Univerzita Karlova v Praze, Fakulta humanitních studií
Tereza Lachmanová, UČO: 6333
Bakalářská práce

Formy občanské neposlušnosti v kyberprostoru

Vedoucí práce:
Mgr. Denisa Kera

Praha 2006

Prohlašuji, že jsem práci vypracovala samostatně s použitím uvedené literatury a souhlasím s jejím eventuálním zveřejněním v tištěné nebo elektronické podobě.

V Praze dne 28.9.2006

.....

podpis

Obsah:

1. Úvod

Globální propojení světa počítačovou sítí, proces digitalizace informací a možnost jejich uchování ve virtuální paměti počítače vytvořilo naprosto nový druh prostředí: kyberprostor. Kyberprostor, jakýsi druh ne – místa. Virtuální extenze reality v sobě zahrnuje řadu jedinečných vlastností, díky nimž je možné překonávat jak limitující zákony, tak podmínky interakce ve fyzickém prostoru. To vše dává šanci zrození a růstu nových kulturních forem pohybujících se právě v prostředí digitalizovaných informací, v prostředí, které není determinováno časem ani prostorem.

Počítače a počítači zprostředkovaná komunikace si velice rychle dokázala kolem sebe sama vytvořit svůj vlastní svět. Digitální svět či kybérie má již dnes nespočetně mnoho obyvatel: od běžných uživatelů moderních informačních a komunikačních technologií až po nové, leckdy marginální, chaotické a neviditelné subkultury žijící na úplném okraji kybernetického světa.

Cílem této práce bude snaha popsat a analyzovat právě taková sociální hnutí, která vznikají na základech idejí a artefaktů spjatých s moderními informačními technologiemi a která existují pouze v kyberprostoru či jsou jejich programy a praktiky silně kyberprostorem ovlivněny. Hlavními charakteristikami těchto skupin jsou především využívání a udržování práva občanů na svobodný tok informací, svobodu projevu, svobodu intelektuálního vlastnictví a ochrany soukromí v prostředí internetu a všech počítačových sítí. Další charakteristikou je originální využití moderních technologií k uskutečnění jejich politických a socio-

kulturních cílů. Pro všechny skupiny od *hackerů* přes *hacktivisty, kryptoanarchisty, kyberfeministky,* mediální aktivisty, až po jednotlivé nezařaditelné virtuální komunity a jednotlivce bloudící po kyberprostoru, je možné i přes různorodost cílů a technik nalézt společného jmenovatele. Všichni využívají počítačové technologie způsobem, který neodpovídá záměru, pro který byly vytvořeny. V mnoha případech za účelem útoku na převládající společenské normy a názory týkající se politicko-ekonomických systémů, nepsaných společensko-kulturních pravidel či konzumního způsobu života a zábavy.

Svou pozornost zaměřuji především na subkulturu hackerů a z ní vzrostlé nové odnože hackování - hacktivismus, jehož základy spočívají v aplikování a rozšíření teze o právu na občanskou neposlušnost. Hacktivismus je aktivismem ve virtuálním prostoru, k čemuž využívá všech možností, které tento prostor nabízí, a také kreativních schopností hackerů, jejich prostředků a filozofie. Zásadním rozdílem mezi nimi je fakt, že hacktivisté se snaží svojí aktivitou upozornit širokou veřejnost na určité politické a společenské kauzy.

Aby bylo opravdu možné pochopit filozofii a aktivity vyvíjené mnou vybranými kybersubkulturami, je zapotřebí zpočátku přiblížit oblast, ve které se tyto skupiny pohybují. Na začátku své práce tedy předkládám několik teorií zabývajících se vlastnostmi kyberprostoru, svobodami a možnostmi, které nám nová extenze reality umožňuje, ale také tím, co nám tato nová virtuální realita může z fyzického světa a života odejmout. Blízká těmto subkulturám bude například teorie Hakima Beye o nových teritoriích svobody a dočasně autonomních zónách, či popis Kyberie Douglasem Rushkoffem. Pro porovnání předkládám také teorie, které budou těmto skupinám vzdálené, jako například teorie Paula Virilia o „nemoci zrychlené dopravy“[1] a informatické bombě či teorie Jeana Baudrillarda o internetové totalitě nahrazující realitu.

[1] Virilio P.: *Informatická bomba*, z francouzského orig. *La bombe informatique*, Galilée 1999, přel. M. Pacvoň, Červený Kostelec, nakl. Pavel Mervart 2004, 49 s.

2. Kyberprostor: hájemství digitalizovaných informací

Díky pokroku ve vývoji informačních a jiných moderních technologií se kyberprostor postupně z produktu literární představivosti autorů kyberpunkové literatury, těmi nejznámějšími jsou například William Gibson či Bruce Sterling, přerodil v pojem označující skutečný sociální prostor, v němž, ať už dobrovolně nebo z nutnosti, žije minimálně většina technologicky vyspělého světa. Telefony, faxy, počítače a bezdrátová technologie[2] se staly víceméně naprostou samozřejmostí pro čas strávený zaměstnáním, ale stejně tak i pro volný čas. Pro někoho se staly jediným možným nebo nejvíce schůdným prostředkem komunikace s druhými. A jsou to právě především moderní informační technologie, které citelně a nejvíce zasáhly mezilidské vztahy na všech úrovních. Jimi se nám otevřel nový digitální svět, nový prostor – kyber prostor. Douglas Rushkoff ve své knize *Kyberie, život v kyberprostoru* píše: „Dnes, kdy jsou osobní počítače propojeny do sítí, jež obepínají zeměkouli a sahají i mimo ni, tráví mnoho lidí většinu svého času tam venku v „kyberprostoru“ – v hájemství digitální informace.“[3]

Jednou z prací systematicky se zabývající kyberprostorem je studie francouzského filozofa a univerzitního profesora Pierra Lévyho *Kyberkultura: Zpráva pro Radu Evropy v rámci projektu „Nové technologie: kulturní spolupráce a komunikace“*. Důležitým faktem pro Lévyho je skutečnost, že kyberprostor jako takový nevznikl jako záležitost řízená státní mocí nebo mocí korporací, přestože jimi byl počátku silně podpořen, ale

[2] Jedná se o tzv. wireless technologies, označované jako Wi-Fi , tedy bezdrátové technologie, která umožňuje přenášet data ne prostřednictvím kabelů, ale vzduchem skrze radiové vlny. Např. Bluetooth.
[3] Rushkoff D.: *Kyberie, život v kyberprostoru*, z ang. org. *Cyberia*, HarperCollins 1994, přel. S. Neumann, Praha, SPVČ 2000, 012 s.

spíše jako experimentální počin mladé generace snažící se nalézt nové, alternativní způsoby komunikace, nezávislé na mainstreamových médiích.

Z technického hlediska se jedná o „komunikační prostor otevřený vzájemným světovým propojením počítačů a počítačových pamětí“.[4] To, co především tato sdílená počítačová síť umožňuje, je komunikace na dálku, neomezená geografickými principy. A tak se mohou různé sociální skupiny a komunity sdružovat čistě na základě společných zájmů a znalostí bez potřeby a nutnosti překonávat fyzické vzdálenosti a společenské bariéry.

Z hlediska socio-kulturních dimenzí můžeme o kyberprostoru hovořit jako o prostoru univerzálním, otevřeném, interaktivním, globálním, decentralizovaném a fluidním. Univerzalita tohoto ne–místa je dána z velké části právě díky digitalizaci informací. Hlavním projevem a vlastností kyberprostorové univerzality je možnost kohokoliv do tohoto prostoru vstoupit, čerpat z něj a obohacovat ho o jakékoliv informace. Zapotřebí je jen přístup k určitým technologiím. Všichni jeho návštěvníci se podílejí na upevňování této univerzality a svým způsobem na bourání totality geofyzického světa svými interakcemi, definicemi a redefinicemi již zveřejněných informací. Po pojmu globální vesnice, o které ve spojitosti s moderním a postmoderním světem hovoří například sociolog Anthony Giddens, se nyní objevuje nový pojem globální elektronické vesnice. A i ta, stejně jako vesnice reálná či již zmíněná globální, má své přednosti a svá úskalí. „Nebezpečí takové komunikace spočívá v tom, že na každý příspěvek jsou upřeny stovky, možná tisíce potenciálně

[4] Lévy P.: *Kyberkultura, Zpráva pro radu Evropy v rámci projektu „Nové technologie: kulturní spolupráce a komunikace“*, z fr. orig. *Cyberculture (Rapport au Conseil de l´Europe)*,Éditions Odile Jacob / Éditions du Conseil de l´Europe 1997, přel. M. Kašpar, A. Pravdová, Praha, Karolinum 2000, 83 s.

kritických očí. Každý chybný údaj může být rozpoznán, lež odhalena, na plagiátorství se přijde. Kyberprostor je jako sérum pravdy. Porušení kybernetické morálky či vesnické etiky okamžitě vyjde najevo a šíří se komunikačními okruhy celé datasféry rychlostí světla.“[5]

Douglas Rushkoff tedy popisuje kyberprostor jako globální elektronickou vesnici, kde přestaly platit zákony lineární reality, neboť vzdálenosti, které lidi oddělovaly, již neplatí a všichni jsme tak víceméně svými sousedy, o kterých se vždy můžeme dozvědět přesně to, co právě dělají. Prostřednictvím tohoto nového a globálního prostoru se může propojovat a šířit informace velké množství různých lidí bez ohledu na geografické, časové, národnostní či náboženské omezení. Kyberprostor tak může být obrazem globalizačních tendencí, avšak bez možné přímé kontroly, neboť globální síť není omezena fyzickými hranicemi jednotlivých států a nepodléhá tak vybudovaným tradičním principům suverenity a kontroly. Se vznikem globálních a elektronických vesnic však například nesouhlasí Jaron Lanier, tvůrce pojmu virtuální reality a člověk, který založil první společnost zaměřenou na aplikaci virtuální reality *VPL Research*. „Nevznikla žádná globální vesnice. Konečně jsme uviděli, co se stane, když informační technologie ovládnou svět. Vesnice je něco stabilního, kde každý zná svou roli. Místo toho se ale všechno dalo do pohybu.“[6]

Lidstvo rozšířilo svět a život o jedno další pole působnosti, které nenabízí jen pouhé produkty a obsahy určené k pasivnímu přijímání, konzumaci. Vytvořilo nové, zcela dynamické prostředí, které komukoliv umožňuje miliony možností pohybu a interakcí.

[5] Rushkoff D.: *Kyberie, život v kyberprostoru*, z ang. org. *Cyberia*, HarperCollins 1994, přel. S. Neumann, Praha, SPVČ 2000, 039 s.
[6] Lanier J.:*Digitální inventura, Co se vlastně změnilo v posledních pěti letech?*, Živel, 1999, 14, 40 – 41 s.

2.1. Kyberprostor: Digitální krajina bez času, prostoru a hierarchie

V současnosti je možné převést jakékoliv informace – od vizuálních, textových až po akustické materiály, do digitální podoby. Takto zakódované a převedené informace do binární soustavy jedniček a nul lze přenášet ve velice krátkém čase a víceméně na jakákoliv místa po celé planetě, kde se nacházejí k tomu potřebné technologie (telefonní připojení, popřípadě v současnosti se rozšiřující bezdrátové připojení, počítač a modem). Čas i prostor se již v předávání zpráv a informací jeví jako irelevantní, časoprostorová dimenze tak ztratila svůj význam. Můžeme sedět kdekoliv na světě, kde bude již zmíněné vybavení, a v ten samý okamžik komunikovat s kýmkoliv jakkoliv vzdáleným, dokonce i s jakkoliv velkou skupinou lidí a to prostřednictvím různých kyberprostorových diskusních klubů, které umožňují simultánní interakce většího množství lidí.

Další důležitou vlastností kyberprostoru je multidimenzionalita, která je založena na nelineárním uspořádání digitální sítě, například v podobě hypertextu. Díky němu se můžeme při vyhledávání informací volně pohybovat po sítí hypertextových odkazů, zavádějících nás vždy na nové internetové stránky, jež opět o něco rozšiřují námi hledanou informaci. Každá nová webová stránka je také novým zdrojem informací. Díky hypertextům je také kyberprostor decentralizovaný a otevřený, chybí mu centrum a hierarchie. To vše znemožňuje systematickou kontrolu, ale zároveň tím umožňuje také vytvářet v kyberprostoru nové teritorium svobody.

2.2. Internet jako slušná varianta anarchie.

Na počátku šedásátých let 20. století se Ministerstvo obrany Spojených států obrátilo na americké univerzity s žádostí o vypracování studie o počítačových vědách. Důvodem nebyla pouze potřeba vylepšení úrovně armádních tajemství, která se extrémně zvyšovala s vynálezem a užíváním atomových zbraní, ale také potřeba Spojených států reagovat na vypuštění sovětského satelitu Sputnik v roce 1957.[7]

V roce 1962 zahájil J.C.R. Licklider z MITu[8] program na výzkum počítačů DARPA, jehož hlavním cílem bylo vytvořit globálně propojenou síť počítačů, ze které by měl kdokoliv rychlý a snadný přístup k potřebným datům a programům z jakéhokoliv místa v počítačové síti. Projekt DARPA s pomocí počítačových a jiných odborníků posléze vykrystalizoval ve vojenský projekt nazvaný ARPAnet, který byl financován jedním z oddělení amerického Ministerstva obrany.[9] Tak se objevila již víceméně současná podoba Internetu, „který byl původně navrhován jako decentralizovaná komunikační síť určená k udržení velení, kontroly a komunikace v případě nukleární války“.[10]

Univerzity a instituce, jako například *MIT* či *Stanford*, které na tomto projektu pracovaly, však začaly tento projekt používat i ke svému prospěchu, tedy k potřebě sdílet znalosti a výsledky výzkumů. Tak se započala cesta Internetu jakožto

---

[7] Hauben M.: *History of ARPANET, Behind the Net – The untold history of the ARPANET*, nedatováno, [cit. 23.6.2006]. Dostupný z: http://www2.dei.isep.ipp.pt/docs/arpa.html

[8] Michigan Institut of Technology

[9] Cerf G.V., Clark D.D.,Kahn E.R.,Kleinrock L., Leiner M.B., Lynch C.D.,Postel J.,Roberts G.L., Wolff S.: *A Brief History of the Internet*,

Internet Society, 2003, [cit. 23.6.2006]. Dostupný z: http://www.isoc.org/internet/history/brief.shtml#cerf

[10] Thomas D.: *Hacker Culture*, Minneapolis, The University of Minnesota Press 2002, 14 – 15 s.

prostředku a nástroje k volnému šíření informací dostupných komukoliv, kdo o ně má zájem a přístup k potřebné technologii.

