Kyberválka ve veřejném prostoru

Jak hackeři bojují o budoucnost kyberprostoru.

Nebo ne?

JAKUB MIKULÁŠ

375 750

Masarykova univerzita

Filozofická fakulta - Ústav hudební vědy

Teorie interaktivních médií

Pokusil jsem se prozkoumat pojem hacktivismu a jevy s ním spojené. Odkud pochází? O co mu jde? Jakými prostředky? Zajímalo mě hlavně napojení hacktivstů na velké medializované údalosti jako Wikileaks, Arabské jaro, LulzSec nebo #occupy.

I tried to explore the concept hacktivism and phenomena associated with it. Where does it come from? What are their goals? By what means? I was interested mainly in connection of hacktivism and events such as Wikileaks, Arab Spring, LulzSec or #occupy.

OBSAH

Internet is not for sissies
Paul Vixie

"Collateral murder", "Afghan War Diary", "Iraq War Logs" a "Cablegate" jsou názvy 4 velkých leaků, za kterými v roce 2010 stál web Wikileaks v čele s Julianem Assangem. Všechny sklidily obrovský mediální ohlas. Média se musela velmi rychle vyrovnat s novou terminologií a přístupem k informacím. Ne vždy to šlo snadno - výhružkami, vojenskými soudy a tresty smrti se nešetřilo: *"The Assassination of Julian Assange"*[1].

1 Youtube: The Assassination of Julian Assange. [online]. [cit. 2011-09-15]. Dostupné z: http://youtu.be/3Fab1IsCZzY - na video odkazoval i Twitter Wikileaks - https://twitter.com/#!/wikileaks/status/63756154437767169

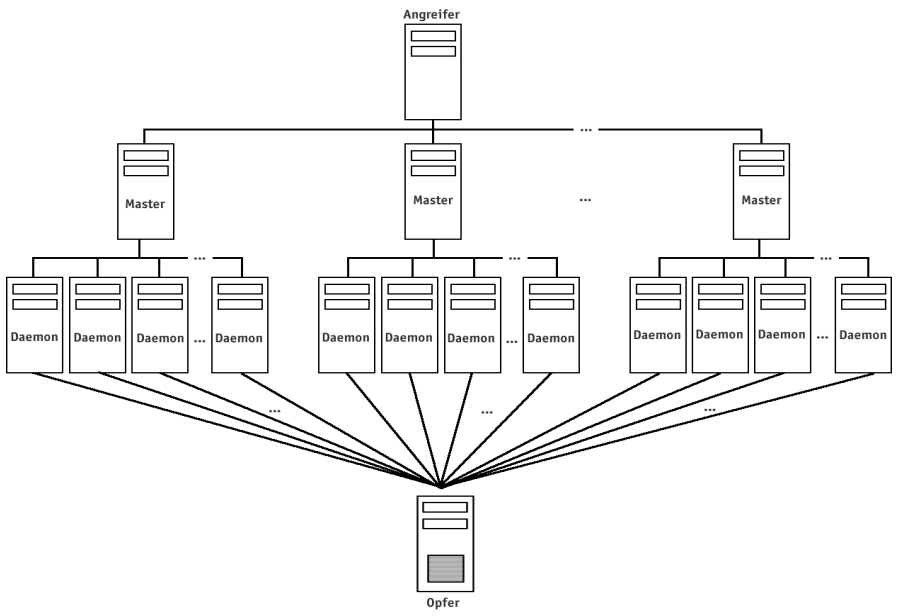
Leaky Wikileaks vyvolaly tvrdou odpověď. Objevily se útoky na infrastrukturu Wikileaks využívající DDoS[2] a později i komplexnější útoky - jako napadnutí name serverů apod. Nejde zjistit, kdo přesně za nimi stál, ale k DoS/DDoS útokům se přihlásil hacker "*The Jester*"[3]. Další podezřelí jsou vlády. Nejrazantnějším krokem bylo vydírání firem, které poskytovaly Wikileaks technologické zázemí - od hostingu až k DNS. Došlo i na *platební blokádu (Banking Blockade)*[4]: Bank of America, VISA, MasterCard, PayPal a Western Union zmrazili Wikileaks účty. Mělo se jednat o milióny dolarů, které Wikileaks získala z dotací - její právní status je totiž nezisková organizace[5] a právě dobrovolné příspěvky jsou její hlavní příjem.

DDoS

Distributed denial-of-service attack

Typ útoku na server. Pointou útoku je přetížit cílový server dotazy, a tím ho znepřístupnit ostatním. Je velmi populární převážně pro svou nenáročnost. Zprovoznit populární DoS nástroj LOIC (Low Orbit Ion Canon) je otázka několika vteřin i pro méně technicky znalé.

Distribuovaná verze počítá se zapojením více počítačů. Nikdy se však nejedná o skutečně nebezpečný typ útoku.



Wikileaks nebyla neznámá služba. Nápad měl Assange *(nejspíše)* už v druhé polovině 90. let, kdy na jeho serveru byla k nalezení služba LEAKS[6], o které však nikdo nic nevěděl. V roce 1999 si Assange zaregistroval doménu

---

2 WikiLeaks: We are under denial-of-service attack. CNET News [online]. 28.9.2010 [cit. 2011-11-12]. Dostupné z: http://news.cnet.com/8301-1023_3-20023932-93.html?tag=content;siu-container

3 The Jester Hits WikiLeaks Site With XerXeS DoS Attack. Infosec Island [online]. 29.9.2010 [cit. 2011-11-12]. Dostupné z: http://www.infosecisland.com/blogview/9865-The-Jester-Hits-WikiLeaks--Site-With-XerXeS-DoS-Attack.html - The Jester při svém útoku nevyužil žádnou botnetovou síť či jiný typ distribuovaného DoS. Využil chybu v Apachech serverech (na kterých běží dnes většina webů), díky které mohl na servery útočit z jediného PC.

