti nám, uplatňovaný v rámci tzv. války proti terorismu, pak vedl ke zhoršení amerických vztahů s mnohými spojenci."[53] Barack Obama se oproti tomu snažil o dialog a získání podpory svých spojenců pro své kroky. „*Jeho styl je spíše orientován na ‚opravování' světa než na jeho ‚tvarování' ".*[54]

Ovšem i přes snahu prezidenta o větší otevřenost Spojených států vůči svým občanům zůstává pravdou, že v určitých případech je žádoucí, aby vláda držela některé informace v utajení.[55] Zároveň je ale přesto nutné zajistit, aby i přes legitimní nárok státu na svá vládní tajemství byl stát schopen odlišit legitimní tajemství od těch nelegitimních. Mezi podporovateli otevřené vlády panuje konsenzus o tom, že americká vláda si již dlouhou dobu nechávala až příliš mnoho informací pro sebe a zbytečně je udržovala v tajnosti. Příliš velké množství vládních tajemství totiž v konečném dopadu státu škodí. Pokud veřejnost a jiné orgány nemají přístup k důležitým informacím, nemohou efektivně pracovat a vzniká tzv. „over-classification". Bohužel v důsledku aktivit Wikileaks a jí podobných aktivistů se tato tendence ještě posílila.[56]

Prezident Obama byl ve funkci necelé dva roky, když se musel potýkat s Wikileaks, coby novým fenoménem snažící se ovlivnit vnímání politiky Spojených států doma i v zahraničí. Jak záběry ze střelby

[53] KOZÁK, K. et al. *Zahraniční politika USA na začátku 21. století,* 1.vyd. Praha: Asociace pro mezinárodní otázky, 2009, s. 65-66.

[54] NAU, H.R. Obama's Foreign Policy. *Policy Review,* 160, 2010, s. 29.

[55] CUILLIER, D., PIOTROWSKI, S.J. Internet information-seeking and its relation to support for access to government records. *Government Information Quarterly,* 2009, 26, s. 442.

[56] BRIAN, D. Wikileaks is a wake-up call for openness. *Government Information Quarterly,* 2011, 28, s. 135.

z armádního vrtulníku Apache na civilisty, tak i rozsáhlé soubory dokumentů o válce v Afghánistánu a Iráku, vznikly za doby působení jeho předchůdce George Bushe. Ze souboru diplomatických depeší, datujících se od roku 1968, se k jeho působení ve funkci vztahují pouze depeše mezi začátkem roku 2009, kdy nastoupil do funkce, a únorem následujícího roku, kde uniklé depeše končí. Pro Baracka Obamu tedy jde více než o otázku, co jsme udělali špatně, spíše o otázku, jak mohlo k takovému úniku vůbec dojít?

Co ale samotné uniklé informace pro Spojené státy znamenaly a co se díky nim změnilo? K zodpovězení této otázky je třeba posuzovat jednotlivé případy zveřejnění zvlášť. Informace o zacházení s vězni ve věznici Guntánamo Bay budou mít jistě jiný dopad než fakta vyplývající z diplomatické korespondence.

Takzvané ‚*Gitmo files* se zabývají unylými informacemi o věznici Guantánamo Bay, která byla zřízena v roce 2002 na námořní základně na Kubě. Tato věznice byla založena jako speciální zajatecký tábor, určen původně pro zajatce z Afghánistánu. Když byl v roce 2010 do funkce prezidenta Spojených států zvolen Barack Obama, patřilo mezi jeho hlavní cíle po nástupu do funkce také uzavření věznice Guantánamo Bay. Tento krok se zdá odůvodnitelný vzhledem k emocím, které toto zařízení budilo ze strany veřejnosti, zvláště mezi ochránci lidských práv.

Dále se zaměřme na zveřejnění diplomatických depeší z konce listopadu roku 2010. Dle oficiálních stránek Wikileaks jde celkem o soubor 251 287 diplomatických depeší rozdělených podle označení na tajné, důvěrné a neklasifikované. Depeší klasifikovaných jako tajné je z celkového počtu pouze necelých 16 tisíc.[57]

[57] Secret US Embassy Cables [online databáze].*Wikileaks* [cit. 2012-04-24]. Dostupné z: http://wikileaks.org/cablegate.html#

„Diplomacie může být definována jako provádění mezinárodních vztahů pomocí jednání a dialogu, nebo jako podpora mírových vztahů mezi státy.“[58] Vídeňská úmluva o diplomatických stycích z roku 1961 definuje práva a povinnosti jak vysílajícího státu, tak i státu přijímajícího. Státy, které přijaly tuto úmluvu, se zavazují respektovat právo vysílajícího státu na volný pohyb, přístup k informacím, specifické postavení diplomata vůči zákonům platící v přijímajícím státě a také nedotknutelnost diplomatické korespondence, která je zaručena článkem 27.