Důležitým momentem na cestě rozšíření Internetu mimo univerzitní instituce bylo připojení tzv. BBS (Bulletin Board Systems) budovaných po celých Spojených státech na principu a technologii telekomunikačních propojení. V takto vystavěné a rozšiřující se síti rozpoznaly jednotlivé korporace a především státy ohromný potenciál, a proto byly ochotny finančně podpořit projekt Internetu na tolik, že se z něho mohla v průběhu deseti let stát síť globálního rozměru. A přestože se může dnes mnoho lidí domnívat, že takto vzniknuvší kyberprostor podlehl ekonomické a politické nadvládě, je nutné uvědomit si, že stále díky svým vlastnostem poskytoval a neustále poskytuje prostor pro jakoukoliv skupinu a jakýkoliv projekt, který tuto digitální krajinu dotváří, vylepšuje a obohacuje, ale na druhé straně také i pro ty, který tento prostor ničí a zneužívají.

„Slušná varianta anarchie je očividně možná. Už to bylo řečeno mnohokrát, ale ještě stále to není banální prohlášení: Web vytvořily miliony lidí proto, že ho chtěly, jako místo bez chamtivosti, strachu, hierarchie, autorit, etnického rozlišování, reklam nebo jakékoliv formy manipulace. Nic takového dosud lidstvo nepoznalo.“[11]

[11] Lanier J.:*Digitální inventura, Co se vlastně změnilo v posledních pěti letech?*, Živel, 1999, 14, 40 – 41 s.

2.3. Zrychlování reality aneb realita reálnější než realita

> „Nemoc rychlé dopravy – nezývaná kinetóza, která z nás na omezenou dobu dělá motorizované tělesně postižené, cestující voyeury – logicky předchází nemoci okamžitého přenosu, s níž brzy přijdou narkomani multimediálních sítí, net – junkies, webolici a ostatní kyberpunkeři postižení nemocí IAD (Internet addition disorder). Jejich paměť se stane vetešnictvím, odpadem přeplněným hromadou obrazů vší možné provenience, opotřebovanými symboly ve špatném stavu, nakupenými bez ladu a skladu.“[12]

Kybernetický svět nám otevřel tedy nové místo pro život, místo setkávání se, výměny informací a zkušeností. Ovšem stejně tak je nutné uvědomit si, že nám zároveň postupně odebírá různé a stále ještě běžné zkušenosti života fyzické reality. Internet a celý kyberprostor může být jak tím nejlepším tak i tím nejhorším. Fenomény odvrácené stránky informačních a vůbec nových technologií se blíže zabývají filozofové a sociologové jako například Paul Virilio či Jean Baudrillard.

Paul Virilio ve své knize *Informatická bomba* zdůrazňuje dva komplementární aspekty současné globalizace. Těmito aspekty jsou „na jedné straně extrémní redukce vzdáleností vyplývající z ČASOVÉ KOMPRESE dopravy a přenosu, a na druhé straně probíhající generalizace TELEDOHLEDU“.[13] Teledohledem je zde myšlen dohled nad čímkoliv a kýmkoliv na dálku, umožněný právě prostřednictvím kybernetické interaktivity „v elektronickém éteru našich moderních telekomunikačních

[12] Virilio P.: *Informatická bomba*, z francouzského orig. *La bombe informatique*, Galilée, 1999, přel. M. Pacvoň, Červený Kostelec, nakl. Pavel Mervart 2004, 49 s.
[13] Tamtéž, 22 s.

prostředků“.[14] Přesněji pak říká: „Slavná „virtuální realita“ tedy není ani tak plavbou KYBERNETICKÝM PROSTOREM sítě, jako hlavně ROZŠÍŘENÍ OPTICKÉ ŠÍŘKY zjevů reálného světa.“[15] Z tohoto důvodu je pak podle něj naprosto nutné rozdělit původní geofyzickou realitu a vypracovat tzv. stereo–realitu, složenou jak z aktuální reality tak z virtuální reality mediálních trans-zjevů. A pokud nebudeme takového rozdělení schopni, hrozí nám podle Virilia ztráta smyslovosti, neschopnost používání našich receptivních orgánů, ztráta fyzického světa a bezprostředních počitků, víceméně všeho, co je člověku nejvíce vlastní. Postupně bychom se všichni mohli přerodit v internauty, tedy kosmonauty pohybující se po internetu, ale v něm zároveň uzavřeni a odděleni od skutečné reality.

Díky našemu nekritickému přijímání a oslavování techniky a technologie ztrácíme podle Virilia vlastní svobodu chování, sklouzáváme „k technokultuře a v posledku k dogmatismu *totalitního technokultu*, kdy je každý chycen v pasti. Ne v pasti nějaké společnosti, jejích zákonů či jejích morálních, sociálních, kulturních a jiných zákazů, nýbrž v pasti právě toho, co z nás, *z našich vlastních těl*, udělala staletí pokroku“.[16]

Dalším zásadním aspektem kybernetické sítě sítí je problém nové informační revoluce, která s sebou nejenom že přináší „revoluci všeobecného udavačství“[17], umožněnou skutečností teledohledu, ale také nové a četné prostředky na doposud nejrozsáhlejší a nekontrolovatelné proměny mínění. „Po první bombě, po atomové bombě, která dokáže prostřednictvím radioaktivní energie rozbít hmotu, se na konci tisíciletí

---

[14] Virilio P.: *Informatická bomba*, z francouzského orig. *La bombe informatique*, Galilée, 1999, přel. M. Pacvoň, Červený Kostelec, nakl. Pavel Mervart 2004, 15 s.

[15] Tamtéž, 23 s.
[16] Tamtéž, 50 – 51 s.
[17] Tamtéž, 76 s.

vynořuje přízrak druhé bomby, *informatické bomby*, která dokáže rozbít mír národů prostřednictvím interaktivity informace“.[18]

S postupnou digitalizací také dochází k opouštění analogické podobnosti blízkého a srovnatelného a k nástupu „numerické pravděpodobnosti vzdáleného“[19], samozřejmě jakkoliv vzdáleného. Tím se však dopouštíme podle Virilia jak znečištění ekologie vnímatelného, tak „znečištění vzdáleností a lhůt, z nichž se skládá svět konkrétní zkušenosti“.[20]

Dalším filozofem zabývajícím se odvrácenou stránkou úspěchů naší moderní civilizace je Jean Baudrillard, který tvrdí, že srovnáme-li moderní koncepci klasických map a jejich vazbu na nereprezentovatelnost totality skutečného světa, pak internet, jakožto postmoderní mapa, se stává sám totalitou nahrazující reálný svět. Tento moment nazývá precesí simulaker, moment, kdy původně model určuje a definuje svět, jenž zpočátku jen napodoboval. Přičemž internet už jednoduše neurčuje síť jednotlivých propojení a neruší vzdálenosti, ale „vytváří a udržuje svoji vlastní simulaci světa v prostoru světa fyzického a s jeho prostorovými vzdálenostmi“.[21] Jak skutečná realita tak lidské tělo se postupně jeví jako něco zbytečného a rozsáhlého. „Technologie již neobklopuje svět, nyní ho nahrazuje simulací „reality reálnější než realita“.“[22] Simulaci „reality reálnější než realita“ nazývá Baudrillard hyperrealitou, jež je dále tvořena simulakry, tedy znaky, u nichž však již nelze rozlišit, do jaké míry se vztahují k realitě nebo zda jsou již čistou virtualitou. Dostáváme se tak podle Baudrillarda k okamžiku katastrofy, kdy se

---

[18] Virilio P.: *Informatická bomba*, z francouzského orig. *La bombe informatique*, Galilée, 1999, přel. M. Pacvoň, Červený Kostelec, nakl. Pavel Mervart 2004, 76 s.
[19] Tamtéž, 131 s.
[20] Tamtéž, 134 s.
[21] Nunes M.: *Baudrillard in Cyberspace: Internet, Virtuality, and Postmodernity*, Georgie Perimeter Collage, 1995,[cit. 16.8.2006]. Dostupné z: http://www.gpc.edu/~mnunes/jbnet.html

[22] Tamtéž

jazyk, významy znaků definovaných jejich vztahem k jevům reálného světa z tohoto světa naprosto vytrácí. Podle Baudrillarda se tak vytrácí základní systém utvářející naše myšlení.

„V prostoru symbolické totality „světa“ nám internet nabízí simulovaný svět totality, uzavřenou smyčku bezprostřednosti a průhlednosti. Zkušenost v tomto simulovaném světě se stává zkušeností kybernetické reality: již neexistuje realita, nýbrž virtualita.“[23]

2.4. Kyberprostor. Mainstream a počítačový underground.

Spíše než hmatatelným, konkrétním místem je kyberprostor *ne–místem*, nezmapovatelnou, hyperdimenzionální realitou s nesmírným počtem digitalizovaných informací, virtuálních komunit, interakcí jednotlivců a skupin rozličných zájmů a zaměření.

V kybernetickém oceánu dnes nalezneme různá sociální hnutí. Některá již dnes natolik známá, že je není možné označovat za subkultury, některá, která tak rychle, jak se objeví, zmizí v temnotách digitálního vesmíru, a další, která se komercionalizují a zapojují do silného proudu mainstreamu nebo naopak zůstávají záměrně schována a nepoznána v tajných chodbách datasféry. Existuje zde tedy zřetelný rozdíl mezi těmi, kdo se rozhodli kolonizovat kybernetický svět za účelem ekonomické a politické kontroly a využití toků globálního kapitálu, a těmi, kdo se v něm pohybují za účelem vytvoření nových teritorií svobody, enkláv kulturního a sociálního odboje.

[23] Nunes M.: *Baudrillard in Cyberspace: Internet, Virtuality, and Postmodernity*, Georgie Perimeter Collage, 1995,[cit. 16.8.2006]. Dostupné z: http://www.gpc.edu/~mnunes/jbnet.html

Sledování těchto digitálních undergroundových a avantgardních hnutí nám poskytuje zároveň pohled na současnou masovou kulturu, neboť jsou to většinou právě subkultury, které dávají vyniknout tvarům a směrům mainstreamové kultury, a zároveň jsou to také ony, jež jsou schopny uvést v život nové trendy a bořit zastaralé, tradiční formy a hodnoty. To, co se nám může jevit jako okrajová a bezvýznamná záležitost, se v budoucnosti může projevit jako revoluční změna.

Kyberprostor tak není pouhou technologickou záležitostí propojených počítačů do společné sítě, je také novou společenskou formou, otevřením nových prostorů pro myšlení a jednání lidí, které se mohou odrážet na všech aktivitách jak jednotlivců, tak celých společenství. „Pavučina propojených počítačových sítí poskytuje výsostné elektronicko-neurologické rozšíření působnosti pro rozvíjející se lidskou mysl. Překračovat tuto technologickou hranici lidského vědomí znamená znovu definovat samu podstatu informace, lidské tvořivosti, vlastnictví a mezilidských vztahů“.[24]

Vše, co se odehrává na vlnách kybernetického oceánu, není pouze technologickou záležitostí, ale také záležitostí sociální, kulturní a možná především filozofickou.

---

[24] Rushkoff D.: *Kyberie, život v kyberprostoru*, z ang. org. *Cyberia*, HarperCollins 1994, přel. S. Neumann, Praha, SPVČ 2000, 021 s.

3. Nová teritoria svobody

> „...udeř a uteč. Uveďte do pohybu celý kmen, i kdyby mělo jít jen o data v Síti.“[25]

Mnoho autorů a členů různých subkultur vnímá kyberprostor také jako svým způsobem novou dimenzi vnímání či jistý druh spirituality. Například v pojetí Douglase Rushkoffa je kyberprostor rozšířen také na zkušenosti, jež nemusí být zprostředkovány výhradně informačními technologiemi. Podle jeho názoru se spíše jedná o stav mysli, duševní krajinu, do které lze vstoupit několika způsoby, ať už prostřednictvím výše zmíněných technologiích nebo například pomocí různých chemických látek. „Kyberprostor je také určitou metaforou, která odpovídá mnoha dalším druhům lidské zkušenosti. Drogy, tanec, duchovní techniky, matematika chaosu a pohanské rituály – to všechno uvádí člověka do podobných sfér vědomí, kde omezení časem, vzdáleností a tělesnou schránkou ztrácí svůj význam. Lidé se těmito prostory pohybují podobně jako počítačovými programy či videohrami – bez limitujících zákonů lineární, hmotné reality.“[26]

Tak se mohl v takto vnímaném kyberprostoru zrodit i nový typ kočovníka – elektronického nomáda pohybujícího se z místa na místo. Aby mohl šířit informace nepotřebuje již překonávat žádné fyzické vzdálenosti. Jednoduše vstoupí do kyberprostoru, jako bojovník za svobodu, jako rozvraceč systému a řádu, jako prorok, či jakkoliv jinak. Neboť kybernetický svět umožňuje jak podrývání tak také posilování moci. Elektronický nomád

---

[25] Bey H.: *Dočasná autonomní zóna*, z ang. org. *Temporary Autonomous Zone*, neuvedeno, 2004, přel. Blumfeld, Praha, Tranzit 2004, 009 s.

[26] Rushkoff D.: *Kyberie, život v kyberprostoru*, z ang. org. *Cyberia*, HarperCollins 1994, přel. S. Neumann, Praha, SPVČ 2000, 012 s.

nemusí být osamocený a izolovaný, může libovolně vytvářet či se spojovat s kteroukoliv kybernetickou komunitou či skupinou. Jakmile začíná pociťovat, že ho určitý systém, společenství nebo instituce svazují, může a vlastně musí zmizet. Tak se mu daří unikat spárům autorit a dále šířit nové informace.