4 Banking Blockade. Wikileaks [online]. 24.10. 2010 [cit. 2012-01-20]. Dostupné z: http://wikileaks.org/Banking-Blockade.html

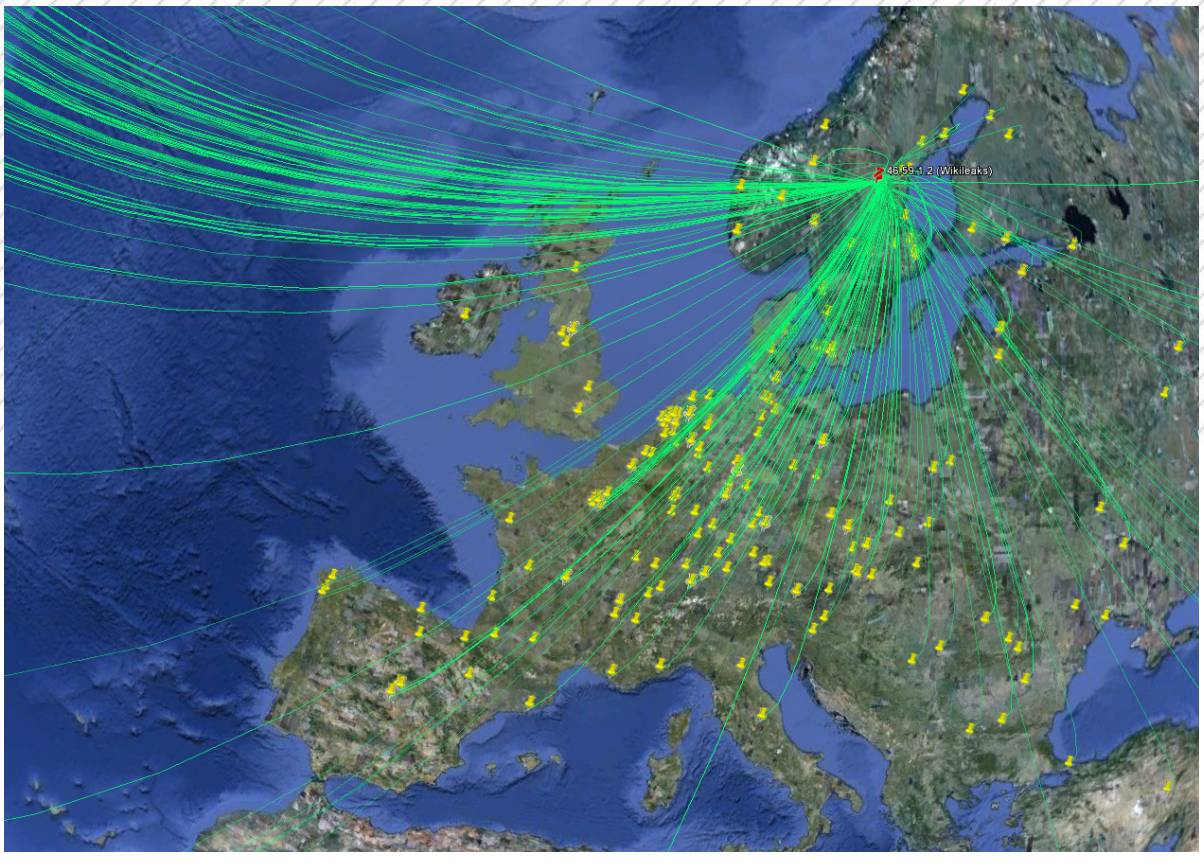
5 Ačkoliv je to s definicí Wikileaks jako právního subjektu stále velmi složité.

6 The Cypherpunk Revolutionary Julian Assange: The Cypherpunk Revolutionary Robert Manne on Julian Assange. Cryptome.org [online]. Březen 2011 [cit. 2011-06-18]. Dostupné z: http://cryptome.org/0003/assange-manne.htm

leaks.org, se kterou však nic nedělal. Web Wikileaks.org oficiálně vznikl v roce 2006, pod švédskou legislativou, která umožňuje účinně chránit novinářské zdroje[7]. Od té doby již stihl vydat celou řadu dokumentů různé důležitosti[8]. Všechny aktivity jsou označovány za žurnalismus - tudíž jsou chráněny - v USA například prvním dodatkem Listiny práv o svobodě tisku.

7 Což z principu „plausible deniability“, kdy nikdo z Wikileaks, díky propracovanému systému anonymního nahrávání dat, ani nemůže vědět (natož prozradit u soudu) kdo informace vynesl. Samozřejmě je poté větší tlak na ověření takto získaných informací.

8 Information published by WikiLeaks. In: Wikipedia: the free encyclopedia [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2012-01-20]. Dostupné z: http://en.wikipedia.org/wiki/Information_published_by_WikiLeaks



Odezva

Odezva na *Banking Blockade* se dala vyloženě očekávat. Pro spoustu netizens je *net neutrality* stále velmi silný pojem. Hackerská komunita, digitální aktivisté[9] i někteří digerati jsou velmi hákliví na státní zásahy do kyberprostoru. Na BBC se dokonce objevil rozhovor s členem skupiny Anonymous, kteří ve jménu Wikileaks podnikali DDoS útoky na weby Visy, PayPalu aj. V rozhovoru zazní, že Anonymous nešlo přímo o data, která web Wikileaks vypouštěl, ale o skutečnost, že se někdo pokusil zastavit šíření těchto dat[10]. Mělo jít o odboj vůči státní moci v kyberprostoru.