> 1. Přijímající stát povolí a bude chránit svobodné spojení mise ke všem oficiálním účelům. Při spojení s vládou, jakož i s ostatními misemi a konzuláty vysílajícího státu ať jsou kdekoliv, může mise použít všech vhodných sdělovacích prostředků, čítajíc v to diplomatické kurýry a kodované nebo šifrované zprávy. Mise však může zřídit a používat radiostanici pouze se souhlasem přijímajícího státu.
>
> 2. Úřední korespondence mise je nedotknutelná. Pod úřední korespondencí se rozumí veškerá korespondence mající vztah k misi a jejím funkcím.
>
> 3. Diplomatická pošta nesmí být otevřena ani zadržena.[59]

Nehledě na obsah zveřejněných depeší je jasné, že v tomto případě došlo k jasnému porušení této úmluvy. Diplomatická korespondence svým charakterem nepatří na veřejnost. Jedná se o interní komunikaci, která nemusí mít vliv na konečnou podobu zahraniční politiky. Tento článek Vídeňské úmluvy ale nebyl porušen státem, nýbrž

---

[58] CORNAGO, N. Diplomacy. Encyclopedia of Violence, Peace, & Conflict, 2. edit. 2008, s. 574.

[59] O ministerstvu. *Vídeňská úmluva o diplomatických stycích.* [online]. MZV ČR. [cit. 13.3.2013].Dostupné z: http://www.mzv.cz/jnp/cz/o_ministerstvu/videnska_umluva_o_diplomatickych_stycich.html

jednotlivcem, který diplomatickou korespondenci předal Wikileaks k uveřejnění.

Z povahy diplomatické korespondence je jasné, že je určena pouze úzkému okruhu lidí. Psána byla s vědomím, že se v této podobě informace nemají dostat na veřejnost, ale mají formovat informační základ pro tvoření oficiální zahraniční politiky. V tomto duchu se Spojené státy k tomuto problému také vyjádřily. Ve svém prohlášení z konce listopadu 2010 ministryně zahraničních věcí Spojených států Hillary Clintonová jasně deklaruje odmítavý postoj Spojených států vůči činnosti stránky Wikileaks. Z jejich pohledu se jedná o jasné porušení práva na komunikaci mezi vysílajícím a přijímajícím státem a současně tímto aktem došlo k ohrožení zájmů Spojených států ve světě. Přesto ale z jejího prohlášení jasně vyplývá, že na základě již proběhlých jednání se zahraničními partnery Spojených států došly obě strany k tomu, že budoucí jednání budou probíhat zcela normálně jako doposud.[60] Pro Spojené státy tedy šlo spíše o ukázku selhání jejich vnitřních systémů komunikace než o otřesení jejich systému vedení diplomatické komunikace.

„Dlouhodobým důsledkem zveřejnění diplomatických depeší může být větší uzavřenost a netransparentnost diplomacie, neboť se diplomaté i další pracovníci mohou obávat obdobných úniků, a proto se budou omezovat ve svých reportech pro Spojené státy.“[61] (Přeloženo autorem) Uniklé informace patří k interní komunikaci mezi zastupitelskými orgány Spojených států s vysílajícím orgánem. Tato komunikace z povahy věci

[60] CLINTON, H. R. Remarks to the Press on Release of Purportedly Confidential Documents by Wikileaks. *U.S. Department of State,* [online]. U.S. Department of State, 2010 [cit. 2012-06-25]. Dostupné z: http://www.state.gov/secretary/rm/2010/11/152078.htm

[61] THOMAß, B. WikiLeaks and the question of responsibility within a global democracy. *European View,* 2011, 10(1), s. 20.

neměla být nikdy zveřejněna, a tudíž i její obsah se nemůže považovat za oficiální prohlášení.

