AKADEMIE MÚZICKÝCH UMĚNÍ V PRAZE

FILMOVÁ A TELEVIZNÍ FAKULTA

Filmové, televizní a fotografické umění a nová média

Audiovizuální studia

BAKALÁŘSKÁ PRÁCE

Hacking v kontextu uměleckého aktivismu

Jonáš Svatoš

Vedoucí práce : Miloš Vojtěchovský

Oponent práce : Ondřej Vavrečka

Datum obhajoby : 13.9.2016

Přidělovaný akademický titul : BcA.

Praha, 2016

ACADEMY OF PERFORMING ARTS IN PRAGUE

FILM AND TELEVISION FACULTY

Film, Television and Photographic Arts and New Media

Audiovisual Studies

BACHELOR THESIS

Hacking in the context of artistict activism

Jonáš Svatoš

Thesis adviser : Miloš Vojtěchovský

Examiner : Ondřej Vavrečka

Date of defence : 13.9.2016

Academic title to be assigned : BcA.

Praha, 2016

P r o h l á š e n í

Prohlašuji, že jsem bakalářskou práci na téma

Hacking v kontextu uměleckého aktivismu

vypracoval samostatně pod odborným vedením vedoucího práce a s použitím uvedené literatury a pramenů.

Praha, dne ....
podpis diplomanta

Upozornění

Využití a společenské uplatnění výsledků diplomové práce, nebo jakékoliv nakládání s nimi je možné pouze na základě licenční smlouvy tj. souhlasu autora a AMU v Praze.

Evidenční list

Uživatel stvrzuje svým podpisem, že tuto práci použil pouze ke studijním účelům a prohlašuje, že jí vždy řádně uvede mezi použitými prameny.

Jméno	Instituce	Datum	Podpis

Abstrakt:

Práce se zabývá aspekty různých taktických nástrojů a strategií, navržených k narušení, či znemožnění přenosu informace, zejména otázkami intervence v informačních sítích. Práce se věnuje problematice tzv. hackingu, který nastiňuje i z historického kontextu mediálního aktivismu, jako i z pohledu umělecké praxe.

Abstract:

The work deals with various aspects of the tactical tools and strategies designed to disrupt or disable transmission of information, in particular regarding to issue of intervention in information networks. The work addresses the issue of “hacking”, which also outlines in the historical context of media activism, as well as from the perspective of artistic practice.

Obsah

Předmluva

Tématem práce je průzkum a popis různých forem subverzivních intervencí do informačních sítí, zejména s důrazem na vizuální či konceptuální uplatnění nástrojů aktivismu v době informační společnosti. Nejprve se zabývám obecnou problematikou počítačového aktivismu, jeho původem, společenským kontextem a technologickými předpoklady. V dalších kapitolách analyzuji tzv. hacking jako uměleckou strategii, přičemž uvádím několik příkladů. Závěrečná část textu je pokusem o shrnutí této problematiky. Snažím se používat především české výrazy, nicméně v několika případech vzhledem ke specifickému zaměření český překlad neexistuje – přistupuji tedy k vysvětlení pojmu pod čarou.

Úvod

Text pojednává o „narušení“ komunikačního prostředí, především z perspektivy hackerů, experimentátorů, průzkumníků a umělců – kyber-aktivistů, kteří usilují o prosazení určité myšlenky nebo postoje pomocí specifických nástrojů – například schopnosti nalézat „chybu“ v cizím kódu, vytvářením kódu vlastního, či posunutím informačních a komunikačních technologií do kontextů které kladou otázky po roli vzájemně propojených strojů ve společnosti. Pomocí hledání vstupu do systémů nastavených omezení, které původně splňují především komerční účely, či mají funkci restrikce přístupu veřejnosti k jistému druhu informací, vznikají nové souvislosti a prostory pro diskuzi,

Bruce Sterling popisuje podobné aktivity v textu „**Zátah na hackery“** následovně :

„Hackeři se různí svým stupněm nenávisti k autoritám a násilnickostí své rétoriky. Ale všichni v zásadě nerespektují zákon. Nepovažují současná pravidla chování v cyberspace za žádoucí úsilí o ochranu práva a pořádku a udržení bezpečí. Považují je za nemorální snahu bezduchých společností chránit své zisky a ničit opozici. „Hloupí“ lidé, včetně policie, obchodníků, politiků a novinářů, prostě nemají právo soudit akce elitních expertů, uskutečňujících technickou revoluci.“[1]

1 Sterling, Zátah na hackery, 1994, s. 17

To vše jak za určitým cílem, ale i ze zvědavosti či pro prosté pobavení se na cizí účet. Používáním nesrozumitelných rozhraní vytvořených na míru vytvářejí mimikry které není jednoduché prohlédnout.