Velkými leaky v roce 2010 Julian Assange, předvedl světu novou vlnu západních aktivistů. Bylo jasné, že "*být aktivistou na internetu*" bude znamenat více, než psát protivládní blog a přispívat na uzavřené fórum. Ne každý hacker je mu nakloněn. Ani jeho prostředkům - přece jen, hackeři pocházejí z různých politických zázemí[11]. Je tedy jasné, že když postavíte

9 Digitálními aktivisty nemyslím hacktivisty. Digitální aktivisté jsou blogeři, podcasteři a všeobecně lidé, kteří se určitým způsobem snaží naplňovat utopistické ideje o občanském internetu z 80. a 90. let

10 Wikileaks activist: ‚Anonymous' member, ‚Coldblood'. BBC News [online]. 9.12.2010 [cit. 2011-11-12]. Dostupné z: http://www.bbc.co.uk/news/technology-11960045

11 Hackerské komunity už v 80. i 90. letech obsahovaly kompletní politické spektrum - včetně anarchistů a extrémní pravice i levice. Technocentralismus × decentralismus / technokrati i technokritici.

hackerské komunity před politický problém, dostanete velmi rozdílné výstupy. Avšak narušení suverenity kyberprostoru je hackersky mainstreamové téma.

Anonymní webová síla[12] nejdříve mirrorovala celé stránky wikileaks.org/wikileaks.ch[13] a v případě „*Afghan War Diary*“ jen archiv. Po začátku Banking Blockade začali organizovat[14] útoky na weby Paypalu nebo Visy.

Jednalo se o odboj s těžko definovatelnou společnou základnou. Co o nich víme? Snad jen, že jim jsou společné principy net neutrality *(viz. komentář člena Anonymous na BBC)* a svobody informací. Ale to je vše. Byli víceméně decentralizovaní a dostatečně chytří[15], aby nebylo možné zjistit příliš. Otázkou také zůstává, zdali někdo operaci Payback řídil - vzhledem k anonymnímu prostředí si nemůžete být jisti od koho přijímáte cíle a *agendu/diskurz*. Kdykoliv se objeví politicky motivované akce na internetu, objeví se otázky, zdali šlo skutečně o *crowdsourcing* nebo o přesně zorganizovanou akci např. politickým rivalem. Zažili jsme to i v českých podmínkách[16].

---

12 „anonymní“ nejen kvůli zapojení Anonymous

13 Wikileaks se kvůli ztráty bezpečného hostingu museli přesunout na švýcarskou doménu. Dnes je jejich doména wikileaks.org opět funkční pro všechna necenzurovaná připojení k internetu.

14 Organizace probíhala skrz letáky na Twitteru a webu 4chan.org. Ale na informace o operaci Payback jste mohli najít i v diskuzích na zpravodajských serverech apod. Vzniklo také několik blogů a single serving sites. Jako mnohem účinnější formou organizace se ukázal tzv. „Hive Mind“ mód v programu LOIC. LOIC se připojil na velitelský IRC kanál, odkud přijímal informace o dalším cíli, na který se má zaútočit.

15 či při nejmenším vybaveni dostatečně chytrým softwarem jako Tor, LOIC apod.

16 http://www.lidovky.cz/cssd-z-vajickovych-utoku-opet-obvinuje-ods-a-pozaduje-ochranu-p60-/ln_domov.asp?c=A090527_090018_ln_domov_ani

Válečná vítězství

Zastánci Wikileaks *vyhráli*. Nikomu se (samozřejmě) nepodařilo zastavit šíření leaků. Nikomu se nepodařilo zastavit Wikileaks. Každý další leak a vítězství ve formě volně dostupných dat a širokého novinářského pokrytí ukazovalo, jak kyberprostor mění poměr sil. Alespoň podle vyjadřování zapojených hacktivistů. Začalo se také hovořit o *asymetrické kyberválce* a kyberválce obecně - někteří lidé vycítili, jak moc jsou státy v kyberprostoru zranitelné a bezmocné. Ani velmoc jako USA nedokázala zabránit úniku informací - ani postihnout své nové nepřátele v kyberprostoru. Toto je záležitost, která provází kyberprostor od počátku: Při jeho vzniku v něm každý byl začátečník – i vlády.

V roce 2010 se objevila minimálně ještě jedna závažná skutečnost: *Stuxnet*. Podle některých se jedná o první vládní *kyberzbraň*. Minimálně je to velmi komplexní virus[17]. Podle indícií se jedná o americko-izraelský projekt[18] [19] - původně zaměřený převážně proti jaderným kapacitám (turbínám) v Íránu. Stuxnet také skutečně v několika incidentech spojených s Íránským jaderným programem a selháním turbín figuroval jako hlavní podezřelý - Izra-


HACKERS CAN TURN YOUR HOME COMPUTER INTO A BOMB

. . . & blow your family to smithereens!

By RANDY JEFFRIES / Weekly World News

WASHINGTON — Right now, computer hackers have the ability to turn your home computer into a bomb and blow you to Kingdom Come — and they can do it anonymously from thousands of miles away!

Experts say the recent "break-ins" that paralyzed the Amazon.com, Buy.com and eBAY websites are tame compared to what will happen in the near future.

Computer expert Arnold Yoberson, president of the Washington-based consumer group National CyberCrime Prevention Foundation (NCPF), says that as far as computer crime is concerned, we're only seen the tip of the iceberg.