Je problematické stanovit přesný dopad uniklých materiálů. Přestože ve vztahu ke Spojeným státům americkým nedošlo k nějakému razantnímu zvratu, ve vztahu k jiným státům k tomu dojít mohlo. Mezi takové státy mnozí řadí Tunisko, kdy se po zveřejnění informací o zkorumpovanosti prezidenta Zine al-Abidine Ben Aliho zvedla silná vlna nevole vůči představiteli státu, který posléze ze země uprchl.[62]

Kromě již zmíněného předchozího informování svých zahraničních protějšků pak krátce po zveřejnění materiálů na Internetu byli šéfové zahraničních misí požádáni o prozkoumání k jejich misi se vztahujících materiálů, na které pak měli vypracovat shrnutí a hodnocení závažnosti. Dalším nutným krokem bylo pověření expertů z oblasti informačních technologií, aby podnikli kroky k zabezpečení vládních informačních toků a tím se zamezilo možným podobným únikům v budoucnosti.[63]

Vztah mezi americkou společností a vládou se po únicích nijak zásadně nezměnil.[64] Diplomatické depeše neprozrazují nic, co by se americkou společností dalo považovat za šokující nebo nadmíru překvapivé. Spojené státy bedlivě sledují dění okolo strategických zemí a snaží se zabránit tomu, aby americké zbraně padly do nepravých rukou. Nic z toho se nedá považovat za něco, proti čemu by se mohla americká společnost stavět. Spojené státy měly jistou výhodu i v tom, že je Wikileaks o připravovaných únicích dopředu informovaly. Tím byl poskytnut prostor pro přípravu možných postupů a kroků k minimalizaci

[62] FENSTER, M. Disclosure's Effects: WikiLeaks and Transparency. *Iowa Law Review*. 2012, 97(3), s. 802.

[63] KENNEDY, P. F. Information Sharing in the Era of WikiLeaks: Balancing Security and Collaboration. *U.S. Department of State,* [online]. U.S. Department of State, 2011. [cit. 26.6.2012]. Dostupné z: http://www.state.gov/m/rls/remarks/2011/158400.htm

[64] FENSTER, M. Disclosure's Effects: WikiLeaks and Transparency. *Iowa Law Review*. 2012, 97(3), s. 802.

škod a k nalezení vhodného prostředku, jak podobným situacím v budoucnu zabránit. Nedá se tedy předpokládat, že by Wikileaks byla v blízké době schopna provést další podobnou akci.

Jiný dopad pro Spojené státy mohly mít zveřejněné informace o válkách v Afganistanu, Iráku nebo video „Collateral murder“. V těchto případech mohla společnost nahlédnout do skutečného způsobu vedení probíhající války a válečných operací jednotek Spojených států. Zde se mohly reálné informace zveřejněné Wikileaks dostat do střetu s tím, jak se válečné operace v zahraničí snaží Spojené státy svým občanům a široké veřejnosti prezentovat. Video „Collateral murder“ jasně ukazuje, že válka není pouze o statečnosti amerických vojáků, ale také o

V souvislosti s tím můžeme říct, že jak v případě uniklých materiálů vztahujících se k válce v Afghánistánu a Iráku, tak i diplomatických depeší nevyšlo najevo nic, co by americká společnost nebyla ochotna akceptovat. Obecně řečeno, vláda Spojených států činila kroky nutné k ochraně svých zájmů a zájmů svých obyvatel.

Co se ovšem Wikileaks podařilo, bylo upoutat pozornost na situaci zabezpečení interních informačních systémů nejen na úrovni státní, ale i na úrovni dotýkající se běžných uživatelů. Také společnosti začaly klást daleko větší důraz na to, jak zabezpečené jsou jejich interní informační systémy. To vedlo ke změně pohledu a požadavků, které jsou kladeny na jednotlivá IT oddělení.[65]

4.2 Dopad pro Wikileaks

K tradičním právům v každé moderní demokratické společnosti patří právo na volný přístup k informacím. Lidé se ale prakticky mohou k informacím o aktivitě svých politických představitelů dozvědět buď

[65] BLIGH, K. Journalists, Companies Wrestle With Consequences of Wikileaks. *Econtent*, 2011, s. 12.

z jejich oficiálních prohlášení, nebo na základě informací, které předkládají média. Média ovšem také nedisponují neomezeným přístupem ke všem informacím. Wikileaks se tuto situaci snaží změnit. Skrze uveřejňování utajovaných informací chtějí zvýšit informovanost veřejnosti o tom, jak vláda hájí jejich zájmy. Také tím chce do jisté míry podnítit veřejnost, aby se hlouběji zajímala o dění kolem sebe a o činnost svých vlád. Žurnalisté musejí zkoumat, prověřovat a shromažďovat data. Tyto bariéry Wikileaks snížily.[66]