Nomádství, rezistenci a kmenovost kybersubkultur je možné vysvětlit na základě teorie dočasně autonomních zón (D.A.Z.), vytvořené anarchistickým teoretikem Hakimem Beyem. Ten svoji pozornost ve své knize *Dočasná autonomní zóna* zaměřuje na koncept vymaňování se z autority a moci. Vše se děje na principu vytváření osvobozených prostorů, kde jejich návštěvníci mizí dříve, než stát a společnost přijde na jejich porušování všeobecně přijímaných a tím pádem dominantních společenský pravidel a řádů. Svoji teorii Hakim Bey staví na pirátských utopiích a vyprávěních o korzárech, kteří v osmnáctém století brázdili oceány, a o jejich systému informačních sítí. Systém byl vždy postaven tak, že jim umožňoval neustále unikat a žít mimo zákony společností, které je kriminalizovaly. A právě paralelu mezi těmito piráty oceánů a nomády kočujícími ať už fyzickým prostředím nebo kyberprostorem vidí ve vytváření dočasně autonomních zón, jakýchsi „enkláv svobody“.

Dočasně autonomní zóna nemá a nesmí být revolucí, neboť ta nabízí pouze nové společenské a myšlenkové uspořádání, které bude opět pro někoho nepřijatelné a bude s největší pravděpodobností opět zničeno, aby mohlo nastoupit nové, „lepší“. Revoluce je začarovaným kruhem, ve kterém nedocílíme nikdy opravdové svobody. D.A.Z. je podle Beye povstáním, které není přímo namířeno proti státu, ale je operací „partyzánských jednotek“ a osvobozuje prostor, ať už geografický, časový,

sociální, kulturní či jen prostor imaginace. Ale ihned poté se musí rozplynout, aby se mohla obnovit na jiném místě a v jiném čase. To vše proto, aby ji stát nemohl zlikvidovat. „Povstání se svým způsobem podobá saturnáliím, které nevázanost vyprostila z jejich kalendářního sevření a nyní mají svobodu začít kdykoli a kdekoli. I když je vzpoura nezávislá na čase a místě, neztrácí čich pro nazrálost situací a je spřízněna s geniem loci.“[27]

Udeř a uteč – neustálé unikání a mizení je nejdůležitější a nejsilnější stránkou konceptu D.A.Z.. Pro nomáda, který není ukotven na jednom místě, nabízejí veškerá místa nové možnosti a výzvy. A právě v tom spočívá celá taktika D.A.Z. – přeskupování z místa na místo, oživování a osvobozování dalších prostorů, ale pouze za podmínky její neviditelnosti, bez které by nikdy nemohla začít fungovat. V neviditelnosti spočívá její největší síla. „Stát ji nedokáže rozpoznat, protože historie nedisponuje žádnou její definicí. Jakmile je D.A.Z. někde pojmenována, musí se rozpustit, rozplyne se a zanechá po sobě jen prázdnou slupku, aby se znenadání objevila znovu někde jinde, opět neviditelná, protože nedefinovatelná.[...] D.A.Z. je tedy dokonalou taktikou pro oblast, v níž Stát působí jako všudypřítomný a všemocný, a přesto současně plný skulin a děr.“[28]

Na D.A.Z. se také podle Beye silně podílí ještě jeden faktor, kterým je Síť informačního propojení. Nutno dodat, že se nejedná pouze o informační a komunikační propojení prostřednictvím technologie. Na Síti informačního propojení se podílejí také vyřknutá slova, pošta, časopisy a jiná média. Rozlišuje existenci Síťě (netu), v jejímž rámci se však postupně začala vynořovat jakási otevřená pavučina, kterou nazývá Webem. *Net* je totalitou veškerých proudících informací a přenosů, z nichž některé mohou být privilegované a pro některé tedy nepřístupné. Z tohoto důvodu je také Net do určité míry uzavřený a hierarchický, zatímco *web* či pavučina,

[27] Bey H.: *Dočasná autonomní zóna*, z ang. org. *Temporary Autonomous Zone*, neuvedeno, 2004, přel. Blumfeld, Praha, Tranzit 2004, 014 s.
[28] Tamtéž, 008 – 009 s.

disponuje otevřenou a alternativní horizontální strukturou výměny informací. Net je tak obrazně všudypřítomnou pravidelnou sítí obklopující celou planetu a web je chaoticky upletená pavučina mezi jednotlivými oky sítě, netu. V rámci webu je možné ještě rozlišit jakousi kontra–síť, kterou Bey vyhrazuje k označení utajovaného, rebelského či kontrakulturního využití webu. Pod pojem kontra–sítě pak můžeme zahrnout aktivity a jednotlivé skupiny, které budou rozebírány a analyzovány v následujících částí této práce. Jedná se například o skupiny a jednotlivce hackerů, hactivistů či činnosti softwarového a datového pirátství či o jiné jakkoliv podvratné aktivity v prostředí Beyovského webu.

4. Kontra/subkultury a hnutí v kyberprostoru

Zaměříme–li se na Beyovo rozlišení Sítě a webu pouze v rámci využívání informačních a komunikačních technologií, je to právě web a jeho kontrakulturní využití, které se stávají společným jmenovatelem všech subkultur a hnutí pohybujících se v prostředí kyberprostoru. Tyto subkultury a hnutí maximálně využívají nové technologie, ať už počítačů, samplerů, mobilních telefonů, digitálních kamer či fotoaparátů, ovšem ne z hlediska klasických spotřebitelských a konzumních principů. Moderní technologie zde slouží spíše jako prostředky a zbraně určené k rozvracení dominantních společenských, kulturních nebo politických struktur a norem, popřípadě jako prostředky k zviditelnění a zveřejnění problematických otázek týkajících se sociálního či politického fungování.

Vzhledem k charakteristikám současné celosvětové globální sítě - Internetu, jakými jsou právě decentralizace a nehierarchie, si mohla tato síť doposud zachovat odolnost vůči strategickým útokům. Z toho důvodu se ani samy subkultury a hnutí fungující v kyberprostoru nesnaží o jakékoliv vytvoření vlastní strategické centrály, která by se jednoduše a logicky stala terčem útoků jejich odpůrců (zejména státu a jeho legislativě) za účelem zneškodnit, paralyzovat nebo naprosto vymýtit jednotlivé součásti digitálního undergroundu.

A nejenom neexistence centra stěžuje vypátrání skupin provádějících podvratné až leckdy i úmyslně ilegální aktivity. Dalšími takovými faktory jsou anonymita v kyberprostoru vznikající díky možnosti vytváření alternativních identit osob pohybujících se v kyberprostoru, jako například různá ID a přezdívky uživatelů, a dále skutečnost, že je možné připojovat

se z různých IP adres[29] nebo přímo IP adresy pozměňovat a fingovat.

[29] Číslo přiděłované každému počítači zapojenému v síti.

Jak již bylo řečeno, povaha kyberprostoru umožňuje vznik a rozšiřování různorodých kybersubkultur a skupin jednotlivců s různými zájmy a cíly. Důvodů vzniku a šíření těchto alternativních skupin a hnutí je nesčetně, ať už se jedná pouze o snahu vzepřít se, vymanit se z mainstreamového proudu, dokázání si vlastní autonomie a moci nezávislé na dominantních socio-kulturních normách, prosazení specifického životního postoje, nebo o snahu přeměnit současné politické, ekonomické a sociální programy jednotlivých států či korporací.

V následujících oddílech této práce se budu snažit přiblížit některá známá a méně známá alternativní uskupení v rámci kyberprostoru, mající výše zmíněné zájmy a cíle. Pozornost však zaměřím především na skupiny hackerů a dále hacktivistů, jejichž jediným důvodem a cílem je právě prosazení změn v politických, ekonomických a sociálních strukturách prostřednictvím kyberprostoru.

5. Hackeři: piráti informační dálnice?

> „Ano, jsem zločinec. Mým zločinem je zvědavost. Mým zločinem je posuzování lidí podle toho, co říkají a co si myslí. Ne podle toho, jak vypadají. Mým zločinem je to, že jsem chytřejší než ty, a to je to, co ty mi nikdy neodpustíš.“[30]

Subkulturu hackerů by bylo možné považovat za nejambivalentnější společenství pohybující se v rámci kyberprostoru. To z toho důvodu, že nebýt těchto techno–nadšenců, elektronických nomádů, nevznikl by pravděpodobně nový kybernetický svět a už vůbec by se nerozšířil do téměř každého zákoutí a okamžiku každodenního života. Zároveň je však tato subkultura ve veřejných představách vnímána jako hrozba, neboť je to ona, která je možná nejvíce schopna struktury kyberprostoru nabourávat, rušit a pozměňovat. V době, kterou nazýváme „informačním věkem“, jsou hackeři těmi, kdo budují a současně nabourávají samotnou podstatu tohoto věku. Ale protože zároveň redefinují podstatu informace, vlastnictví a tím i mezilidských vztahů, představují určitou alternativu současné civilizace.

Za pomoci mediální, především senzacechtivé, kampaně, přinášející jen příběhy o kriminálních činech některých hackerů, a rozšířeného civilizačního strachu z technologie, se v současnosti vnímání „hackování“ zaměřuje jen na určité okruhy počítačové činnosti, jako například neautorizované pronikání do cizích systémů, nepovolené získávání informací, nacházejících se v počítačových sítích, a jejich zneužívání.

[30] Hacker The Mentor in Thomas D.: *Hacker Culture*, Minneapolis, The University of Minnesota Press 2002,79 s.

Ani mediální obraz a tím pádem ani představa veřejnosti se nesnaží tuto omezenou definici složitého fenoménu „hackování“ pozměnit či rozšířit. Hackeři a jejich praktiky nabourávající společenský systém, který je založen na soukromém vlastnictví, nedotknutelnosti soukromí a s ním spojeného nárůstu potřeby utajení důležitých informací, jsou v současnosti víceméně pro společnost synonymem zločinu, specifičtěji – počítačového zločinu.Opomíjeny zůstávají pozitivní aspekty této subkultury.

Zkoumáním počítačového undergroundu, digitální kultury a především subkultury hackerů se podrobněji zabývá Douglas Thomas ve své knize *Hacker Culture*. Pozornost zaměřuje především na vzájemný vztah této subkultury a mainstreamové kultury, médií a zákonů. Především zdůrazňuje, že obraz hackerů v médiích, zákonech a populární kultuře nám říká daleko více o současných kulturních postojích a strachu z technologie, než o kultuře hackerů či samotné činnosti hackování. Různé technologie a především pak počítač a elektronická síť nabízejí členům subkultury i jednotlivcům specifický způsob resistence. Tento způsob resistence ovšem směřuje k daleko širším otázkám technologie a kultury vůbec, neboť technologie je především podle Thomase o zprostředkování lidských vztahů.

Strach společnosti z technologie a potažmo strach z aktivit hackerů vysvětluje Thomas následovně: „[...] tempo technologického vývoje předehnalo schopnost společnosti tento vývoj zpracovat. Objevila se určitá technofobie, která staví technologii vždy nad nás a která vyvolává strach ztělesněný v mladých lidech současné kultury, jež umí s počítači takové věci, které není stará generace schopna pochopit.“[31]

[31] Thomas D.: *Hacker Culture*, Minneapolis, The University of Minnesota Press 2002, 32 s.

Podle Thomase je však nanejvýš důležité uvědomit si fakt, že to, co činí hackování hrozbou, nejsou jeho prostředky a nástroje (počítač, modem, telefonní linka atd.) či hacker sám, ale především technologie jakožto kulturní fenomén, který poukazuje v první řadě na lidské vztahy a způsoby, jakými jsou tyto vztahy zprostředkovány.

Tak všeobecné vnímání a chápání subkultury hackerů buď omylem nebo úmyslně opomíjí skutečnou podstatu hackování, kterému jde v první řadě o dokonalé porozumění technologiím a umění využít tyto technologie tvůrčím způsobem, i například za účelem vylepšení vztahů jak mezi lidmi samotnými, tak vztahů mezi lidmi a technikou.

Hackování v sobě v současnosti zahrnuje celou škálu činností. Od neomezeného prozkoumávání nových možností kyberprostoru, vyhledávání rizikových míst v bezpečnostních systémech a jejich následné zajištění, přes nové formy mediálního aktivismu, až po nechvalné zneužívání nedostatků počítačových systémů, počítačové špionáže, vytváření virů a krádeže dat.

5.1. Etika hackerů. Informace chce být svobodná.

Téměř od úplných počátků počítačové vědy a z ní později vzešlého počítačového undergroundu se vědci a počítačoví nadšenci řídili určitými morálními pravidly. První hackeři pracující v počítačových laboratořích na amerických univerzitách a institucích, jako Cornell, Harvard či MIT, se snažili ze společnosti odstranit pocit ohrožení z vyspělé

technologie, kterou vytvářeli, tím, že ji chtěli učinit přístupnou, otevřenou a „krásnou“. Sami sebe považovali za ochránce technologie a za svůj morální kodex pak považovali pravidla velice podobná „Zákonům Robotiky“ v podání spisovatele Isaaca Asimova. Jednak nesmí být technologie používána k poškozování lidských bytostí, a jednak informace musí být svobodná a volně dostupná, přičemž požadavek hackerů na svobodu a dostupnost informací vyústil v neobvyklý antropomorfismus a motto: „Informace chtějí být svobodné.“[32]

Postupně si tato subkultura vytvořila vlastní morální kodex zahrnující šest základních tezích. Tyto teze znamenaly určitou filozofii, kterou se řídily a nadále řídí i nové, mladší generace hackerů. Na jejich základě lze i pochopit základní motivace celé subkultury.

1. Přístup k počítačům – a cokoliv, co by tě mohlo naučit něco o tom, jakým způsobem pracuje svět – má být neomezené a absolutní. Vždy ustoupit praktickému imperativu!
2. Všechny informace mají být svobodné.[33]
3. Nevěř autoritám – podporuj decentralizaci.
4. Hackeři mají být posuzováni podle svých dovedností, ne podle falešných kritérií, jako jsou vysokoškolské diplomy, věk, rasa nebo postavení.
5. Pomocí počítače můžeš stvořit umění a krásu.
6. Počítače mohou změnit tvůj život k lepšímu.[34]

---

[32] Thomas D.: *Hacker Culture*, Minneapolis, The University of Minnesota Press 2002,11 s.