"We've grown accustomed to those nuisance online hijinxsters are the least of our worries," Yoberson told Weekly World News.

"There are brilliant but unscrupulous hackers out there who have developed technologies that the average person can't even dream of. Even people who are familiar with how computers work have trouble getting their minds around the tech bit things that can be done.

"It is already possible, for an assassin to send someone an e-mail with an innocent-looking attachment connected to it. When the receiver

KABOOM! It might not look like it, but an innocent home computer like this one can be turned into a deadly weapon.

stories." Yoberson said.

"Soon it will be sold to terrorists cults and fanatical religious-fringe groups.

"Instead of blowing up a single place, these groups will be able to switch into the central computer of a

elští i Američtí představitelé se usmívají a potvrzují, že Íránský nukleární program byl zbržděn circa o 3 roky[20]. Objevují se i názory, že za Stuxnetem stála Čína, která měla pro jeho vytvoření Stuxnetu jak zdroje tak technologické možnosti. Stuxnet i jeho potomek Duqu[21] jsou reálnou hrozbou.

---

17 tak komplexní, že málokdo pochybuje, že by se nejednalo o zbraň vyvíjenou státem/více státy

18 A Declaration of Cyber-War. GROSS, Michael Joseph. Vanity Fair [online]. Duben 2011 [cit. 2012-01-11]. Dostupné z: http://www.vanityfair.com/culture/features/2011/04/stuxnet-201104

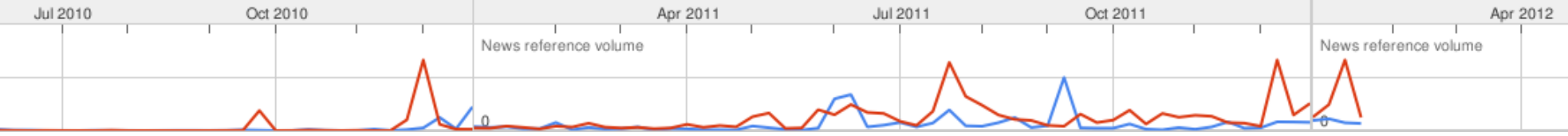
19 W32.Stuxnet Dossier. In: Symantec Security Response [online]. únor 2011 [cit. 2012-01-12]. Dostupné z: http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf

20 Israeli Test on Worm Called Crucial in Iran Nuclear Delay. BROAD, William J., John MARKOFF a David E. SANGER. The New York Times [online]. 15.1.2011 [cit. 2012-01-11]. Dostupné z: http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?_r=2&ref=general&src=me&pagewanted=all

21 Duqu: The Precursor to the Next Stuxnet. Symantec [online]. 2011 [cit. 2012-01-12]. Dostupné z: http://www.symantec.com/outbreak/?id=stuxnet

Možnost kyberválky s sebou však přináší spoustu otázek: může kyberválka vůbec existovat? Software skutečně může být výborným nástrojem pro rušení komunikací, účinné zneškodnění rakety narušením jejich zaměřovacích systémů nebo snad i ničení některých fyzických cílů. Ale takový útok potřebuje, když odečtu měsíce na přípravu kódu, minimálně týdny, než se rozmnoží. Také není vždy možné zasáhnout všechny určené sítě. Mnoho důležitých institucí přešlo na uzavřené sítě (jaderné elektrárny, vojenské základny atd.).

Výše uvedený scénář počítá s kyberútokem jako s něčím, co předchází útok hlavních pozemních vojsk. Ale pokud by šlo pouze o kyberútok, jakkoliv velký, často nemáte možnost zjistit, od koho pocházel. Pokud by zítra došlo k kyberútoku na USA, jak poznáte, kdo za ním stál? Čína? Rusko? Anonymous? Izrael? Někdo z USA? Je to podobně nový druh války, jakým byl ve 20. století terorismus. Těžko identifikovatelná hrozba, neznámé důsledky a pokřivený slovník - *war on terrorism*. Když zůstaneme u paraley: existují *teroristické zbraně?*