Wikileaks se dostalo velké mediální pozornosti a jejich snaha nebyla zcela bez odezvy. Činnost Wikileaks a její idea světa o transparentnosti inspirovala celou řadu dalších lidí. Vznikly podobně zaměřené weby, které se snaží o zvýšení informovanosti veřejnosti a poskytnutí prostoru pro uveřejňování dokumentů odhalujících nekalé praktiky ať už státu nebo jiných organizací. Mezi následovatele odkazu Wikileaks můžeme zařadit stránky jako unileaks.org nebo ruleaks.net. V České republice funguje stránka pirateleaks.cz, která se zaměřuje výhradně na zveřejňování informací o činnosti tuzemských úřadů.[67]

Široká veřejnost díky Wikileaks získala možnost volby. Pokud se jim do rukou dostanou důkazy o nekalé činnosti vládních orgánů nebo společností, mohou předat takovéto informace dál k případnému zveřejnění, a tím i přispět ke změně daného systému, ale zároveň sami zůstat v anonymitě. Také se mohou rozhodnout, zda se identifikují s kroky podnikanými jejich jménem. Tím ale také musejí převzít daleko větší odpovědnost za své volby.

Otázkou je, zda se kromě poskytnutí této možnosti volby podařilo Wikileaks dosáhnout něčeho zásadnějšího. Julian Assange rád prezentoval sebe a Wikileaks jako neziskovou organizaci zakládající si

[66] THOMAß, B. WikiLeaks and the question of responsibility within a global democracy. *European View,* 2011, 10(1), s. 17-23.

[67] Zásady projektu PirateLeaks, http://pirateleaks.cz/www/onas,

na zásadách žurnalistické etiky.[68] Pokud ale porovnáme principy a zásady práce profesionálních žurnalistů, pak se nedá říci, že by Wikileaks takové zásady zcela splňovala. Zvláště v případě zveřejnění diplomatických depeší nalezneme dosti rozporů. Nejmarkantnějším z nich je již zmiňované uveřejnění jmen a osobních údajů, které mohou sloužit k identifikaci spojenců a informátorů USA a ti jsou tím pádem, kvůli snaze Wikileaks o naprostou transparentnost, vystaveny ohrožení života.

To, že o sobě někdo řekne, že je žurnalista, z něj ještě nedělá skutečného žurnalistu. Toto odvětví se řídí mnoha pravidly a profesionální žurnalista je musí respektovat. Stejně tak musí mít odpovědnost za informace, které poskytne veřejnosti. Nejde jen o to zveřejnit veškeré získané materiály. Na materiálech se musí pracovat, musí se dát do souvislostí a musí být rozlišeno, kdy daná informace může být pro veřejnost více škodlivá než užitečná. Toto Wikileaks nesplňuje. Wikileaks je předstupněm skutečné profesionální žurnalistiky. Poskytují informace k dalšímu zpracovaní. Ovšem v jejich případě jsou tyto informace poskytnuty celé veřejnosti, nikoli jen žurnalistům.[69]

Samotná Wikileaks si jistě od své práce představovala daleko více. Mimo pouhé zveřejnění informací a poskytnutí veřejnosti možnost učinit si objektivní názor na svou vládu, zde byla také myšlenka na změnu současné situace. Ovšem tyto představy nedošly naplnění.[70]

Pravdou je, že díky rychle se rozvíjejícím nových technologiím je zveřejňování utajovaných informací daleko jednodušší než dříve. Už není potřeba mít fyzickou kopii dokumentu, ani ho není potřeba někam přemisťovat. Vše, co je k tomu potřeba, je počítač a schopná osoba.

[68] About. *What is Wikileaks?* [online]. Wikileaks. [cit. 15.4.2013]. Dostupné z: http://wikileaks.org/About.html

[69] BLIGH, K. Journalists, Companies Wrestle With Consequences of Wikileaks. *Econtent*, 2011, s. 10-12.

[70] ROBERTS, A. The Wikileaks Illusion. *The Wilson Quarterly*, 2011, 35(3), s. 19.