[33] V originále se jedná o heslo „All information should be free“. Anglické slovo „free“ v tomto kontextu nelze přeložit bez ztráty všech významů. „Free“ – ve významu volný, svobodný, zdarma. Informace by tedy měly být

volně dostupné, volně manipulovatelné, nekontrolované ve smyslu vlastnictví, měly by volně cirkulovat a měly by být poskytovány zdarma.
[34] Levy S. in Thomas D.: *Hacker Culture*, Minneapolis, The University of Minnesota Press 2002, 10 s.

To jsou tedy nejdůležitější principy, kterými by se měla celá komunita hackerů řídit. Samotná organizace této subkultury je založena na principech neelitářského, rovnostářského modelu prosazujícího technologický optimismus. Nejdůležitějším principem však nadále bude neustálý boj za svobodu informací a boj proti autoritám přivlastňujících si moc a právo tok informací kontrolovat. Ať už tím, že vybírají, které informace budou zveřejněny, nebo naopak které zůstanou utajeny. Informace se tak stávají pouhou komoditou na mocenském a komerčním trhu.

Jako paradox současnosti Thomas vnímá skutečnost, že nová generace hackerů v důsledku rozvoje a rozšíření technologie do naprosto běžného a každodenního života „představuje největší strach z toho, co bylo snem v šedesátých letech 20. století, tedy strach ze svobodných a otevřených informací“.[35] Osvobozováním a zpřístupňováním informací znamenají hackeři hrozbu pro společnost, jejíž nejintimnější informace jsou dnes skladovány v prostředí onoho ne–místa, v kybernetických úschovnách, do kterých mají přístup k tomu jen určení. Hrozbou se tak stává narušení či úplné zrušení tajemství, odstranění utajení, tedy skutečná svoboda informací.

Není samozřejmě pochyb o tom, že morální kodex - hackerskou etiku nedodržují všechny skupiny a jednotlivci pohybující se po tajných a utajených chodbách datasféry. Takové pak většinou sami hackeři označují jako *crackery*[36] nebo „černé hackery“, kteří programují viry a nabourávají systémy za účelem poškodit je či ukrást informace v nich obsažené.

---

[35] Thomas D.: *Hacker Culture*, Minneapolis, The University of Minnesota Press 2002, 33 s.

[36] Existuje rozdíl mezi anglickým a českým výrazem *cracker*. V angličtině se tento výraz používá pro označení zlomyslného hackera, zatímco v českém jazyce jde spíše o označení člověka zabývajícího se prolamováním kódů, které chrání software před jeho kopírováním a nelegálním šíření. Crack je pak označením softwaru, jehož zdrojový kód byl prolomen (cracknut).

A jsou to právě tyto protizákonné aktivity, které nejvíce přitahují pozornost médií a veřejnosti a stírají tak jiné, pozitivní aspekty hackerských socio-kulturních aktivit.

Důležitým prvkem v utváření etického kodexu subkultury hackerů je také dle názoru Douglase Thomase samotná mainstreamová kultura. „Na jedné straně mají hackeři vlastní kulturu. Mají své normy, terminologii, konference, místa setkání a pravidla chování. Na druhé straně je jejich kultura zcela závislá na mainstreamové kultuře a to nejen jako na něčem, proti čemu se bouří, ale spíše jako na půdě, jež mohou zkoumat.“[37]

5.2. Vznik a vývoj hackování

Hackování má svou vlastní složitou a zajímavou dějinnou trajektorii, která zahrnuje jak odlišnou paletu samotných aktivit, tak vůbec několik různorodých a leckdy i možná protichůdných postojů svých členů. Postava počítačového hackera je od určité doby nerozlučně spojována s kulturním, sociálním a politickým vývojem počítače a jako taková je komplikovaná a plná rozporů, které pramení právě z mainstreamového mediálního obrazu a kulturně podmíněného strachu z technologie.

Stejně tak různorodé je užívání výrazu „hacker“, který je v současnosti rozšířen na pojmenování mnoha různých skupin lidí a jednotlivců. Z toho důvodu je přesné definování hackera a hackování velice komplikované i pro samotné členy této

subkultury. Douglas Thomas se přiklání k variantě přemýšlet o hackerech „jako o skupině počítačových nadšenců působících

[37] Thomas D.: *Hacker Culture*, Minneapolis, The University of Minnesota Press 2002, 3 – 4 s.

v takovém prostoru a takovým způsobem, který může být správně definován ve smyslu nezměrné zvídavosti a touhy poznat fungování věci“.[38]

Aby tedy bylo možné pochopit, kdo hackeři jsou a co dělají, je nutné přiblížit si jejich historii.

5.2.1. Hacker staré školy

Historie hackerů se počíná v rozmezí padesátých a šedesátých let 20. století v počítačových laboratořích na Harvardu, MIT a Cornellu. Díky umožnění přístupu k přístrojům a finanční podpoře, která se jim dostávala od státních institucí, je možné je chápat spíše než jako stvořitele subkultury jako stvořitele institucionální, i když někdy vzdorující, kultury. Pracovali především na vývoji hardwaru a softwaru řídící vojensko–průmyslový celek a na inovacích v oblasti utajení a kontroly. Jednalo se tedy o univerzitní počítačové experty, osamělé vědce zabývající se vymýšlením a zlepšováním programů a přístrojů, které o něco málo později vedli k vytvoření prvního osobního počítače, jenž pozměnil fungování celé společnosti a vlastně vůbec umožnil zrod nové generace hackerů, operující již se svými vlastními počítači a bez jakékoliv institucionální podpory.

Tito programátoři „staré školy“ chápali svoji práci jako objevování nových teritorií, hackování pro ně bylo především intelektuálním tréninkem. Hack je tedy původně originálním

programovacím postupem, který si žádá notnou dávku kreativního myšlení a experimentování, snahou o lepší porozumění programovacím systémům. „Nejobratnější hack nespočíval

[38] Thomas D.: *Hacker Culture*, Minneapolis, The University of Minnesota Press 2002, 3 s.

v napsání nové řádky kódu, ale v nalezení způsobu, jak udělat něco s již existujícím kódem – něco, co ještě nikdy nikdo neviděl – vyřadit kód tak, aby program běžel rychleji a s větší elegancí.“[39]

V průběhu deseti let se tato „stará škola“ přestěhovala do centra technologického pokroku, kterým byla americká oblast Silicon Valley. Zde se také časem zrodila myšlenka sdílení a výměny informací prostřednictvím počítačových sítí i mimo vojensko-průmyslové záležitosti. Omezení, která přicházela ze stran vládních institucí, pro něž tito „programátoři hackeři“ pracovali, je však přiměla ke kritickému pohledu a prvním úvahám o nutnosti volného přístupu k technologiím a informacím. Byl to právě omezený a privilegovaný přístup k technologiím, jenž nasměroval počítačové nadšence ke společnému cíli: zpřístupnit počítač široké veřejnosti tak, aby se na těchto privilegiích, ale také na vylepšování softwaru i hardwaru, mohlo podílet daleko více lidí, víceméně kdokoliv se schopnostmi k tomu potřebnými. Během 70. let se pak podařilo uskutečnit technologickou revoluci zveřejněním prvních osobních počítačů, kterými byly původně Altair z roku 1975 a o rok později Apple vytvořený Jobsem a Wozniakem.

Silicon Valley se tak postupně přetvořilo v epicentrum zrodu nové subkultury, která si začala uvědomovat revoluční potenciál osobních počítačů a kritizovat jejich využívání čistě k vojenským a politickým zájmům.

5.2.2 Hacker nové školy

Zatímco byl tedy „hacker staré školy“ povětšinou diplomovaným univerzitním studentem, jejich následovníci z dob osmdesátých a devadesátých let 20. století byli podstatně

[39] Thomas D.: *Hacker Culture*, Minneapolis, The University of Minnesota Press 2002, 14 s.

mladší a měli naprosto odlišný postoj a vztah k technologii a aktivitám s ní spojených. Rozdíl mezi hackery „staré a nové školy“ tkví jednak v přístupu a hlavně v dostupnosti k technologii, a jednak také v tom, že tato mladá generace již od počátku naprosto postrádá jakoukoliv institucionální podporu. První hackeři se k počítačům dostali jen prostřednictvím počítačových laboratoří na univerzitách, jejich následovníci již díky nim k počítačům získali snadný a častý přístup. Hackování jim tak bylo umožněno praktikovat z jejich domovů a škol. Přístup mladé generace k počítačům a hackování se díky tomu značně odlišuje od přístupu hackera – počítačového profesionála.

Ohledně přístupů mladé generace hackerů osmdesátých a devadesátých let 20. století k hackování Thomas ve své knize říká: „Pro některé znamená zkoumání, učení a fascinaci vnitřním fungováním technologie, která nás obklopuje; pro jiné jde spíše o dětinské vylomeniny jako předělávání cizích webových stránek nebo umisťování pornografických obrázků na veřejné servery. Ve většině případů jde však nepochybně o přizpůsobení se „chlapecké subkultury“ věku technologie.“[40] Přičemž charakteristickými rysy této subkultury jsou především ovládnutí technologie, nezávislost a konfrontace s autoritou dospělého. Počítače využívají k tomu, aby vstoupili do světa dospělých za vlastních podmínek a tím tak ovlivňovali své sociální a někdy i fyzické prostředí.

V průběhu osmdesátých let 20. století se hackování a postava hackera dostávají také poprvé výrazněji do popředí mediálního zájmu a vůbec do povědomí celé společnosti.

S uveřejněním filmů, jako *Válka her*, *Tron* či o deset let později například film *Hackři* a ještě později *Matrix,* se rozpoutala vlna masivního zájmu o hackery a jejich aktivity.

---

[40] Thomas D.: *Hacker Culture*, Minneapolis, The University of Minnesota Press 2002, X s.

V souvislosti s takovouto mediální reprezentací a neuvěřitelně snadnou dostupností potřebné technologie se tak nechala a nechává řada i pouze průměrně technologicky zdatných jedinců inspirovat obrazem postmoderního antihrdiny – hackera. Bez přesných znalostí toho, jak které systémy pracují a fungují, se snaží o experimentální průniky do různých systémů, aniž by si uvědomovali možné důsledky takovýchto aktivit.

Tak se také nová generace hackerů rozštěpila v posledních letech na dva protichůdné tábory. Jedním z nich jsou skupiny hackerů stále respektujících původní etický kodex. Jejich aktivity, jako například nabourávání se do různých státních i korporátních systémů, jsou zaměřeny především na odhalování nedostatků v zabezpečení těchto systémů. Většinou se jedná o systémy obsahující množství osobních dat, které by bylo možné zneužít. O to skutečným hackerům ovšem nejde. Naopak upozorňují na to, že je potřeba tyto systémy lépe zabezpečovat a neustále vylepšovat.

Na základě specializace při vymýšlení nových softwarů (rozdělení práce na vývoji jednotlivého softwaru, např. testování, psaní, kódování), potřebě jednoduššího sdílení informací či taktik a spolupráce na určitých cílech, se začali tito mladí hackeři sdružovat v různých kolektivech. Nejznámějšími z těchto skupin jsou například Inner Circle, Master of Deception, Legion of Doom, Cult of the Dead Cow.

Jak se rozvíjela a rozšiřovala kultura osobních počítačů, rozdělovala se i samotná kultura hackerů. Na dodržování

hackerského etického kodexu a vylepšování bezpečnostních systémů tím, že vyhledávají chyby a nalézají způsoby, jak je opravit a odstranit, si zakládají skupiny tzv. „bílých hackerů“. Díky jejich aktivitám se rozvinulo celé odvětví počítačového zabezpečení. V opozici k nim stojí „černí hackeři“, nebo tzv. „skripteři“. Ti se povětšinou také zaměřují na hledání nedostatků a mezer v zabezpečení systému, ale za účelem jejich zneužití k zničení systému či vykradení informací v něm uložených. Případně se baví vytvářením a rozšiřováním virů poškozujících celé systémy. „Skripteři“ k hackování používají již někým předepsané programovací skripty, hacky, aniž by alespoň trochu rozuměli tomu, co dělají a jaké to může mít následky. A přesně skupiny těchto crackerů, skripterů či „černých hackerů“ jsou těmi, které nejvíce přitahují pozornost médií, veřejnosti a potažmo státu a jeho legislativy. Z toho důvodu je také všeobecně současná generace hackerů téměř výhradně spojována s počítačovou kriminalitou a vandalismem.

Velice výstižnou definici hackera přiblížil hacker Goldstein v rozhovoru pro český časopis *Živel*: „Do vašeho počítače se může vloupat kdekdo, kdekdo vám může poslat virus. Hackeři jsou ale ti, kteří vám vysvětlí, jak to dokázali. Zkrátka lidé, kteří zjišťují, jak věci fungují. [...] Hackeři neprozradí vaše soukromé údaje, ale řeknou vám: Hele, víte že Amazon používá nezabezpečený systém? Neřekne vám to Amazon, neřeknou vám to média ani vláda. To hackeři jsou ti, kteří volají, že císař je nahý. A ukážou vám proč.“[41]

5.3. Deformovaný obraz hackera

Je jasné, že současná image hackera není rozhodně založena na šesti základních tezí hackerského kodexu. To, jak veřejné mínění vnímá hackera, a to, co hacker dělá, vychází daleko více z toho, co o něm bylo napsáno kyberpunkovými autory, nebo

jak ho ztvárnili tvůrci celovečerních dobrodružných filmů o hackerech, a především pak to, co o něm bylo řečeno v médiích.

---

[41] Bella T., Adamovič I.: *Goldstein, technika, svobody: rozhovor s Emmanuelem Goldsteinem*, Živel, Jaro 1994, 19-23.