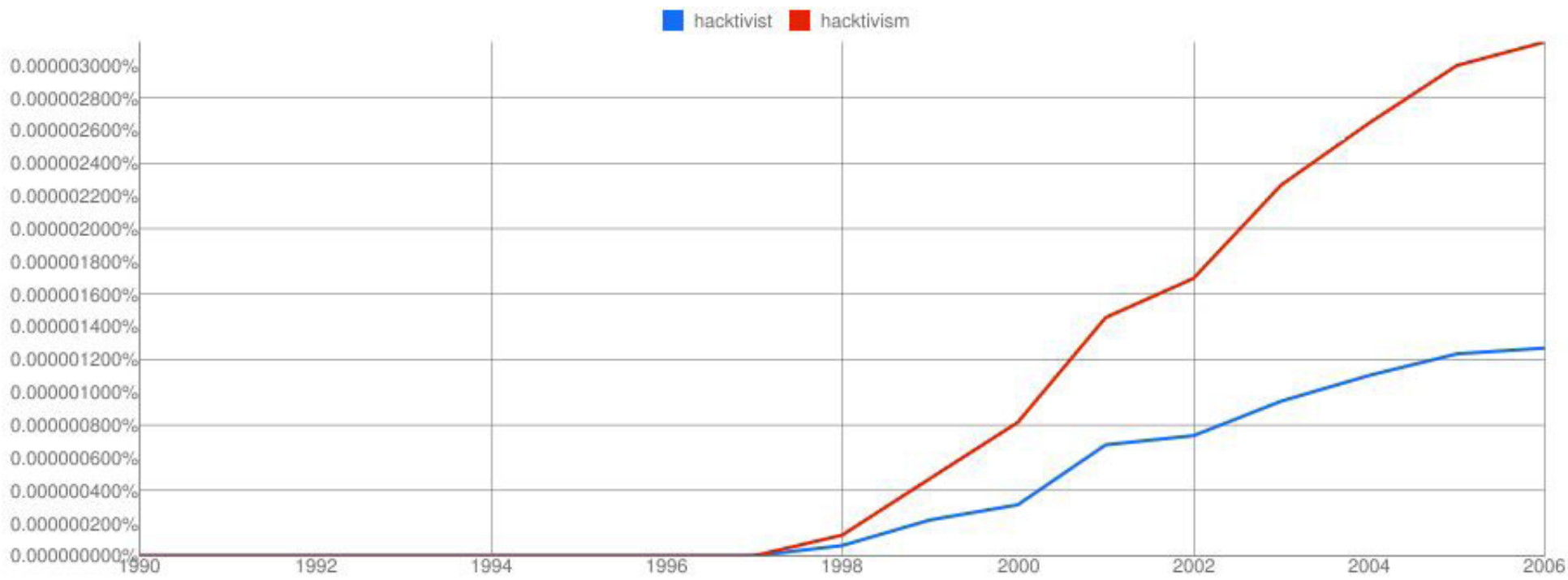


Hacktivismus

Výskyt slova hacktivism a hacktivist v anglicky psaných novinových článcích 2010-2012
www.culturomics.org

Bylo to právě v roce 2010, kdy se slovo hacktivism začalo používat ve významu, jak jej chápeme dnes. Termín hacktivism přejala už i velká média. Hacktivismus je relativně nový termín, jeho obsah však ne. Široká definice by měla znít asi takto: „*Hacking s politickými cíli*“. Jenže, jak jsem psal výše: politická základna hackerských skupin byla velmi roztříštěná - to je také důvod proč nelze zařadit hackery *doprava či doleva*. Nejde je ani označit za technokraty nebo alternativní skupinu.

Jak je to tedy s hacktivismem?



Výskyt slova hacktivism a hacktivist v anglicky psaných textech. 1990-2006
www.culturomics.org

V roce 1984 se členové CCC[22] pokusili upozornit na bezpečnostní chyby videotexového[23] systému Btx. Btx, jakožto prodělečný projekt placený (západoněmeckou) vládou, si nemohl dovolit žádnou negativní reklamu nebo pochybnosti u veřejnosti. Mělo přece jít o vládou zastřešený telekomunikační kanál - předpovědi počítaly s milióny prodaných přístrojů, *nesměly* se objevit problémy. V reálu se jich prodaly pouze stovky tisíc, takže uživatelé byli často právě hackeři z celého Západního Německa. Zodpovědní

22 Chaos Computer Club

23 Interaktiní informační systém - z dnešního pohledu hybrid mezi teletextem (videotext byl interaktivní) a internetem (videotext byl centrálně řízený).

lidé námitky CCC ignorovali. O několik měsíců později byl Btx (jehož součástí byl i platební systém) hacknut a hackerům se podařilo na účet CCC připsat 135 000 DM - tyto peníze (za doprovodu tisku) přišli o několik dní později předat zpět.

Bylo hacknutí Btx projevem hacktivismu? Na jednu stranu: nejednalo se o vyloženě *politický hack*. Aktéři do něj nevstupovali s politickými úmysly. Naproti tomu stojí argument, že CCC byl značně zpopularizován a do budoucna si nesl nálepku *těch hodných hackerů*. Jejich akce měly také za následek změnu zákonů týkajících se hackingu. Zákon „*2. WiKG*“[24] se snažil řešit právní otázky jako: „Jsou data v počítači (= výsledky matematických operací) přípustné jako důkaz u soudu?“ „Je nedovolené vniknutí do nezabezpečeného počítače trestným činem? A co zabezpečený počítač? A je trestným činem jen vniknutí nebo se jedná o trestný čin až při změně/zkopírování dat?“.

Nakonec však Btx hack nejspíše můžeme považovat za hacktivismus, protože se CCC podařilo změnit zákony i celkový obraz hackerů v 80. letech. Zvrátili ve svůj prospěch názor veřejnosti, médií i některých politiků (viz. 2. WiKG), kteří se nemohli rozhodnout, zdali jsou hackeři více hrozbou nebo odborníky. CCC je dodnes v Německu uznávaná síla, hlavně díky tomu, že se za posledních 30 let zasloužila o vzdělávání veřejnosti v oblasti technologií.

Pravdou zůstává, že definice hacktivismu je velmi otevřená. A jak do ní možná svými nepolitickými ambicemi nezapadá CCC, tak do ní nedostatkem *hacku* nezapadají současní hacktivisté.

---

24 „2. Wirtschaftskriminalitätsbekämpfungsgesetz“

Did it for the Lulz a Arabské jaro

Rok 2011 byl ještě zajímavější. Facebookové revoluce. *Arabské jaro*. Můžeme na něj pohlížet, jako na okamžik, kdy technologie západních zemí stály proti demonstrantům. O tom za okamžik.