Také už se nejedná jen o relativně malé soubory dokumentů. V případě Wikileaks se jedná o rozsáhlé soubory, obsahující tisíce stránek. Faktem ale zůstává, že jen zlomek z těchto dokumentů byl skutečně označen Spojenými státy jako ‚tajný', zbytek tvoří pouze běžná komunikace a výměna informací, které nemají pro nezasvěcenou veřejnost žádný dramatický význam. Pokud vezmeme v úvahu filosofii zakladatelů Wikileaks, kterým šlo o zveřejňování utajovaných informací bez jakékoli úpravy, pak se tu setkáme s problémem. Ani samotná Wikileaks nemohla vždy plně kontrolovat způsob publikování vlastních dokumentů vzhledem k faktu, že spolupracující deníky jako *Guardian* nebo *El* País, si vybraly pouze ty segmenty informací, které se jim zdály mediálně atraktivní.[71] Proto se daleko více článků zabývá oním pojmenováním premiéra Vladimíra Putina coby ‚alfa samce než problematikou zbrojního programu Iránu a Sýrie.

Dále se tu nabízí otázka, jestli snaha o společnost bez tajemství a zcela otevřené vlády nepřinese spíše opačný účinek. Pokud víte, že cokoliv napíšete, se může okamžitě dostat na veřejnost, pak se můžete začít bát otevřeně mluvit. Veřejnost má právo vědět o krocích podnikaných jejich jménem skrze jejich vládu. Zároveň na druhou stranu má taky vláda právo mít před svými občany tajemství. Mezi těmito dvěma proudy je potřeba najít rovnováhu.[72]

Je pravděpodobné, že vzhledem k nastalé situaci může mít zveřejnění diplomatických depeší vliv na práci diplomatů Spojených států. Tento vliv se může projevovat obavou z případného dalšího úniku a tedy menší ochotou ke komunikaci ze strany zahraničních partnerů.[73] V tomto případě pak záleží na schopnostech a dovednostech zástupců

[71] ROBERTS, A. The Wikileaks Illusion. *The Wilson Quarterly*, 2011, 35(3), s. 16 -17.
[72] FENSTER, M. Disclosure's Effects: Wikleaks and Transparency. *Iowa Law Review*, 2012, 97(3), s. 781.
[73] FENSTER, M. Disclosure's Effects: Wikleaks and Transparency. *Iowa Law Review*, 2012, 97(3), s. 793.

Spojených států postavit se takovým obavám a pracovat na jejich překonání.

Z předchozích informací vyplývá, že i přes původní obavy Spojených států a vysoké cíle Wikileaks, z boje vyšly vítězně Spojené státy americké. Zveřejněné informace poskytly veřejnosti unikátní náhled do skutečného průběhu války, bez příkras a vládních úprav. Ukázaly, jak reálně pracují zaměstnanci amerických ambasád v zahraničí a co vše tito lidé sledují a jaké informace Spojené státy zajímají. Únik takových informací byl pro Spojené státy do určité míry ztrapněním, do jisté míry impulsem pro zlepšení zabezpečení jejich informačních systémů. Tomuto útoku na vnitřní záležitosti státu se Spojené státy postavily rázně a jednoznačně. Aktivně komunikovaly se svými zahraničními partnery a snažily se napravit způsobené škody. Na druhou stranu tvrdě vystoupily proti takovému jednání a vyvodily z toho pro Wikileaks důsledky.

Wikileaks získala značný mediální prostor pro prezentaci svých postojů. Přispěla k informovanosti veřejnosti o krocích podnikaných jejím jménem, zároveň ale na sebe přitáhla pozornost řady kritiků za postupy, které k tomu použila. Většina z nich se shodla, že zveřejněním jmen a údajů spojenců Spojených států je Wikileaks vystavila velkému riziku, kterému se dalo snadno předejít vymazáním nebo začerněním jejich jmen v dokumentech. Wikileaks sice ukázala, jakým směrem se bude v budoucnu vyvíjet boj o informace, ale sama Wikileaks nebyla schopna v tomto boji jednoznačně obstát. Po sérii blokací ze strany finančních institucí a poskytovatelů internetového prostoru byla Wikileaks nucena stáhnout se do pozadí a zastavit příjem možných tajných dokumentů ke zveřejnění. Postupem času daleko více pozornosti přitahoval Julian Assange díky svému charismatickému vystupování a snahy prezentovat Wikileaks coby oběť perzekuce ze strany Spojených států. Wikileaks opustila své původní záměry a zaměřila se více na vlastní přežití.