Co je **kyberaktivismus**, jaká je jeho genealogie? Jedná se aktivity jenž se uskutečňují na pomyslné hrací ploše – uvnitř **kyberprostoru**.
Tento termín označuje *„nehmotné prostředí, v kterém probíhá komunikace mezi elektronickými systémy“*[2]. Jako první[3] tento pojem v kontextu virtuálního světa použil William Gibson v krátké povídce „Burning Chrome“:
„Konsenzuální halucinace prožívaná denně miliardami legitimních operátorů, v každém národě, dětmi, které se učí matematickým pojmům... grafické zobrazení dat abstrahovaných z pamětí každého počítače v lidské společnosti. Nepředstavitelná komplexita. Linie světla rozprostírající se v neprostoru mysli, klastry a konstelace dat. Jako světla velkoměsta, vzdalující se..."[4]

V souvislostech současnosti by bylo uvažovat o kyberprostoru jako o synonymu pro internet pošetilé. Kyberprostor je třeba chápat jako nižší rovinu systému, nad kterou se nachází další druhy sítí, jako **elektronický proto-prostor,** ze kterého ostatní vycházejí. Do něho pak vstupuje jen omezená komunita operátorů, administrátorů, „údržbářů“ a dobrodruhů, kteří zde hledají potěšení či předmět obskurního podnikání. Nejde pouze o síť WWW[5] či e-mail, jedná se o nespočet dalších protokolů jako MQTT, RTP, RTSP, XMPP[6], které obsluhují služby vzájemné komunikace mezi uživateli či zařízeními. Jedná se o sítě neveřejné, i sítě naopak skrze internet „tunelované“ a dostupné každému, jako například TOR[7], jakýsi „internet v internetu“ ,který vytváří zdánlivě neviditelnou strukturu, v níž je možno se „ukrýt“.

2 [cit. 2016-08-29] http://www.oxforddictionaries.com/definition/english/cyberspace
3 První zmínka o tomto slově pochází patrně z názvu dánského víceúčelového prostoru “Atelier Cyberspace“, avšak dle jeho tehdejších členů „Pojem cyberspace pro nás byl pouze o manipulaci s prostorem, nešlo o nic ezoterického, nic digitálního. Byl to pouze nástroj, místo bylo konkrétní, fyzické“. [onilne] http://www.kunstkritikk.com/kommentar/the-reinvention-of-cyberspace/
4 William Gibson, Neuromancer, překlad Josef Rauvolf, Laser-books, 2010, ISBN 978-80-7193-318-2
5 WWW – World Wide Web je informační prostor vzájemně propojeného hypertextového obsahu založený na protokolu HTTP.
6 MQTT – Machine Queuing and telemetry protocol, RTP – Realtime transport protocol, XMPP – extensible messaging and presence protocol.
7 TOR – The Onion Router – https://torproject.org/

Technologická sofistikovanost tohoto „ne-prostoru“ a současná předvídatelnost na základě pravidel definovaných počitačovým systémem – a tedy zákony matematické logiky, dává vzniknout množství rozmanitých rozhraní vhodných k jeho prozkoumávání: od textových (např. Bulletin Board systémy), až po rozhraní kombinující různá multimédia (World Wide Web, Geocaching, Augumented Reality).

Míra sofistikovanosti jednotlivých, nad kyberprostorem postavených rozhraní, je úměrná výpočetní kapacitě soudobých počítačových systémů a průměrnou propustností linek, které jednotlivé segmenty propojují. Jako kyberprostor lze chápat i „vnitřní“ prostředí většiny dnešních počítačů, jelikož jejich technologický design je od podstaty založen na principu sítě[8]. Každý program může pak být pouze jedním z mnoha vnitřních uživatelů počítače, komunikace s ostatními programy probíhá na stejném principu jako komunikace dvojice lidí přes datové spojení například mezi kontinenty. Dle mého názoru **v kyberprostoru neexistuje rozdíl mezi člověkem a strojem**, jelikož uživatel existuje pouze v podobě symbolické reprezentace sebe sama prostřednictvím kódu a dat, které jsou alokovány v paměti počítače. Jinak řečeno, jeho prezentace odpovídá struktuře a funkcionalitě nástroje, který si pro komunikaci v kyberprostoru zvolil.

Druhý pojem z kterého výše uvedený termín vychází - **aktivismus** (z lat. a*ktivus* – činný[9]) - označuje společenský nástroj, datující se od dob, kdy došlo ke společenské segregaci vlivem kumulace moci a majektu elitními skupinami na úkor níže postavených vrstev. Tato nerovnost je pak působením sociální dynamiky vyrovnávána buď prosazováním myšlenek či postojů, a tím vytvářením sociálního pnutí, nebo vytvořením intelektuální či informační převahy, s cílem vyvolání změny shora, skrze cestu přejímání myšlenek vládnoucí třídou.
Jedná se tedy o **soubor taktických nástrojů k použití „přímé akce“ k dosažení určitého cíle**.
Aktivismus je rozdělován Ondřejem Císařem v práci „Politický aktivismus v České republice“[10] do několika hlavních směrů.