Nemám v plánu hlouběji analyzovat Arabské jaro - jen připomínám, že nejdůležitější kanály byly Facebook, Twitter a YouTube. Je brzo přesněji vnímat všechny síly a kontexty Arabského jara, ale názor, že bez sociálních sítí by revoluce nezískaly hybnost, není úplně nepravdivý[25]. Díky sociálním sítím a jejich konceptům získali protestující možnost rychle komunikovat a reagovat v rámci nestátního a otevřeného média, ale také se dostali na kanály, kde byl západ ochoten naslouchat. Na chvíli byli součástí západní kultury. Silný příběh o utlačovaných národech zvítězil. Blízký východ se na chvíli svým „bojem za svobodu“ přiblížil západnímu kyberprostoru, protože používal stejné kanály. A bojoval proti něčemu, čeho se celý internet bojí – státní kontrola (digitálních) informací. Alespoň to Arabské jaro znamenalo pro mnoho hacktivistů. Každá revoluce si s sebou táhne dávku patosu.

---

25 So, Was Facebook Responsible for the Arab Spring After All?. The Atlantic [online]. 3.9.2011 [cit. 2012-01-20]. Dostupné z: http://www.theatlantic.com/technology/archive/2011/09/so-was-facebook--responsible-for-the-arab-spring-after-all/244314/

Hackeři již dříve pomáhali obcházet státní kontrolu internetu ve státech s omezeným přístupem k internetu - příkladem jsou čínští disidenti snažící se překonat Great Firewall of China. Takže pomocná ruka, bojující proti filtrování informací, ze strany západu nebyla novinka. Novinkou byl blízký kontakt, který mezi sebou účastníci navázali právě díky médiím jako Twitter a Facebook, kde mohli individuálně komunikovat. Právě to, co je tak důležité u revolucí obecně - společné smýšlení.

Internet (a sociální média) během revolucí fungoval pouze jako médium. Nepodařilo se mi vysledovat, že by použití nového/decentralizovaného média změnilo podstatu, že stále jde o *revoluci*. Snad jen snadnější tvorbu a sdílení ikonických výjevů, fotek a mučedníků - osobně bych to přirovnal ke změně, jakou znamenalo zapojení médií do Vietnamské války v 60. a 70. letech. Mohli bychom hledat paralely mezi zastřelením důstojníka vietcongu a zavražděním Saeeda Khaleda. Internet neudělal revoluce během Arabského jara méně (či snad více) násilné a krvavé.

Souběžně s Arabským jarem vznikl také pojem, který na hodnou chvíli zaplnil média: *LulzSec*.

Skupina LulzSec, jejich web lulzsecurity.com a twitter účet @lulzsec byly jakýmsi hybridem mezi Wikileaks a Arabským jarem. De facto není důležité koho hackli nebo jak hackli - ale spíše jde o to, co představovali.

Just saw a thread on [4Chan.org] where they're trying to hunt us, you /b/tards realize that we are everything you've ever tried to be?[26]

LulzSec se předváděli. Necítili se ohroženi, média se je snažila uchopit a zklamala, což pro ně bylo mnohem vtipnější. Sami označili Anonymous za blbce. DDoS na weby jako cia.gov nebo leaky dokumentů Arizonské policie na sebe upoutali pozornost bezpečnostních složek. Ostatní hackerské skupiny se rozhodly, uraženy jejich nízkou úrovní a předváděním se[27], LulzSec odhalit *(předně hacker The Jester a skupina TeaMpoisoN_)*.

Když se vysmívají The Jesterovi, hodnotí úspěch podle publicity[28]. Ne podle skillu, jak by u hackerů mělo být zvykem podle hackerské etiky. Nejsou skrytí - dobývají noviny. Nehackují - předvádí se. Moc korumpuje.

LulzSec nejspíše byla parta script kiddies, kteří útočili na náhodné stránky. Původně patřili k Anonymous, ale nikdy k *velkým hackerům*. Kromě toho, že nám vrátili Tupaca[29], možná také předznamenali některé změny, které se blíží. Kromě jiného se ale také zasloužili o to, co nejeden hacker: upozornění na chyby v systému. Pokud v podstatě amatérská skupina dokázala způsobit takové pozdvižení, naše bezpečnost na tom musí být opravdu špatně. Nesmí nás potom překvapit, že opravdu nebezpečný virus, jako Stuxnet, dokáže nepozorovaně měsíce pronikat do systémů, aby dokázal vyřadit raketový/obranný/jaderný potenciál celé země.

V roce 2010 i 2011 se znovu také projevily 2 důležité narativy: hodný hacker, zlý hacker. Jedná se o staré rozdělení, z podobné doby jako zákon 2. WiTG, ten s úmyslem hackera počítal jako s ukazatelem, jak posuzovat hackerský čin. Toto dělení bylo později označeno za naprosto zbytečné (a například v Německém zákoně se s možností *hodného/whitehat hackera* přestalo počítat).

Jenže dnes se tento narativ vrací. Zlí hackeři útočí na státní databáze. Zlý protistátní hacktivisté blokují naše linky DDoS útoky nebo dokonce naše města skrz #occupy protesty. Jenže ze zlých hackerů vynášejících informace najednou byli bojovníci za svobodu, kteří pomáhali překonávat internetové blokády opresivních režimů. Najednou hackeři stáli na "správné straně", pomáhali přece bojovat za svobodu. Bojovat proti diktátorům. Problém je, že to často jsou ti stejní lidé, kteří zkrátka brání internet, protože je to poslední politické téma digitálně nativních uživatelů.

Kyberprostor na počátku 21. století je aréna plná komplexních stavů - akce jednotlivých stran ovlivňují globální vztahy, které zpětně ovlivňují další strany. To není novinka, ale kyberprostor globalizaci dovádí často do absurdních rozměrů. Jako příklad bych uvedl firmu NetApp (USA), která přes dodavatele vyvážela software pro monitorování a blokování internetu

29 http://linearfix.wordpress.com/2011/05/30/lulzsec-hacks-pbs-and-publish-fake-article/

do Sýrie[30]. Kde byl používán proti demonstrantům. Nebo izraelská softwarová firma vyvážející spyware do Íránu[31] (!). Návrhy na regulaci vývozu softwaru jsou nejspíše blízká budoucnost (podobná regulace jako u zbraní - šifrovací softwaru[32]).