Touha po stvoření světa bez tajných dohod, ujednání a zpráv, kterou sdílejí zakladatelé Wikileaks, se zdá neuskutečnitelná. Do této chvíle se jim ničeho zásadního v tomto ohledu nepodařilo dosáhnout. Sice vzbudili pozornost médií a široké veřejnosti, ale na druhou stranu díky jejich činnosti nedošlo k žádným razantním změnám. Navíc vlna zájmu ohledně Wikileaks i jeho představitele Juliana Assange již opadla a jediné zprávy, které se v tisku objevují, se týkají jeho možného předání do Švédska. Wikileaks se díky odstřižení od svých bankovních kont ocitla ve finanční tísni, kterou se snaží vyřešit sbírkou na svou činnost. Zajímavostí je, že přestože jim dříve společnost Paypal zamezila přístup ke svým službám, v současné chvíli je již znovu možné využít službu PayPal jako jednu z možností, jak zaslat Wikileaks finanční prostředky na podporu jejich činnosti.[74]

Mnozí si po uveřejnění dokumentů položili otázku, zda je takovéto chování správné a zda je to pro společnost tak prospěšné, jak se Wikileaks snažila tvrdit. Vedle otázky ohledně legálnosti a prospěšnosti zveřejňování interních dokumentů si ale veřejnost byla nucena položit otázku, jak vůbec mohlo dojít k únikům tak velkého množství dokumentů. Jak se podaří relativně malé skupině lidí působící v kybersvětě získat přístup k tak citlivým materiálům?

Informační a komunikační technologie přináší vládě a společnostem na jedné straně možnost větších zisků, ale na straně druhé nás také vystavuje většímu riziku kyber útoků a kyber zločinů.[75] Wikileaks ukázala, že zabezpečení informací, které společnosti nechtějí zveřejnit, není tak nezdolatelné, jak by si někteří mohli myslet.

---

[74] *Donate,* [online] http://shop.wikileaks.org/donate

[75] CHOO, R.K. The cyber threat landscape: Challenges and future research directions. *Computers & Security*, 2011, 30(8), s. 719.

5 ZÁVĚR

Předchozí stránky se snažily ukázat, že Wikileaks se skutečně podařilo uveřejnit řadu dokumentů, které by jinak pro veřejnost zůstaly utajené. Změny v řízení zahraniční politiky Spojených států amerických ale dosáhnout nedokázala. Jejich akce týkající se uveřejnění diplomatických depeší se ve výsledku zdá být přeceňovaná. Důvodem mohla být nekomplexnost a rozsáhlost zveřejněných materiálů. Bylo jich mnoho a byly zveřejněny ve své surové podobě. Data nebyla dostatečně interpretována, prostudována a dosazena do kontextu a příběhu. Byly proto pro společnost nestravitelné.

Také zahraniční partneři USA se k nastalé situaci postavili ve většině případů tolerantně. Často pouze vydali prohlášení o respektování charakteru interní komunikace mezi ambasádami a vysílajícím státem.

Ani samotný obsah diplomatických depeší nepřinesl žádné šokující zjištění. V rámci budování svých diplomatických vztahů Spojené státy následovaly zvolený směr zahraniční politiky určené prezidentem a v rámci toho se tedy jejich diplomatičtí zástupci chovali. Vzhledem k povaze této komunikace se tady často vyskytují osobní názory a postoje, které nemají s oficiálním postojem Spojených států nic společného. Spojené státy z tohoto střetnutí s Wikileaks vyšly vítězně.

Wikileaks tedy nedokázala dosáhnout svého cíle, ale na druhou stranu se jí podařilo ukázat, jak silným nástrojem může v současné moderní společnosti Internet být. Spojené státy se této hrozbě postavily rázně a důsledky pro Wikileaks byly velmi bolestivé. Díky odříznutí od svých bankovních účtů a také díky aféře svého hlavního představitele byla Wikileaks odsunuta do pozadí veřejného zájmu. Přestože není v silách Spojených států smazat veškeré uniklé materiály z Internetu, podařilo se jim nastalou situaci zvládnout.

6 SEZNAM POUŽITÉ LITERATURY

BIRSEN, H. Internet Journalism and Journalistic Ethics: Working Conditions and Qualifications of Journalists in the New Media. *Journal of US-China Public Administration*. 2011, vol. 8, no. 2, s. 230-240. ISSN 15486591.

BRIAN, D. Wikileaks is a wake-up call for openness. *Government Information Quarterly,* 2011, vol. 28 no. 2, s. 135-136. ISSN 0740-624X.

CHOO, R.K. The cyber threat landscape: Challenges and future research directions. *Computers & Security*, 2011, vol. 30, no. 8, s. 719-731. ISSN 0167-4048.

CORNAGO, N. Diplomacy. *Encyclopedia of Violence, Peace, & Conflict*. 2. edit. Academic Press, 2008. ISBN 0123695031.