To vše se silně odráží v současném obrazu hackera a představ o něm. Leckdy nejen široká veřejnost, ale i hackeři samotní se nechávají takto mediálně a literárně vypracovanou ambivalentní či spíše zákeřnou postavou virtuálního světa ovlivnit. Vše je ještě podtrženo kulturně podmíněným strachem z technologie, který vychází především z té části společnosti, která se odmítá či již není schopna rychle se přizpůsobovat tempu technologického vývoje. Ke strachu z technologie také přispívá uživatelsky stále přívětivější hardware a software, díky kterým je sice běžný uživatel schopen vykonávat jednodušeji a více činností, ale díky kterým také čím dál méně rozumí tomu, jak počítače ve skutečnosti fungují.

Na strach lidí z technologie a z lidí, kteří ji mistrně ovládají a kontrolují, potažmo na objevení se nového světa kyberprostoru, reaguje technooptimista a nadšenec virtuální reality Jaron Lanier takto: „Dospělí jsou nervóznější. Bojí se, že ztratí kontrolu nad mladou generací, která si lépe rozumí s počítači. Jelikož rodiče nerozumí tomu, co jejich děti provádějí na Webu, množí se volání po internetové cenzuře a po kontrole komunikací, která by předčila vše, čeho kdy dosáhl jakýkoliv diktátor. Na mladé kyberžertéře lidé reagují s přehnanou histerií. Měli bychom si uvědomit toto: právě teď jsme svědky nejproduktivnější, nejinteligentnější a nejoptimističtější vzpoury mladé generace v dějinách.“[42]

[42] Lanier J.:*Digitální inventura, Co se vlastně změnilo v posledních pěti letech?*, Živel, 1999, 14, 40 – 41 s.

6. Hacktivismus. Elektronická forma občanské neposlušnosti

S nejpřímějším využitím práva na občanskou neposlušnost se v kyberprostoru setkáme v aktivitách hacktivismu. Jak již sám název napovídá, jedná se o spojení hackování a aktivismu, a to převážně aktivismu v rámci politicko–sociálních otázek. Se vzestupem možností Internetu a vůbec využití možností kyberprostoru jako celku se mnoho aktivistických hnutí, buď naprosto nebo jen své určité aktivity, přesunula do této celý svět obklopující sítě, jež víceméně umožňuje efektivní působení v jakkoliv vzdálených částech světa. Hacktivismus využívá stejných prostředků jako subkultura hackerů. Zde je však hlavním cílem především potřeba upoutat pozornost veřejnosti na některé politické či sociální problémy.

Přestože se s určitými formami aktivismu v rámci kyberprostoru můžeme setkat již od sedmdesátých let 20. století, kdy byly některé aktivity hackování ovlivněny anarchistickými a levicovými ideály hnutí hippies a tím i zpolitizovány, s označením „hacktivismus“ přišel až dlouhodobý člen známé hackerské skupiny Cult of the Dead Cow (cDc) Omega v roce 1996, snažíc se tak popsat a definovat hackování jakožto činnost s politickým záměrem. Ačkoliv toto označení bylo zpočátku myšleno spíše jako bonmot, rozšířilo se během velice krátké doby po celém světě a stalo se velice oblíbeným. „Náhle se každý stal „hacktivistou“. Nikdo neměl ani tušení, co to znamená, ale znělo to fakt dobře.“[43]

Důležitým bodem opory se pro členy skupiny cDc a především pro hackera/odborníka Oxblooda Ruffina stal závazný dokument ICCPR(The International Covenant on Civil and Political Rights)[44], jenž vstoupil v platnost dne 23. 3. 1976,

---

[43] Oxblood Ruffin: *Hacktivism, From Here to There*, Yale Law School,2004,[cit.15.7.2006].Dostupný z: http://www.cultdeadcow.com/cDc_files/cDc-0384.php

[44] Mezinárodní pakt o občanských a politických právech

a který v bodě 2 článku 19 říká: „Každý má právo na svobodu projevu; toto právo zahrnuje svobodu vyhledávání, přijímání a sdělování informací a názorů všeho druhu, bez ohledu na hranice jednotlivých států, ať už ústně, písemně či v tisknuté podobě, ve formě umění nebo prostřednictvím jakýchkoliv jiných médií dle vlastního výběru.“[45] Na základě tohoto textu Oxblood Ruffin definoval význam hacktivismu jako „užívání technologie za účelem zlepšení lidských práv napříč elektronickými médii“.[46]

Díky několika aktivistickým činům některých skupin hackerů, jakou byla například skupina LoU (Legions of the Underground), která vyhlásila kybernetickou válku proti Číně a Iráku kvůli tamějšímu porušování lidských práv a jejíž nabourání sítí výše jmenovaných států mohlo vyvolat silný mezinárodní konflikt, se koalice amerických (cDc, the L0pht, Phrack) a evropských (Chaos Computer Club, Hispahack, Pulhas, Toxyn atd.) hackerských společenství rozhodla vymezit určitá základní pravidla hacktivismu. Stát se hacktivistou neznamená jednoduše přidat ke slovu aktivista písmeno „h“.

Hacktivismus je možné označit za elektronickou formu občanské neposlušnosti. Pojem občanské neposlušnosti poprvé použil americký spisovatel H.D. Thoreau v názvu své eseje již v roce 1848. O sto let později se k myšlence o občanské neposlušnosti přihlásil Gándhí a rozšířil ji o filozofii nenásilného boje. Britská anarchistka April Carter vyučující politiku na Lancasterské univerzitě občanskou neposlušnost definuje následovně: „Pojmem se obvykle označuje úmyslné neuposlechnutí z důvodů náboženských, morálních či politických

[45] Mezinárodní pakt o občanských a politických právech, 1966, v platnost 1976,[cit.18.7.2006].Dostupný z: http://www.ohchr.org/english/law/ccpr.htm#art49

[46] Oxblood Ruffin: *Hacktivism, From Here to There*, Yale Law School, 2004, [cit.15.7.2006]. Dostupný z: http://www.cultdeadcow.com/cDc_files/cDc-0384.php

zásad. V striktním smyslu občanská neposlušnost porušuje zákon, který je sám o sobě nespravedlivý, ale pojem se vztahuje i k protestu proti konkrétní politice, jež vnímá zákon jako byrokratický produkt, nebo k tlaku ve prospěch politických reforem.“[47]

Elektronickou formu občanské neposlušnosti, zkráceně ECD (Electronic Civil Disobedience – pojem, který byl poprvé užit skupinou The Critical Art Ensemble),pak definuje člen skupiny The Hacktivist.com Metac0om ve své eseji „Co je elektronická občanská neposlušnost?“ z roku 2001 takto: „Elektronická občanská neposlušnost (ECD) je legitimní formou nenásilné, přímé akce prováděné jako nátlak na instituce zapojené v neetických a kriminálních činnostech. [...] ECD je mimo - parlamentním projevem univerzálních mezinárodních sítí, který se snaží podporovat určité politické cíle a apelovat na ducha univerzálních práv a svobod.“[48] Tato forma občanské neposlušnosti může být mechanismem, jak změnit hodnotový systém jednotlivých států, pro které je informace leckdy vyšší hodnotou než samotný jedinec. Mechanismus, který se snaží, aby se informace vrátily zpět jako služba určená lidem, nikoliv jako prostředek vydělávající peníze pouze některým institucím, nebo prostředek sloužící ke kontrole a ovládání společnosti. Hacktivismus nemá odrážet individuální zájmy jednotlivců, je výrazem hromadné nespokojenosti s fungováním státní moci či velkých komerčních společností a snahy vzniklé situace napravit

ve znění základních lidských práv. Je určitou formou resistence.

---

[47] Carter A.: *Občanská neposlušnost*, nedatováno,[cit. 25.8.2006]. Dostupné z: http://www.differentlife.cz/pravalidska06.htm

[48] Metac0m: *What is Electronic Civil Disobedience?*, 2001, [cit. 25.8.2006]. Dostupné z: http://www.thehacktivist.com/?page_id=98

V teorii ECD můžeme podle Metac0ma objevit tři různé myšlenkové rámce, které není nutné od sebe striktně oddělovat. Ve většině případech budou zastánci jednotlivých názorů souhlasit i s těmi ostatními. Jednou skupinou jsou zastánci toho, že elektronická občanská neposlušnost na internetu je jinou variantou pouličních demonstrací. Druhou skupinou jsou ti, kteří podporují a schvalují praktiky politicky motivovaného hackování a nabourávání se do počítačů a sítí. Poslední směr tvoří ta skupina, jež se snaží vyjádřit potřebu po spíše kreativně vymyšleném, hackerském řešení situace a problému na rozdíl od pouhého ničení a napadání.

ECD v mnohém odráží metody tradičních forem protestu v reálném, fyzickém světě, jakými jsou například pouliční demonstrace, fyzické blokování nebo pronikání do důležitých a strategických míst. S tím rozdílem, že díky již výše zmiňovaným vlastnostem kyberprostoru, mají aktivisté daleko více možností takto činit, aniž by byli omezeni jakoukoliv fyzickou bariérou. Tím je také možné rozpohybovat a přimět daleko větší masu lidí po celém světě k určitým akcím a protestům. Přestože elektronická forma občanské neposlušnosti probíhá v nereálném, virtuálním prostředí, má značné a leckdy dalekosáhlejší důsledky na svět reálný, než protesty prováděné přímo v reálném prostoru. A to právě díky neomezenosti v rámci geofyzických hranic ať už národních států či přímo kontinentů. Těchto vlastností jsou si však také vědomi i instituce, proti jejichž aktivitám různé formy aktivismu či hacktivismu

vystupují. Vlády, komerční subjekty, armády či teroristické skupiny mohou a využívají možností kyberprostoru stejným způsobem se stejně rozsáhlými důsledky na společnost a svět.

Stefan Wray, student doktorského studia na New York University ve své eseji *O elektronické občanské neposlušnosti* shrnuje budoucnost této nové formy občanské neposlušnosti ve vztahu k jejím tradičním formám takto: „Přestože může být z části pravdivé tvrzení skupiny The Critical Art Ensemble, že účast na pouličních demonstracích se stává stále více bezvýznamnější a marná a že budoucí resistence musí být především nomádická, elektronická a kyberprostorová, je nepravděpodobné, že fyzické, pouliční protesty, zahrnující reálné lidi na zemi, brzy ustanou. S největší pravděpodobností budeme spíše svědky toho, že se elektronická občanská neposlušnost stane nedílnou součástí nebo doplňkem tradiční občanské neposlušnosti.“[49]

Terčem hacktivistických aktivit jsou tedy zejména státy a mocenské struktury potlačující svým jednáním osobní svobody a základní lidská práva, dále také komerční a nadnárodní korporace, které se snaží zavést systematickou kontrolu kyberprostoru a učinit z něj místo čistě konzumní a vydělávající peníze.

6.1. Hacktivismus, on–line aktivismus, kyberterorismus

Vymezit přesné hranice mezi hacktivismem, on–line aktivismem a kyberterorismem není jednoduché a vzhledem k užívání víceméně stejných prostředků ani dostatečně možné. Přesto mezi nimi nalezneme minimálně jisté rozdíly v záměrech a cílech.

On–line aktivismus je neškodným a zcela legálním využíváním prostředí internetu k upozornění společnosti na určité společensko-politické problémy. Ať už se jedná o formu

kampaně (například ekologické) a nebo o výzvy k uživatelům internetu, aby nějakým způsobem podpořily určité aktivistické projekty. Příkladem takovéto výzvy může být například *March on Washington from Your Home* (Demonstrujte ve Washingtonu ze svého domova), kdy aktivisté žádali prostřednictvím internetu lidi z celého světa, aby zaplavili Bílý dům e-maily, faxy a telefonáty. Zásadním rozdílem mezi hacktivismem a on–line aktivismem je způsob využívání moderních technologií. On–line aktivismus netvoří nové prostředky a nástroje k protestu, pouze využívá těch již stávajících. Metac0m o rozdílu mezi aktivisty a hacktivisty říká: „Hacktivismus není pouhým začleněním aktivistických technik do digitální sféry. Spíše je vyjádřením dovedností hackerů v podobě elektronické přímé akce. Což dosvědčuje, že ani taktiky a ani cíle hacktivismu nejsou statické. Naopak, za účelem větší efektivity se musí neustále vyvíjet. Tím je dán rozdíl mezi hackery zabývajícími se aktivismem a aktivisty pokoušejícími se užívat technické aspekty hackování k napodobování a racionalizování tradičních forem aktivismu.“[50]

Kyberterorismus také zahrnuje veškeré hackerské prostředky a techniky, ale s tím rozdílem, že je využívá ke skutečnému zničení nebo vážnému narušení počítačových systémů za účelem vlastního obohacení nebo vyvolání reálného společenského konfliktu. Jedná se o aktivity označované jako závažná počítačová kriminalita, kdy jsou komunikační a informační technologie zneužívány k šíření extrémistických názorů, k nabádání jednotlivců k fyzickému násilí s politickým podtextem, k ohrožování či přímo zcizování cizího majetku.

Hacktivismus také využívá hackerských prostředků a technik, avšak jeho cílem není ničit a obohacovat se, ale

---

[49] Wray S.: *On Electronic Civil Disobedience*, New York, 1998, [cit. 16.7.2006]. Dostupné z: http://www.thing.net/~rdom/ecd/oecd.html

naopak kreativně vytvářet nové hodnoty, které mají důrazně poukázat na společenské problémy.

[50] Metac0m: *What is Hacktivism?*,2003, [cit. 25.8.2006]. Dostupné z: http://www.thehacktivist.com/?page_id=97

6.2. Praktiky a pravidla hacktivismu

> „Hacktivismus je základ. Je využitím kolektivní nebo individuální vynalézavosti k překročení limitů, nalezení chytrého řešení složitých problémů s pomocí počítačů a Internetu. Hacktivismus je neustále se vyvíjejícím a otevřeným procesem; jeho taktiky a metody nejsou statické. V tomto smyslu nikomu hacktivismus nepatří – nemá svého proroka a nemá své evangelium a kanonizovanou literaturu. Hacktivismus je rizomatickým fenoménem s otevřeným zdrojem.“[51]

Hacktivismus má k dispozici celou škálu hackerských praktik. Nejběžnějšími metodami je narušování ochranných prostředků jednotlivých systémů a počítačů a následné pronikání do nich. To vše je možné prostřednictvím nalézání bezpečnostních mezer operačních systémů či infikování speciálními viry. Dalšími metodami jsou například emailové bombardování, web – squatting[52], přesměrování DNS[53] záznamů či útoky na bázi DoS[54].