Poslední 2 roky také ukázaly, že v kyberprostoru operují přinejmenším tyto síly:

- Státy, jejich bezpečnostní složky a státní agentury
- Soukromé organizace, IT firmy (i Facebook)
- Nezávislé skupiny (EFF, CCC) a jednotlivci (The Jester)

Toto je poněkud vzdálené kyberutopistickým vizím o lidském-občanském--anarchistickém prostoru.

---

30 Wired For Repression: The Surveillance Market and Its Victims. Bloomberg [online]. 20.11.2011 [cit. 2012-01-07]. Dostupné z: http://www.bloomberg.com/data-visualization/wired-for-repression/

31 Iran Using Israeli Spyware. Israel National News [online]. 23.11.2011 [cit. 2012-01-08]. Dostupné z: http://www.israelnationalnews.com/News/News.aspx/151023

32 kryptgorafický software nesměl být vyvážen mimo USA - cypherpunkeři vynalezli způsob jak PGP natěsnat do 3 řádků textu, které následně posílali jako podpis v emailech

Hacktivisté, hackeři a ti ostatní

Hacktivismus není vždy o "hacku". DDoS útok není *hack* jako takový. Jak se v roce 1998 vyjádřil člen cDc[33] *"Omega"* při popisu NetStrike[34]: použil termín *"virtual sit-in"*. Ale připojit se k DDoS útoku nevyžaduje téměř žádné technické znalosti. Což je na jednu stranu pozitivum pro organizátory DDoS, díky jednoduchým nástrojům jako LOIC[35] se může zapojit co nejvíce lidí (což je pointa). Na druhou stranu nízký práh vede v digitálním světě k slacktivismu. Mám pocit, že slacktivismus bude velmi brzy důležitější termín, než samotný hacktivismus.

Když jsem na začátku psal o tom, že být digitálním aktivistou bude znamenat více, než psát protivládní blog a přispívat na uzavřené fórum - má tento jev i druhou stranu. Hacktivismus v dnešní podobě počítá s účastí širší digitální veřejnosti. Proto dochází ke zjednodušování témat a jejich převodu na lépe stravitelné a šiřitelné myšlenky. Heslovitost se stává hybatelem - myslím, že pro vývoj internetu blízké budoucnosti se musíme blíže podívat na to, jak fungují např. internetové memy a virální videa. Musíme více vnímat propojení politiky a marketingu.

Když se podíváme na výše zmíněné události, uvidíme, že kolem všech se vybudoval velmi jednoduchý étos a příběh o boji za pravdu *(Wikileaks)* spravedlnost *(#occupy a protesty proti SOPA/PIPA)* a svobodu *(Arabské jaro)*. Jednoduché příběhy - avšak jen na pohled, protože všechny z nich přesahují internet. Stejně tak #occupy protesty stojí za změnu[36], avšak neví jakou.

33 Cult of Dead Cow

34 de facto starší název pro DDoS

35 LOIC je skutečně jednoduchý. Během několika hodin se mi podařilo vytvořit podobný program v HTML5

36 Opět je to zabstrahovaný korporátní/bohatý nepřítel někde nahoře, kteří vše kontroluje a řídí.

Hacktivismus se snaží nostalgicky napodobovat hackerskou symboliku: LulzSec používali ve svých zprávách ASCII art. Často se také odkazovali k Anonymous. Dříve však Anonymous byla spíše myšlenka, společný a prázdný virtuální štít, který byl právě díky své prázdnotě tak stěží uchopitelný[37]. Neexistovalo žádné *„patřit do Anonymous“* - všichni byli Anonymous, jak říká heslo ‚*WE are Anonymous*‘. Dnes se o Anonymous hovoří jako o skupině. Někdo může *patřit k #AntiSec, ale nepatřit k Anonymous*[38].

K současnému hacktivismu dnes velmi často patří populistické slogany a jejich tupé opakování. A hlavní témata? Desítky let stará hesla o svobodě informací. Současný západní hacktivismus, ačkoliv prezentován jako mladý prvek na politické scéně (někde se tak daleko zatím nedostal), je neprogresivní plácání se v bezpečném rybníčku digitálních práv. Je to hraní na hrdiny a padouchy. Jeho autenticita pramení pouze z toho, že pochází z temně vypadajících krajin hackerství, které si pouze půjčuje. Je to de facto populární zábava. Slacktivistická hra na politiku.

---

37 Stačí zkoumat jak se o Anonymous vyjadřovaly média v době boje proti Scientologické církvi

38 A hacker going by the name Thehacker12, a self-purported AntiSec supporter but not a member of Anonymous - http://en.wikipedia.org/wiki/Operation_AntiSec

Hacktivismus žije!

Neznamená to však, že hacktivismus neexistuje. Hacktivismus existuje. Hackeři, kteří dříve skutečně plnou měrou stáli za hacktivismem, nezmizeli. Přes ukřičené hacktivisty jsou pouze méně vidět. Hacktivisté nejsou lidé, kteří si LOIC zapnou na svém PC. Hacktivisté jsou lidé, kteří LOIC napsali. *The Code is the Law* nabývá nového politického významu. Programátoři a hackeři jsou novou politickou elitou[39]. Kupříkladu 28C3 (28. konference CCC) a její témata[40] ukázala, že hacktivistická elita se stále snaží hacktivismus posouvat dál.