CUILLIER, D., PIOTROWSKI, S.J. Internet information-seeking and its relation to support for access to government records*. Government Information Quarterly*, 2009, vol. 26, no. 3, s. 441–449. ISSN 0740-624X.

CULL, Nicholas J. WikiLeaks, public diplomacy 2.0 and the state of digital public diplomacy*. Place Branding & Public Diplomacy*. 2011, vol. 7, no. 1, s. 1-8. ISSN 17518040.

DEMIR, M. Importance of Ethic, Credibility and Reliability in Online Journalism. *European Journal of Social Science*. 2011, vol. 24, no. 4, s. 537-545. ISSN 14502267.

FENSTER, M. Disclosure's Effects: WikiLeaks and Transparency. *Iowa Law Review.* 2011, vol. 97, no. 3, s. 753-807. ISSN 0021-0552.

GIRALTE, L.C. et al., Detecting denial of service by modelling web-server behaviour. Computers and Electrical Engineering, 2012. ISSN 0045-7906.

GROENHARTA, H.P., BARDOELB, J.L.H. Conceiving the transparency of journalism: Moving towards a new media accountability currency. *Studies in Communication Sciences*, 2012, vol. 12, no. 1, s. 6-11. ISSN 1424-4896.

JIRÁK, J., KÖPPLOVÁ, B. *Masová média*. Praha: Portál, 2009. ISBN 978-80-7367-466-3.

KOZÁK, K. et a *Zahraniční politika USA na začátku 21. století*. Praha: Asociace pro mezinárodní otázky, 2009. ISBN 978-80-87092-11-8.

KREJČÍ, O*. Zahraniční politika USA*. 2. vyd. Praha: Professional Publishing, 2009. ISBN 978-80-7431-003-4.

LAST, J. V. Can You Plug a WikiLeak?.The Weekly Standard. 2010. vol. 16, no. 15, s. 13-14. ISSN 10833013.

LYNN III, W.F. Defending a New Domain: The Pentagon's Cyberstrategy. *Foreign Affairs*, 2010, vol. 89,no. 5, s. 98. ISSN 0015-7120.

MILLER, G.S. The Press as a Watchdog for Accounting Fraud. Journal of Accounting Research. 2006, vol. 44, no. 5, s. 1001-1033. ISSN 00218456.

NAU, H.R. Obama's Foreign Policy. Policy Review. 2010, no. 160, s. 27-47. ISSN 01465945.

NEWTON, K. Mass Media Effects: Mobilization or Media Malaise?. *British Journal of Political Science*, 1999, vol. 29,no. 4, s. 578. ISSN 0007-1234.

NIELSE, S.C. Pursuing Security in Cyberspace: Strategic and Organizational Challenges. *Orbis,* 2012, vol. 56, no. 3, s. 336-356. ISSN 0030-4387.

OTTIS, R. LORENTS, P. Cyberspace: Definition and Implications. Proceedings of the International Conference on Information Warfa, 2010, s. 267-270.

ROBERTS, A. The WikiLeaks Illusion. Wilson Quarterly. 2011, vol. 35, no. 3, s. 16-21. ISSN 03633276.

ROBERTS, A. Wikileaks: The Illusion Of Transparency. International Review of Administrative Sciences, 2012, vol. 78, no. 2.

ROSENTHAL, J. Dear Julian. World Affairs. 2011, vol. 174, no. 4, s. 86-91. ISSN 00438200.

THOMAß, B. WikiLeaks and the question of responsibility within a global democracy. *European View*, 2011, vol. 10, no. 1, s. 17-23. ISSN 1865-5831.

Elektronické zdroje:

CSSI. *Cybersecurity two years later* [online]. 2011, s. 2 [cit. 15.4.2013]. Dostupné z: http://csis.org

About. *What is Wikileaks?* [online]. Wikileaks. [cit. 15.4.2013]. Dostupné z: http://wikileaks.org

BBC News US & Canada. *PayPal cuts Wikileaks access for donations* [online]. BBC, 2013. Poslední změna 4.12.2010 09:33. [cit. 15.4.2013]. Dostupné z: http://www.bbc.co.uk

BBC News US & Canada. *Wikileaks publishes confidential emails from Stratfor* [online]. BBC, 2013. Poslední změna 27.2.2012 20:50. [cit. 15.4.2013]. Dostupné z: http://www.bbc.co.uk

BLIGH, K. Journalists, Companies Wrestle With Consequences of Wikileaks. *Econtent* [online]. 2011 [cit. 15.4.2013]. Dostupné z: http://www.econtentmag.com