Jednou z nejběžnějších technik, se kterou se setkal pravděpodobně každý člověk používající email, je použití

programu trojského koně. Jedná se o program, který například do zcela běžného emailu vloží určitý virus nebo kód. Ten pak

[51] Metac0m: *What is Hacktivism?*,2003, [cit. 25.8.2006]. Dostupné z: http://www.thehacktivist.com/?page_id=97
[52] Jedná se o registrování domén se jmény slavných osobností, se jmény velkých podniků a známých značek. Majitelé těchto značek či jmen jsou pak donuceni, pokud mají o tyto domény zájem, nuceni zaplatit velké částky za odkoupení.
[53] Domain Name Server – počítač se speciálním programem, který překládá textové znění internetových adres do jejich numerického ekvivalentu
[54] Denial–of–service - odmítnutí služby

sleduje, ukládá a přeposílá veškerý text, ať už se jedná například o hesla a jiné přístupové kódy nebo o samotný obsah e-mailu, vyťukaný na klávesnici do počítače, který trojského koně vyslal a který tak získává informace potřebné pro přístup do systému napadeného počítače. Aktivovaný trojský kůň může také přímo otevírat porty ulehčující vstup hackera do systému. Zcela jednoduchým způsobem, jak na nějaký čas vyřadit systém z činnosti, je také například prosté emailové bombardování.

Útoky na bázi DoS jsou zaměřeny na přetížení kapacity serveru. Jedná se o umělé vygenerování takového množství zaslaných požadavků na příslušný server, který se snaží na každý z nich reagovat, přičemž překročí svoji vlastní technickou kapacitu a dojde k „spadnutí“ sítě, serveru. Jedinou možnou ochranou bylo omezení množství zpracovaných požadavků z jedné IP adresy. I tuto ochranu je ovšem možné obejít prostřednictvím výše zmíněného programu trojského koně. Hacker tak může posílat požadavky na daný server z počítačů napadených trojským koněm, tudíž server musí zpracovávat velké množství požadavků z různých IP adres.

Velice oblíbeným a leckdy i vtipným útokem hacktivistů je tzv. DNS přesměrování. Tento útok spočívá ve změně původních údajů na DNS serverech, jež pak umožní přesměrovat webové

stránky, na které se uživatel pokoušel přihlásit, na jiné, ve většině případů na stránky hackera oznamující úspěšný útok.

Klíčovým problémem všech těchto praktik je i pro samotné hacktivisty, kdo a za jakým účelem je používá. Základní tezí hacktivistů je využívání prostředků počítačových technologií a kreativních schopností jedince za účelem vyjádření nespokojenosti s určitým politickým či sociálním stavem. Tyto prostředky a schopnosti však mohou být stejně tak použity někým za účelem vědomého ničení, poškozování či okrádání jiných.

Zneužívání nebo špatné používání hackerských praktik vedlo hackery k přesnějšímu vymezení pojmu hacktivismu (viz. výše) a k zneuznání některých praktik a technik. Například hackerská skupina cDc nepovažuje útoky na bázi DoS nebo předělání a ničení webových stránek za legitimní hacktivistické akce a techniky. Pozměnění nebo zničení webových stránek není podle nich ničím jiným než hi-tech vandalismem, zatímco útoky na bázi DoS jsou vlastně útokem na svobodu projevu. Oxblood Ruffin ve snaze definovat legitimní prostředky a techniky hacktivistů říká: „ Za prvé, žádné znetvořování Webu. Jestliže skupiny či jednotlivci mohou legálně ze zákona publikovat nějaký obsah na Webu, pak jakékoliv narušení jejich práv na šíření informací je poškozování jejich Prvního doplňku práv (svoboda vyjadřování). To samé platí pro útoky na bázi DoS.“[55]

Stejně tak bude jádrem hacktivistického hnutí odmítáno vytváření a aplikování virů či internetových červů. Hlavní činností hacktivistů by mělo být vynalézání nových praktik a technik a kreativní využívání hackerských schopností a dovedností za účelem nikoliv ničit a poškozovat, ale naopak vymýšlet nová a efektivní řešení. Vytvářet, nikoliv ničit.

Tak jako se sami klasičtí hackeři distancují od tzv. crackerů, tak se i hacktivisti postupně dopracovali k dichotomii hacktivismus/craktivismus. Tuto dichotomii Metac0m přibližuje následovně: „První je užíváno k popisu

politicky motivovaného hackování, které je konstruktivní, druhé je ničivé.“[56] Crackování je neautorizovaným přístupem do systému, nelegitimním nabouráváním se do jiných počítačů. Takovýmto neautorizovaným vstupem do systému je právě také například předělávání webových stránek či útoky na bázi DoS.

---

[55] Oxblood Ruffin: *Hacktivism, From Here to There*, Yale Law School,2004,[cit.15.7.2006].Dostupný z: http://www.cultdeadcow.com/cDc_files/cDc-0384.php

[56] Metac0m: *What is Hacktivism?*,2003, [cit. 25.8.2006]. Dostupné z: http://www.thehacktivist.com/?page_id=97

Ale ke škodě hacktivistů jsou to přesně ty techniky a praktiky, které spíše než ostatní přitáhnou pozornost médií, a to i přestože by se o jejich politickém či sociálním motivu dalo značně pochybovat. Přesto jsou v médiích prezentovány jako hacktivistické.

„[...] hacktivisté musí být extrémně opatrní ve způsobech, jakým používají taktiky a stejně tak ve vybraných cílech útoku. Nutně musí být známa jasná příčinná souvislost mezi terčem útoku a tím, proti čemu se protestuje. Kromě toho musí být provedeno řádné prozkoumání týkající se implementace kampaně ECD a zároveň zhodnocení míry úspěšnosti, dopadu a možných vedlejších negativních důsledků.“[57]

6.3. Hacktivismus v praxi

Pro názornou ilustraci podnětů, cílů a praktik hacktivismu bude nejlepší uvést několik již uskutečněných hacktivistických projektů s politickým, sociálním či ekonomickým podtextem.

Jeden z nejstarších a zdokumentovaných případů hacktivismu se objevil již v roce 1989, kdy hackerská skupina WANK vypustila stejnojmenného „politického“ červa, což je program, který se sám rozmnožuje a funguje na podobné bázi jako virus.

Terčem útoku tohoto červa se staly sítě NASA SPAN a HEPnet. Jednalo se o protest proti vyvíjení nukleárních zbraní. Nabourání se do těchto systémů mělo také znemožnit start rakety, jejíž misí bylo vypustit na oběžnou dráhu sondu Galileo. WANK sice na určitou dobu ochromil celý systém, nicméně raketa byla v závěru vypuštěna a systém opraven. Ve chvíli, kdy byl systém napadnut, objevil se na mnoha

---

[57] Metac0m: *What is Electronic Civil Disobedience?*, 2001, [cit. 25.8.2006]. Dostupné z: http://www.thehacktivist.com/?page_id=98

obrazovkách počítačů připojených do sítě NASA a HEPnet grafické zpracování názvu červa – WANK a text: „Červi proti nukleárním vrahům. Váš systém byl oficiálně WANKnut. Celou dobu hovoříte o míru pro všechny, a přitom se připravujete na válku.“[58]

Přestože programoví červi a počítačové viry, ačkoliv jejich vypuštění může mít politický podtext, nejsou stoprocentně uznáváni všemi hacktivisty, objevilo se jich a pravděpodobně i objeví v průběhu dalších let ještě několik. Známý byl například červ nesoucí název Injustice[59] (Bezpráví), odstartovaný po zabití 12tiletého palestinského chlapce Mohammada Al – Durra. Červ nepůsobil žádné škody v napadených systémech, pouze zanechával zprávu o bezpráví a násilí konaném izraelskou armádou vůči Palestině a jejích občanů.

Velice známou skupinou hackerů aktivistů a umělců, podporujících a se skupinou The Critical Art Ensemble spoluzakládajících ideu a praxi elektronické občanské neposlušnosti, byla skupina EDT – Electronic Disturbance Theater[60] (Divadlo elektronického nepokoje). Její dva členové Carmin Karasic a Brett Stalbaum vytvořili software *FloodNet*, jenž v roce 1999 zpřístupnili široké veřejnosti. Tak bylo umožněno víceméně komukoliv podnikat útoky na bázi DoS proti jakékoliv webové stránce. Stačilo zadat IP adresu a program na

ni sám vždy po několika vteřinách opakovaně vysílal požadavek. V roce 1998 použila EDT tento software proti stránkám mexického prezidenta Zedilla a mexické vládě na podporu partizánského hnutí Zapatista, stejně tak proti webovým stránkám dnes již bývalého amerického prezidenta Billa Clintona a Bílého domu, nebo frankfurtské burzy, jakožto symbolu kapitalismu, či Pentagonu, vojenského symbolu

---

[58] http://www.cert.org/advisories/CA-1989-04.html
[59] http://www.sophos.com/virusinfo/analyses/vbsstaplea.html
[60] http://www.thing.net/~rdom/ecd/EDTECD.html

Spojených států. Ve většině případech se podařilo na několik hodin či na celý den způsobit výpadek serveru. Skupina EDT nadále pokračuje s mnoha podobnými projekty.

V rámci základního práva společnosti na svobodný přístup k informacím se američtí hackeři rozhodli protestovat proti čínské cenzuře Internetu a deaktivovali čínskou firewallovou síť.[61] Tato síť bránila čínským uživatelům vstoupit na určité webové stránky, které čínská vláda považovala za „nebezpečné“ svému režimu. Například skupina cDc vytvořila aplikaci nazvanou Peekabooty, která umožnila prolomit jakékoliv firewally a dostat se na libovolné stránky z hostitelského počítače. Nápomocným byl také určitý druh šifrování, tzv. steganografie, která dovoluje skrýt digitální obsah do kořene jiného digitálního obsahu. Jak říká Oxblood Ruffin: „Filtrování DNS a filtrování jednotlivých počítačů sleduje vysílané požadavky na webové stránky týkající se lidských práv, ženských témat a dalších podobných, která jsou pro diktátory nepohodlná. Toto filtrování však nesleduje „obrázky z Disneylandu, moje cesta do obchodu s potravinami“ a jiná banální témata. Tak jsme ukryli zakázaný obsah do přijatelných stránek prostřednictvím procesu steganografie.“[62] Umožnit na krátký čas neomezený přístup na webové stránky uživatelům internetu v Číně se také podařilo hackerům Bronc Busterovi a Zyklonovi.Úspěšným byl také útok skupiny Hong Kong Blondes[63],

které se podařilo získat kontrolu nad důležitým komunikačním satelitem, což mělo zásadní vliv na fungováním sítě čínských vládních a vojenských institucí a stejně tak nad čínským mezinárodním obchodem.

---

[61] Firewall je jedním z druhů ochranného softwaru, který slouží k tomu, aby zabránil vstupu na určité stránky nebo posílání emailů a souborů obsahujících jistý obsah. Slouží především k ochraně osobních informací.
[62] Oxblood Ruffin: *Hacktivism, From Here to There*, Yale Law School,2004,[cit.15.7.2006].Dostupný z: http://www.cultdeadcow.com/cDc_files/cDc-0384.php
[63] http://www.wired.com/wired/archive/5.12/updata.html

Ukázkou toho, že hacktivismus není jen otázkou individuálních zájmů či zájmů malých skupin, jsou například protesty namířené proti Mezinárodnímu měnovému fondu, Světové bance či Světové obchodní organizaci. Tyto protesty jsou zaměřeny na simultánní a kolektivní přímou akci probíhající zároveň jak v reálném světě formou pouličních demonstrací tak v kyberprostoru. Některé hacktivistické skupiny (např. Electrohippies) vytvářejí programy využívající taktiky DoS, které si mohou stáhnout i průměrní uživatelé internetu. Ze svého připojeného počítače pak mohou vyjádřit nesouhlas a nespokojenost s fungováním těchto organizací tím, že pomohou zablokovat jejich stránky. Takto byly například podpořeny protestní akce v Seattlu[64] roku 1999 proti WTO, nebo proti Světové bance v roce 2000 v Praze.[65]

Praktik hacktivismu vyžilo již také několik uměleckých skupin operujících v prostředí internetu. Příkladem může být kauza uměleckého sdružení etoy.com versus eToys, společnosti prodávající hračky. „Válka hraček“[66] začala v okamžiku, kdy obchodní společnost eToys podala trestní oznámení na skupinu umělců kvůli údajně vědomému zneužívání jejich značky, a to i přes to, že webové stránky a umělecká skupina etoy.com vůbec existovaly dávno před touto obchodní společností. Jiným příkladem může být protest net.artistů ze skupiny 0100101110101101 [67] proti komercionalizaci internetového umění.

Ti se rozhodli naklonovat některé placené webové galerie a zdarma je zpřístupnit všem.

---

[64] http://news.bbc.co.uk/1/hi/uk/543752.stm
[65] http://www.villagevoice.com/news/0042,ferguson,19055,1.html
[66] http://www.rtmark.com/legacy/etoymain.html
[67] http://0100101110101101.org

6.4. Hacktivismus: boj za naše práva nebo zločin?

Postoj společnosti, vlád či velkých obchodních korporací je k činnostem hacktivistů stejně jako u hackerů velice ambivalentní. Leckdy je opravdu obtížné určit, do jaké míry se jedná o boj za naše práva v kyberprostoru a ve fyzickém světě, a kdy už je možno hovořit o kriminalitě a poškozování.

Stejně jako v každé společnosti nalezneme i mezi hackery a rádoby hacktivisty uličníky, vandaly a zloděje. A podobně jako v reálném životě budou mít jednotlivé společnosti vždy problémy zamezit působení škodlivých živlů, tak není v rámci hackerských a hacktivistických idejí o svobodě toku informací, o svobodě projevu a potřeby sdílení a vylepšování určitých prostředků, možné stoprocentně zamezit zneužívání těchto idejí a prostředků.