Současní hacktivisté nám neustále podstrkují ideu konfliktu a nutnost boje. Samozřejmě, hackeří často vznikají z konlfiktu s mocí, kdy něco nemůžou dělat nebo nemůžou něco prozkoumat. Ale idea boje *za internet* zní naivně. Obzvláště nemají-li hacktivisté žádné prostředky, než DDoS a leaky informací. Více hacktivistický přístup by se držel toho, v čem je silný - hackování.

Hacktivismus má potenciál měnit. Pokud se objeví zákony a regulace jako Series of tubes/ACTA/SOPA/PIPA - *hack the law*. Najde si své cesty jak žít dále. Pokud někdo zakázal vyvážet kryptografii - hackeři objevili možnost jak kryptografii exportovat.

Jaké otázky stojí za to si klást: co bude s hacktivismem, když mainstreamová média pochopí, že DDoS nic neznamená a že Anonymous je simulakrum? Až přejde optimismus spojený s revolucemi a novými médii? Hacktivistům jde přece o to být vidět a mít dopad skrz klasická média (LulzSec, Arabské jaro), co si počnou bez odezvy?

---

39 Meet the new political elite: Computer programmers. The Washington Post [online]. 10. leden 2012 [cit. 2012-01-27]. Dostupné z: http://www.washingtonpost.com/blogs/innovations/post/meet-the-new-political-elite-computer-programmers/2010/12/20/gIQAfcg9nP_blog.html

40 http://ondemand.28c3.fem-net.de/

Hlavní zdroje

Morozov - Net Delusion // @evgenymorozov
Furedi - Culture of Fear
Lévy - Hackers
Denker - Does Hacktivism Matter?

Další zdroje

Youtube: The Assassination of Julian Assange. [online]. [cit. 2011-09-15]. Dostupné z: http://youtu.be/3Fab1IsCZzY

WikiLeaks: We are under denial-of-service attack. CNET News [online]. 28.9.2010 [cit. 2011-11-12]. Dostupné z: http://news.cnet.com/8301-1023_3-20023932-93.html?tag=content;siu-container

The Jester Hits WikiLeaks Site With XerXeS DoS Attack. Infosec Island [online]. 29.9.2010 [cit. 2011-11-12]. Dostupné z: http://www.infosecisland.com/blogview/9865-The-Jester-Hits-WikiLeaks-Site-With-XerXeS--DoS-Attack.html

Banking Blockade. Wikileaks [online]. 24.10. 2010 [cit. 2012-01-20]. Dostupné z: http://wikileaks.org/Banking-Blockade.html

The Cypherpunk Revolutionary Julian Assange: The Cypherpunk Revolutionary Robert Manne on Julian Assange. Cryptome.org [online]. Březen 2011 [cit. 2011-06-18]. Dostupné z: http://cryptome.org/0003/assange-manne.htm

Information published by WikiLeaks. In: Wikipedia: the free encyclopedia [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2012-01-20]. Dostupné z: http://en.wikipedia.org/wiki/Information_published_by_WikiLeaks

Wikileaks activist: ‚Anonymous' member, ‚Coldblood'. BBC News [online]. 9.12.2010 [cit. 2011-11-12]. Dostupné z: http://www.bbc.co.uk/news/technology-11960045

A Declaration of Cyber-War. GROSS, Michael Joseph. Vanity Fair [online]. Duben 2011 [cit. 2012-01-11]. Dostupné z: http://www.vanityfair.com/culture/features/2011/04/stuxnet-201104

Israeli Test on Worm Called Crucial in Iran Nuclear Delay. BROAD, William J., John MARKOFF a David E. SANGER. The New York Times [online]. 15.1.2011 [cit. 2012-01-11]. Dostupné z: http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?_r=2&ref=general&src=me&pagewanted=all

W32.Stuxnet Dossier. In: Symantec Security Response [online]. únor 2011 [cit. 2012-01-12]. Dostupné z: http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf

Duqu: The Precursor to the Next Stuxnet. Symantec [online]. 2011 [cit. 2012-01-12]. Dostupné z: http://www.symantec.com/outbreak/?id=stuxnet

http://vimeo.com/25412550

So, Was Facebook Responsible for the Arab Spring After All?. The Atlantic [online]. 3.9.2011 [cit. 2012-01-20]. Dostupné z: http://www.theatlantic.com/technology/archive/2011/09/so-was-facebook-responsible-for--the-arab-spring-after-all/244314/

LulzSec vs. Anonymous: Doing hactivism wrong [sic]. ITworld [online]. 16.6.2011 [cit. 2012-01-18]. Dostupné z: http://www.itworld.com/security/174917/lulzsec-vs-anonymous-doing-hactivism-wrong?source=ITWN-LE_nlt_security_2011-06-16

Dox everywhere: LulzSec under attack from hackers, law enforcement. Ars Technica [online]. 22.6.2011 [cit. 2012-01-12]. Dostupné z: http://arstechnica.com/security/news/2011/06/dox-everywhere-lulzsec-under--attack-from-hackers-law-enforcement.ars

http://pastebin.com/XDXyQ5KQ

Wired For Repression: The Surveillance Market and Its Victims. Bloomberg [online]. 20.11.2011 [cit. 2012-01-07]. Dostupné z: http://www.bloomberg.com/data-visualization/wired-for-repression/

Meet the new political elite: Computer programmers. The Washington Post [online]. 10. leden 2012 [cit. 2012-01-27]. Dostupné z: http://www.washingtonpost.com/blogs/innovations/post/meet-the-new-political-elite--computer-programmers/2010/12/20/gIQAfcg9nP_blog.html