Cablegate. *Action Request: Readout Of Fried-antonov Discussion On Cfe* [online databáze]. Wikileaks, 2011. Poslední změna 8.9.2011. [cit. 25.6.2012]. Dostupné z: http://www.cablegatesearch.net

Cablegate. *Afghanistan's Future - Next Steps* [online databáze]. Wikileaks, 2011. Poslední změna 8.9.2011. [cit. 29.52012]. Dostupné z: http://www.cablegatesearch.net

Cablegate. *Ongoing Proliferation Finance Activities By Iran And North Korea* [online databáze]. Wikileaks, 2011. Poslední změna 8.9.2011. [cit. 29.5.2012]. Dostupné z: http://www.cablegatesearch.net

Cablegate. *Post Requested To Follow Up On Ongoing Matters Of Proliferation Concern Raised At Apec By President Bush* [online databáze]. Wikileaks, 2011. Poslední změna 8.9.2011. [cit. 29.5.2012]. Dostupné z: http://www.cablegatesearch.net

Cablegate. *Reporting and collection needs: the United Nations* [online databáze]. Wikileaks, 2011. Poslední změna 8.9.2011. [cit. 25.6.2012]. Dostupné z: http://cablegate.wikileaks.org

Cablegate. *Response To North Korean Taepo-dong 2 Launch* [online databáze]. Wikileaks, 2011. Poslední změna 8.9.2011. [cit. 25.6.2012]. Dostupné z: http://www.cablegatesearch.net

Cablegate. *Tf United States September Attack Situation Report* [online databáze]. Wikileaks, 2011. Poslední změna 8.9.2011. [cit. 29.52012]. Dostupné z: http://www.cablegatesearch.net

Cablegate. *U.s. And Russian Comm Satellite Collision*. [online databáze]. Wikileaks, 2011. Poslední změna 8.9.2011. [cit. 25.6.2012]. Dostupné z: http://www.cablegatesearch.net

CLINTON, H. R. Remarks to the Press on Release of Purportedly Confidential Documents by Wikileaks. *U.S. Department of State,* [online]. U.S. Department of State, 2010 [cit. 2012-06-25]. Dostupné z: http://www.state.gov

Donate, [online] Wikileaks. [cit. 15.4.2013]. Dostupné z: http://shop.wikileaks.org

HQ, USD-Center. *Soldier faces criminal charges* [online]. 2010. [cit. 24.4.2012]. Dostupné z: http://www.cbsnews.com

KENNEDY, P. F. Information Sharing in the Era of WikiLeaks: Balancing Security and Collaboration. *U.S. Department of State,* [online]. U.S. Department of State, 2011. [cit. 26.6.2012]. Dostupné z: http://www.state.gov

O ministerstvu. *Vídeňská úmluva o diplomatických stycích.* [online]. MZV ČR. [cit. 13.3.2013]. Dostupné z: http://www.mzv.cz

Secret US Embassy Cables [online databáze].*Wikileaks* [cit. 2012-04-24]. Dostupné z: http://wikileaks.org/cablegate.html#

US Executive Office of the President. *Cyberspace Policy Review* [online]. 2009, s. 13-14. [cit. 15.4.2013]. Dostupné z: http://www.whitehouse.gov

US Department of State. *Blue Lantern Program*. [online]. US Department of State, 2012. [cit. 29.5.2012]. Dostupné z: http://exportcontrol.org

US Executive Office of the President. *Cyberspace Policy Review* [online]. 2009, s. 1 [cit. 15.4.2013]. Dostupné z: http://www.whitehouse.gov

7 RESUMÉ

The thesis deals with Wikileaks, specifically with its influence on the United States of America. Wikileaks made several disclosures, which have had a huge impact on how American society, and also government, think about the possibilities of the Internet. Wikileaks shows that cyberspace could be used in many different ways, and some of them may not be pleasant for governments. The purpose of Wikileaks was to show the truth about Iraq war and USA foreign policy in general. The United States were forced to face this new phenomenon. They have to deal with consequences of Wikileaks and they have to find solutions to prevent such situations in the future.

In first chapter I acquaint the reader with the cyberspace and its possible risks for the US security. The Chapter describe what kind of threats are the most dangerous for governments like the US, and why is cybercrime on the increase. Next chapter describes modern mass media in cyberspace and, most importantly, presents Wikileaks, as an organization, its history and greatest achievements. Last chapter examines the results of Wikileaks disclosures for the US and also for Wikileaks as such.