V prvé řadě jde o myšlenku vytváření takových technik a praktik v rámci kyberprostoru, které mají ochránit občany, aktivisty a vůbec celou společnost před cenzurou a přímým dohledem nad svobodným a otevřeným prostorem internetu, tak jako nad reálným světem národních států, a které mají uchovat svobodu projevu a svobodný přístup k informacím, uchovat tedy svobody dané základními lidskými právy. „Hacktivismus není jednoduše uličnictvím, není ani zákeřný ani destruktivní. Není synonymem ničením webových stránek ani útoků na bázi DoS.

Hacktivismus je formou elektronické přímé akce, ve které se spojuje kreativní a kritické myšlení s programovacími schopnostmi a kódy vytvářejícími nové mechanismy za účelem dosažení sociálních a politických změn.“[68]

---

[68] Metac0m: *What is Hacktivism?*,2003, [cit. 25.8.2006]. Dostupné z: http://www.thehacktivist.com/?page_id=97

7. Kryptoanarchisté

V současnosti jednou z nejradikálnějších a nejkontroverznějších skupin pohybující se ve vodách kyberprostoru jsou kryptoanarchisté, někdy sami sebe označující za *cypherpunks* (šifropunky). Spolu s hackery jsou pro většinu Národních bezpečnostních úřadů opravdovým nebezpečím, neboť vyvíjejí takové aktivity, proti kterým nemá žádný stát dostatečné prostředky, jak legislativní tak technické. A i přes určité snahy státní moci legálně zamezit jejich aktivitám, razí kryptoanarchisté dále vlastní teorii a praxi zaměřenou na udržení naprosté anonymity kyberprostoru, která představuje především ochranu osobní svobody a soukromí. Ochrany svobody a soukromí a stejně tak bezpečnosti uživatelů komunikačních technologií je možné dosáhnout prostřednictvím šifrování veškerých zpráv a informací. Kódováním je možné zamezit státním orgánům a jiným institucím kontrolovat jakékoliv informační toky a vůbec zasahovat do soukromí jednotlivých uživatelů nových komunikačních a informačních technologií.

Kryptoanarchista Eric Hughes ve svém *Manfiestu Šifropunkerů* říká: „ Jestliže chceme mít soukromí, musíme si ho bránit. Musíme se spojit a vytvořit systém, který umožní anonymní transakce. Lidé si bránili své vlastní soukromí po staletí šeptáním, tmou, obálkami, zavřenými dveřmi, tajným

potřesením rukou a kurýry. Minulá technologie nedovolovala výrazné soukromí, elektronické technologie však již ano.“[69] Nejdůležitější aktivitou se tak pro kryptoanarchisty stává vytváření a aplikace kódovacích systémů. Tyto systémy pak poskytují volně komukoliv, kdo projeví zájem o ochranu vlastního soukromí.

---

[69] Hughes E.: *A Cypherpunk´s Manifesto*, 1993, [cit. 18.7.2006]Dostupné z: http://www.activism.net/cypherpunk/manifesto.html

Důležitým aspektem této skupiny aktivistů je také boj proti principům vlastnického práva, jenž naprosto odporuje heslu „všechny informace mají být svobodné“. Byl proto vytvořen koncept *copyleftu*, oficiálně označovaný jako GNU General Public Licence (veřejná licence). Tento koncept se ostře staví proti jedinečnému vlastnictví, a to zejména intelektuálnímu, v rámci kyberprostoru, dále proti vydělávání peněz na tom, co by podle nich mělo být zdarma a volně přístupné a co by mělo být otevřeno inovacím a obohacení. Nejznámějším příkladem konceptu copyleftu by mohl být operační systém UNIX a jeho mutace Linux, distribuovaného jako svobodný software. Označení svobodný software znamená, že tento software může kdokoliv libovolně stahovat, kopírovat, rozdávat. Dále k němu získává přístup k jeho zdrojovému kódu, což znamená, že kdokoliv schopný může opravovat, vylepšovat či vymýšlet různé nové aplikace tohoto operačního systému, které budou opět zdarma a volně přístupné všem ostatním. Svobodná inovace a stálé zhodnocování intelektuálního vlastnictví nesmí být podle kryptoanarchistů ničím a nikým omezovány, proto je nutné bojovat jak proti státní kontrole tak proti konceptu vlastnického práva. „Tak jako zdánlivě bezvýznamný vynález v podobě ostnatého drátu umožnil oplocení velkých rančů a farem, a tím naprosto pozměnil koncept půdy a vlastnických práv na divokém západě, tak se i bezvýznamný objev z tajemného

odvětví matematiky stane nůžkami, které přestřihnou ostnatý drát obepínající duševní vlastnictví. Povstaňte, kromě ostnatých drátů není co ztratit!“[70]

Nejznámějším programem, který kryptoanarchisté vytvořili a předali ostatním, byl *PGP – Pretty Good Privacy* (Velice dobré soukromí). Jedná se o rogram umožňující tu nejlépe utajenou

---

[70] May T.C.: *The Crypto Anarchist Manifesto,* 1992, [cit. 18.7.2006]. Dostupný z: http://www.activism.net/cypherpunk/crypto-anarchy.html

komunikaci mezi kýmkoliv. Dokáže sdělení zašifrovat takovým způsobem, že ani ty nejmodernější a nejpropracovanější programy je nejsou schopny zpětně dešifrovat. Jiné programy například dokáží skrýt skutečnost, že zpráva byla vůbec zašifrována. Každopádně tyto oblíbené a po celém světě rozšířené programy znamenají nebezpečí především pro státy a jejich bezpečnostní složky. Pierre Lévy ve své knize o kyberkultuře přímo říká: „PGP vkládá do rukou každého jedince takovou moc, která dosud byla výhradním privilegiem nejmocnějších armád – totiž možnost absolutně tajné komunikace. Kromě toho tento program umožňuje občanům vyhnout se kontrole komunikací (otevírání dopisů, telefonické odposlouchávání, zachycování digitálních zpráv), kterou používala a stále používá policie i těch nejdemokratičtějších států, ať už z důvodů politických (totalitní režimy, sledování opozice, boj proti terorismu) či v boji proti gangům a organizovanému zločinu.“[71] Státy tak v šifrování, kódování a naprosté anonymitě uživatelů vidí ohrožení vlastní suverenity a ohrožení státní kontroly. Z toho důvodu se snaží užívání šifrovacích programů omezovat zákony.

Ani to však nemůže být stoprocentně účinné. Zákony jednotlivých zemí a kontrola jejich dodržování platí vždy na fyzickém území daného státu. Kyberprostor, jak již bylo řečeno, tyto geofyzické hranice a teritoria ovšem

nerespektuje. Občané jednotlivých států se mohou do sítě připojit skrze jakýkoliv server na světě, tudíž nemusí nutně podléhat zákonům o informacích platících v zemi, jejímiž jsou občany, nebo ve které se momentálně připojují k určitému serveru.

---

[71] Lévy P.*: Kyberkultura, Zpráva pro radu Evropy v rámci projektu „Nové technologie: kulturní spolupráce a komunikace“*, z fr. orig. *Cyberculture* (Rapport au Conseil de l´Europe), Éditions Odile Jacob / Éditions du Conseil de l´Europe 1997, přel. M. Kašpar, A. Pravdová, Praha, Karolinum 2000, 186 s.

7.2. Kód a autorská práva

Otázkami kódů, šifrování a především otázkami autorských práv v kyberprostoru se trochu v jiném smyslu zabývá také americký profesor práva na Standfordské univerzitě Lawrence Lessig. Ve své eseji *Kód je právo* (Code is Law), zveřejněné v časopise *Harvard Magazin* v roce 2000, se zabývá možností regulace chování uživatelů na Internetu, přičemž naráží na skutečnost neutrálního kódu, který není schopen rozpoznat a určit zasilatele informace a ani její samotný obsah. Základním kódem jsou protokoly TCP/IP[72]. Ty umožňují přenos jakýchkoliv dat v rámci mezinárodně propojené sítě právě bez ohledu na obsah zasílané informace a bez ohledu na zasilatele a příjemce. Tím je jednotlivým vládám velice ztížena kontrola a regulace chování uživatelů v tomto prostředí.

Koho však podle Lessiga může nejvíce zasáhnou nemožnost regulace chování na Internetu, je komerční sféra, která může velice ztrácet tím, že nebude schopna dostatečně zabezpečit určité transakce, protože není v jejích silách v síti bez struktury najít zdroj rušení, nebo dále díky snadné distribuci nelegálních kopií určitých softwarů nebo například hudby. „Struktura kyberprostoru není dána. Neregulovatelnost je funkcí kódu, ale tento kód může být změněn.“[73] Ve chvíli, kdy budou protokoly a kódy zasazeny do určité struktury, stane se

chování v síti regulovatelné. A to je přesně to, oč se komerční sféra snaží a vlády jí k tomu rádi dopomohou. Oba subjekty tak mohou přeměnit celkový charakter sítě.

---

[72] TCP i IP jsou počítačovými protokoly, přičemž nejzákladnější protokol IP (Internet Protocol) zaručuje správné doručení dat, aniž by však potvrzoval přijetí vyslaných dat druhým počítačem. TCP (Transmission Control Protocol) provádí virtuální spojení, které trvá do doby než daná aplikace spojení ukončí a je potvrzeno, že data byla doručena druhému počítači.

[73] Lessig L.: *Code is Law, On Liberty in Cyberspace*, Harvard Magazíne [on-line], leden – únor 2000, [cit. 25.7.2006] Dostupné z: http://www.harvardmagazine.com/on-line/0100121.html

Z tohoto důvodu je pro Lessiga důležité dobře zkombinovat jak potřebu respektovat již platné zákony vlád a zákony trhu, tak zároveň možnosti nestrukturované sítě Internetu nabízející mimo jiné zcela svobodné zacházení s duševním vlastnictvím. Není jednoduše možné například vypustit vlády a jejich zákony, neboť na jejich místo nastoupí jiné autority, například právě ty komerční, které zdaleka nemusejí být lepší než ty vládní. Stejně tak nelze striktně omezovat svobody, které nám nestruktura sítě nabízí. „Kód reguluje. Může vytvářet hodnoty, ale také nemusí. Umožňuje svobody, ale také nemusí. Ochraňuje soukromí, ale může také podporovat kontrolu. Lidé určují, jak kód pracuje. Jsou to lidé, kdo píší kódy.“[74]

Zapotřebí je tedy hlídat, kdo kódy vytváří a za jakým účelem. Kód je právem proto, protože kód bude vždy určovat to, jaká práva budou mít uživatelé, a práva budou určovat ti, kteří budou psát kódy. V tomto momentě je pro Lessiga důležité uvědomit si, zda se na vytváření práva a kódu budeme podílet společně všichni, nebo ho necháme vytvářet někým, kdo se bude snažit prosadit své vlastní zájmy, například komerční subjekty.

Lawrence Lessig je také mimo jiné jedním ze zakladatelů a zároveň i předsedou neziskové organizace Creative Commons[75], která své projekty zaměřila na problematiku autorských práv. Tato organizace se nestaví přímo proti autorským právům, jen

proti právně chráněné normě ve znění „všechna práva vyhrazena“, které mění na „některá práva vyhrazena“. V současnosti platná vlastnická práva víceméně znemožňují samotnému autorovi díky smlouvám s vydavateli svobodně nakládat se svým dílem, se svým duševním vlastnictvím.

---

[74] Lessig L.: *Code is Law, On Liberty in Cyberspace*, Harvard Magazíne [on-line], leden – únor 2000, [cit. 25.7.2006] Dostupné z: http://www.harvardmagazine.com/on-line/0100121.html

[75] http://creativecommons.org

Organizace tak vytvořila webovou aplikaci, kde je umožněno umělcům a autorům zveřejňovat svá díla ve veřejné sféře, aniž by přišli o svá vlastnická práva. Nabízí jim prostor, kde mohou svá díla pro určité užití a za určitých podmínek svobodně a zdarma zpřístupnit. Narozdíl od GNU GPL (zkratka veřejné licence) je však organizace Creative Commons zaměřena spíše než na svobodný software na různé kreativní práce: webové stránky, fotografie, literatura, vzdělávací projekty, hudba atd. „Jediným cílem Creative Commons pro současné a budoucí projekty je: vytvořit rozumnou a flexibilní rovinu vlastnických práv jako reakci na stále více restriktivní, standardní pravidla.“[76]

[76] Creative Commons*: About Us, "Some Rights Reserved": Building a Layer of Reasonable Copyright*, [www.creativecommons.org] , nedatováno, [25.7.2006]. Dostupné z: http://creativecommons.org/about/history

8. Kyberfeminismus

Dalším velice zajímavým a leckdy kontroverzním hnutím využívajícím ke svým účelům kyberprostor je tzv. kyberfeminismus, jenž stejně jako klasický feminismus představuje určitý teoreticko–praktický myšlenkový rámec, zahrnující jak svým způsobem krajní politický aktivismus, tak zároveň různé esteticko–umělecké projekty.

„Cílem není univerzální solidarita a pochopení mezi ženami, ale vytváření společnosti, která bude tolerantní k různosti a pluralitě ve světě, ve kterém nic není dané, ale všechno možné, ať už je to přeměna na kyborga nebo jen změna pohlaví.“[77] Pro kyberfeminismus se klíčovým bodem stávají moderní technologie a z toho logicky vyplývající boj proti klasické dichotomii příroda/technika či přirozené/umělé, přičemž v době silně patriarchální dominance je ženě ve většině případů přisuzována příroda a mužům technika a technologický pokrok. Kyberfeminismus se ovšem důrazu na spojení ženy a přírody, popřípadě nostalgie po návratu k původní přirozenosti a obnovení moci plynoucí z přírodního řádu, vzdává. Naopak, důležitým pilířem pro vznik nové identity ženy se stávají moderní technologie. „Pro kyberfeminismus se proto stává ústřední vztah žen a nových technologií, který zastiňuje starší témata, jako je vztah žen

a společnosti (liberální feminismus, materialistický – marxistický feminismus) nebo žen a jazyka (francouzský a psychoanalytický feminismus). Změny, které přinášejí informační technologie, jsou historickou šancí pro ženy stát v prvních liniích a nečekat, aby jim muži otevřeli dveře do těchto nových oblastí. Kyberfeministky se nezabývají

---

[77] Kera D.: *Kyberfeminismus: mezi uměním a aktivismem*, 2002, [cit. 25.7.2006].Dostupné z: http://uisk.jinonice.cuni.cz/kera/sylabus2002/03tema5.htm

minulostí, ale jen budoucností, v které vidí možnost pro ženy dosáhnout svých cílů a postavení, a tím i smazat historické křivdy.“[78] Jestliže je pro tradiční feminismus základem sdílení identity, pochopení a solidarita, pak je pro kyberfeminismus základním předpokladem právě pluralita cílů, zájmů a identit.

Zhmotnělou vizí představy kyberfeminismu o spojení člověka a moderní technologie je postava kyborga, člověka–stroje. Kyborg tak v sobě zahrnuje vše, co je pro kyberfeminismus důležité: spojení s přírodou, technikou, kulturou, nová identita, nový vztah společnosti k genderu. „Kyborg je bytostí z post-genderového světa, nemá nic společného s bisexualitou, pre–oidipovskou symbiózou, neodcizenou prací či svůdností organické jednoty, které je možné dosáhnout prostřednictvím konečného spojení veškeré moci částí do vyššího celku. Konečnou ironií ve smyslu západní tradice je, že kyborg nemá svůj mýtus původu – je také apokalyptickou konečnou příčinou (telos) vzrůstající západní nadvlády abstraktní individualizace, konečné já osvobozené od veškeré závislosti.“[79]

8.1. Umění a aktivismus kyberfeminismu

V hnutí kyberfeminismu můžeme odhalit několik různých proudů zaměřených a podporujících aktivistické či umělecké směry. Nalezneme zde ženy teoretičky, ženy umělkyně, ženy programátorky, IT specialistky, webmasterky, či dívky vytvářející vlastní deníky, tzv. weblogy s všemožnými myšlenkami, nápady a radami ostatním ženám.

---

[78] Kera D.: *Kyberfeminismus: mezi uměním a aktivismem*, 2002, [cit. 25.7.2006].Dostupné z: http://uisk.jinonice.cuni.cz/kera/sylabus2002/03tema5.htm

[79] Haraway D.: *A Cyborg Manifesto: Science, Technology, and Socialist-Feminism in the Late Twentieth Century*, 1991, [26.7.2006]. Dostupné z: http://www.stanford.edu/dept/HPS/Haraway/CyborgManifesto.html

Pro vznik kyberfeministického hnutí bylo zásadní vydání několika kyberfeministických manifestů. Jednou z nejvýznamnějších teoretiček a autorek kyberfeministických manifestů je již citovaná Donna Haraway, autorka *Manifestu kyborgů* (The Cyborg Manifesto) z roku 1985. Hranici mezi science–fiction a sociální realitou vnímá jako optickou iluzi, neboť podle ní jsou všichni lidé na konci 20. století díky pokrokům medicíny kyborgy. Ovšem s tím, že postava kyborga má svůj symbol v ženě, neboť kyborgové „nemají „božský“ původ, ani nejsou žádným obrazem boha nebo muže“ a proto jsou „blízké ženám a symbolem emancipace“.[80]

Dalšími autorkami kyberfeministických manifestů byly například členky skupiny VNS Matrix, jejichž manifest má také mimo jiné inspirovat k násilným činům a revolucím. Ženy považují „za nepřátele všech stávajících kódů a za „virus nového světového pořádku““.[81] S touto skupinou spolupracovala známá feministka Sadie Plant a společně byly vůbec prvními ženami, které použily slovo kyberfeminismus a které se zabývaly zkoumáním vytváření sociálních vztahů a otázkami identity a sexuality v technologické kultuře. Klasický ortodoxní feminismus Sadie Plant vnímá jako velice technofobní a upozorňuje, že „v praxi to byly právě ženy, které vytvořily většinu nejzajímavějších prací v nových médiích a které jsou technofobii velice vzdálené, a ve skutečnosti se zdá, že mají

k počítačům intimní vztah. Což zbořilo existující feministické teorie.“[82] Intimní vztah však nemají ženy jen k počítačům, ale víceméně ke všem novým a především komunikačním technologiím. Sadie Plant to dokazuje na aktivním a efektivním využívání technologií jakými jsou telefony, faxy, psací stroje,

---

[80] Kera D.: *Kyberfeminismus: mezi uměním a aktivismem*, 2002, [cit. 25.7.2006].Dostupné z: http://uisk.jinonice.cuni.cz/kera/sylabus2002/03tema5.htm

[81] Tamtéž

[82] Miss M., Plant S., Dement L.: *An interview with Sadie Plant and Linda Dement*,1996,[cit.26.7.2006].Dostupné z: http://www.t0.or.at/dolores/interviews/intervwtoc.htm

kalkulačky, se kterými si ve většině případů budou vědět rady spíše ženy než muži. „Digitální média podrývají veškeré domněnky o tvůrci, géniovi, autoritě, vlastnictví atd. O všem, co bylo po dva a půl tisíce let rozhodující pro západní civilizaci. To vše také v minulosti sloužilo ženám spíše ke škodě.“[83] Zkoumáním historického vztahu ženy k technologiím se snaží ukázat, že žena nikdy nebyla pasivní obětí technologických změn.

Přímou ilustraci a pravděpodobně i radikálnější definici kyberfeminismu nalezneme v jednotlivých uměleckých projektech, které jsou z největší části zaměřeny na vztah nových technologií, těla a jeho modifikací. Mnoho leckdy anonymních uměleckých skupin tohoto směru se nově zaměřilo na oblasti počítačových her a pornografie. Známou kyberfeministickou umělkyní je například Linda Dement z Austrálie, která v rozhovoru s Miss M. a Sadie Plant říká o svém projektu *Cyberflesh Girlmonster* vydaném na CD-Romu: „Práce sama není především o počítačích, ale je v počítačích situována. Líbí se mi představa infikování technologie krví, vnitřnostmi a šílenstvím, těmi všemi nechutnými ženskými věcmi, představa nakazit tu krásnou a uhlazenou technologii, ty krásné a čisté stroje. Tato juxtapozice se mi opravdu velice líbí.“[84] V tomto projektu pospojovala různé naskenované části ženských těl a audio nahrávky ženských hlasů tak, že vytvořila různá malá

monstra a postavy. Tímto a dalšími svými projekty se snaží ukázat, že i pro ženu je agrese a obscénnost něčím přirozeným a ne naopak, jak předpokládá čistě společensky vnucený rámec normality.

---

[83] Miss M., Plant S., Dement L.: *An interview with Sadie Plant and Linda Dement*,1996,[cit.26.7.2006].Dostupné z: http://www.t0.or.at/dolores/interviews/intervwtoc.htm

[84] Tamtéž

Dalšími uměleckými skupinami vyjadřujícími prostřednictvím kyberprostoru své názory na umění a společnost jsou například Heartless Bitches International, Riot Girls či Geurrilla Girls. Ke své kritice sexismu a rasismu ve světě a v umění využívají tato hnutí své umělecké nápady, média a různé performance. Zapotřebí je i určitá forma rebelanství. Velice kontroverzním směrem kyberfeminismu jsou ta hnutí, která podporují pornografii, ať už z důvodu boje za svobodu slova a boje proti cenzuře, či prosazování práva ženy rozhodovat o svém těle, tak z důvodu čistě podnikatelského, uměleckého a zábavního. Jiným specifickým směrem kyberfeminismu jsou skupiny žen, které se profesionalizovaly v oblasti informačních technologií, jako například GeekGirls.

Na čem se však pravděpodobně všechny výše zmíněné směry kyberfeminismu shodnou, bude především snaha zabránit tomu, aby ženy nebyly vnímány a aby samy sebe nevnímaly jako oběti nových technologií, ale naopak, aby je vnímaly jako nový prostředek pro prosazení a nalezení sebe samých.

9. Závěr

Kybernetický svět počítačů a kybernautů již není otázkou daleké budoucnosti, naopak je otázkou velice současnou. Globální síť propojených počítačů lze vnímat jako zatím nejrozšířenější demokratické médium se svými klady i zápory, které mohou daleko více než kdykoliv v minulosti nezvratně a v nepředstavitelné míře ovlivnit současné dění.

Moderní informační a komunikační technologie se staly nedílnou součástí našich životů, součástí, která znatelně naše bytí na světě ovlivňuje a mění. Poskytly nám nový prostor, který postupně zabydlujeme. A je pouze na nás uživatelích, jak bude tento nový prostor vypadat a fungovat.

V této práci jsem se snažila popsat ty uživatele informačních a komunikačních technologií, kteří mají zájem, potřebu a zejména schopnosti podílet se na vytváření přirozeného, užitečného a svobodného prostředí v hájemství digitalizovaných informací, které by mělo především umožnit zlepšení současných životních podmínek. Uživatele, jež nám nabízejí alternativní pohled na vztah člověka a technologie, technologie a lidských práv a svobod. Existence zde zmíněných a dalších kybersubkultur je určitou a důležitou reakcí na současné dění. Proto ji nelze vnímat jako pouhou okrajovou záležitost virtuálního světa. Jsou to specifické subkultury,

které si možná jako první uvědomily a možná i jako první využily možností kyberprostoru jakožto demokratického nástroje občanské společnosti.

I přes své stinné stránky může být kyberprostor díky svým jedinečným vlastnostem zdrojem zrodu nových kulturních a společenských forem obohacujících dosavadní fungování společnosti a nás samotných.

Použitá literatura a prameny:

Bella T., Adamovič I.: *Goldstein, technika, svobody: rozhovor s Emmanuelem Goldsteinem*, Živel, Jaro 1994, 19-23.

Bey H.: *Dočasná autonomní zóna*, z ang. org. *Temporary Autonomous Zone*, neuvedeno, 2004, přel. Blumfeld, Praha, Tranzit 2004

Carter A.: *Občanská neposlušnost*, nedatováno,[cit. 25.8.2006]. Dostupné z: http://www.differentlife.cz/pravalidska06.htm

Cerf G.V., Clark D.D.,Kahn E.R.,Kleinrock L., Leiner M.B., Lynch C.D.,Postel J.,Roberts G.L., Wolff S.: *A Brief History of the Internet*, Internet Society, 2003, [cit. 23.6.2006]. Dostupné z: http://www.isoc.org/internet/history/brief.shtml#cerf

Creative Commons*: About Us, "Some Rights Reserved": Building a Layer of Reasonable Copyright*, [www.creativecommons.org] , nedatováno, [25.7.2006]. Dostupné z: http://creativecommons.org/about/history

Haraway D.: *A Cyborg Manifesto: Science, Technology, and Socialist-Feminism in the Late Twentieth Century*, 1991, [26.7.2006]. Dostupné z: http://www.stanford.edu/dept/HPS/Haraway/CyborgManifesto.html

Hauben M.: *History of ARPANET, Behind the Net – The untold history of the ARPANET*, nedatováno, [cit. 23.6.2006]. Dostupné z: http://www2.dei.isep.ipp.pt/docs/arpa.html

Hughes E.: *A Cypherpunk´s Manifesto*, 1993, [cit. 18.7.2006]Dostupné z: http://www.activism.net/cypherpunk/manifesto.html

Kera D.: *Kyberfeminismus: mezi uměním a aktivismem*, 2002, [cit. 25.7.2006]. Dostupné z: http://uisk.jinonice.cuni.cz/kera/sylabus2002/03tema5.htm

Lanier J.:*Digitální inventura, Co se vlastně změnilo v posledních pěti letech?*, Živel, 1999, 14, 40 – 41 s.

Lessig L.: *Code is Law, On Liberty in Cyberspace*, Harvard Magazíne [on-line], leden – únor 2000, [cit. 25.7.2006] Dostupné z:http://www.harvardmagazine.com/on-line/0100121.html

Lévy P.: Kyberkultura, Zpráva pro radu Evropy v rámci projektu „Nové technologie: kulturní spolupráce a komunikace“, z fr. orig. Cyberculture (Rapport au Conseil de l´Europe), Éditions Odile Jacob / Éditions du Conseil de l´Europe 1997, přel. M. Kašpar, A. Pravdová, Praha, Karolinum 2000

May T.C.: *The Crypto Anarchist Manifesto,* 1992, [cit. 18.7.2006]. Dostupné z: http://www.activism.net/cypherpunk/crypto-anarchy.html

Metac0m: *What is Hacktivism?*,2003, [cit. 25.8.2006]. Dostupné z: http://www.thehacktivist.com/?page_id=97

Metac0m: *What is Electronic Civil Disobedience?*, 2001, [cit. 25.8.2006]. Dostupné z: http://www.thehacktivist.com/?page_id=98

Mezinárodní pakt o občanských a politických právech, 1966, v platnost 1976, dostupné z: http://www.ohchr.org/english/law/ccpr.htm#art49

Miss M., Plant S., Dement L.: *An interview with Sadie Plant and Linda Dement*,1996,[cit.26.7.2006].Dostupné z: http://www.t0.or.at/dolores/interviews/intervwtoc.htm

Nunes M.: *Baudrillard in Cyberspace: Internet, Virtuality, and Postmodernity*, Georgie Perimeter Collage, 1995,[cit. 16.8.2006]. Dostupné z: http://www.gpc.edu/~mnunes/jbnet.html

Oxblood Ruffin: *Hacktivism, From Here to There*, Yale Law School,2004,[cit.15.7.2006].Dostupné z: http://www.cultdeadcow.com/cDc_files/cDc-0384.php

Rushkoff D.: *Kyberie, život v kyberprostoru*, z ang. org. *Cyberia*, HarperCollins 1994, přel. S. Neumann, Praha, SPVČ 2000

Thomas D.: *Hacker Culture*, Minneapolis, The University of Minnesota Press 2002

Virilio P.: *Informatická bomba*, z francouzského orig. *La bombe informatique*, Galilée, 1999, přel. M. Pacvoň, Červený Kostelec, nakl. Pavel Mervart 2004

Wray S.: *On Electronic Civil Disobedience*, New York, 1998, [cit. 16.7.2006]. Dostupné z: http://www.thing.net/~rdom/ecd/oecd.html