8 [cit. 2016-08-29] https://fgiesen.wordpress.com/2014/03/23/networks-all-the-way-down/
9 Rejzek, 2001, s. 48
10 Císař, 2008

Aktivismus politický – *„více či méně profesionální aktivity obhájců určitých politik a sociálních opatření na úrovni politických organizací“*[11].
Enviromenální aktivismus – enviromentalismus je směr, který prosazuje důležitost životního prostředí, a pro který je typická činnost mnoha zájmových skupin napříč hranicemi. Císař konstatuje : *„Tento aktivismus je dnes do značné míry namísto přímé účasti a členství založen na existenci (často malých) nečlenských advokačních skupin, charakterizuje jej závislost na externích zdrojích a důraz na meziorganizační interakce/transakce“*[12], a tento druh aktivismu zařazuje do hlavního politického proudu.
Oproti tomu **radikální aktivismus** je ten, který „nespolupracuje“ : *„Radikálové nespolupracují s mainstreamovými aktivisty a ani ti nestojí o to, aby byli viděni jako spojenci radikálů“*[13]*.* Jedná se o hnutí, které je spojeno s určitou subkulturou, jejímž nástrojem je tzv. „přímá akce“ (Direct Action). Stejně jako v případě „radikálního enviromentalismu“, jehož nástrojem k prosazení cílů je například blokáda dálničních tahů, kyberaktivismus lze chápat jako variantu radikálního aktivismu – s pomocí technologických nástrojů elektronických informačních sítí – například pomocí internetu – je uplatňována snaha o řešení socioekonomického problému.
Jiným strategickým prostředkem je narušení či „pozměnění“ média, které přenáší zprávu (např. pozměnení textu či obrazu během trajektorie mezi odesilatelem a příjemcem). Dalším modelem je zabránění přenosu informace (např. DoS útok[14]).
To je akt sám o sobě významotvorný – McLuhan tvrdí že *„médium je sdělení“*[15], zároveň **absence sdělení je sdělení samo o sobě**.

Dochází tedy k přesunu kontroly nad obsahem z odesílatele na tzv. „muže uprostřed“ (Man In The Middle[16]), který je v tu chvíli tím, kdo získává nad komunikací kontrolu.

V nedávné době se pro podobné aktivity vžilo označení **hacktivismus**. Jedná se pouze o jednu ze spektra taktik, která propojuje uvedené disciplíny. Využitím

11 Císař, 2008, s. 8
12 Císař, 2011, s. 141
13 Císař, 2011, s. 141
14 Denial of Service – umělé zahlcení serveru vysokým množstvím požadavků, což má za následek nedostupnost služby pro legitimní odběratele.
15 McLuhan, 1964, s. 7
16 Man In the Middle – institut třetí strany, která se vyskytuje mezi odesílatelem a přijemcem elektronické zprávy, a může tedy se zprávou a jejím obsahem libovolně manipulovat.

technologické převahy, dosahuje cíle, především útoky na internetové servery s vysokou návštěvností, přičemž na témata upozorňuje nejčastěji jejích znepřístupněním (již zmíněný DoS útok). Motivem takového počínání bývá potřeba tvořit „dobro“ (v mravním smyslu), nicméně ne nezbytně. Z pohledu implicitně obhajitelného aktu vniknutí se používá pojem **ethical hacking**, tedy disciplína specifická pro skupinu tzv. „white-hat“ hackerů, kteří objevují chyby v cizích systémech na základě smluvního vztahu.

V následující části se pokusím popsat hackerskou subkulturu skrze různé její definice.

Hackerské subkultury a jejich geneze

Hacking je disciplínou, spojenou s fenoménem fyzického poznávání a pozměnování zejména technických prostředků (tzv. bastlení), či pronikání do vlastního či cizího počítačového kódu s cílem změny jeho funkčnosti. Buď za účelem šikovné a rychlé úpravy, nebo za ovládnutím určitého elektronického systému bez vědomí jeho autora či vlastníka. Termín je odkazuje na původní význam slova – v překladu z angličtiny sekat – do post-industriální doby, kdy místo opracovávání fyzických materiálů dochází k úpravě vlastností technologických systémů včetně softwarových programů.

Steven Levy popisuje aktivity hackerů ve knize *Hackers: Heroes of Computer Revolution* následovně:
„Přestože některí kolegové v oboru používali termín "hacker" jako formuvýsměchu, to že hackeři byli viděni buď jako sociální outsideři , či "neprofesionální" programátoři, kteří psali ošklivý a nestandardní počítačový kód, vnímal jsem je odlišně. Pod jejich často nevzhlednými zevnějšky se skrývali dobrodruzi, vizionáři, hazardéři, umělci … a ti, kdo nejjasněji viděli, proč je počítač skutečně revoluční nástroj.“[17]

17 Levy, 1984, s.4

Naopak McKenzie Wark popisuje subkulturu v **A Hacker manifesto**[18]: *„Hackeři vytvářejí nové možnosti jak věci přicházejí na svět. Nejsou to vždy skvělé věci, či dokonce ani dobré věci, ale jsou to věci nové. V umění, ve vědě, ve filozofii a kultuře, v každém znalostním odvětví kde vznikají data, z kterých lze extrahovat údaje jež vytvářejí nové možnosti pro svět, všude tam jsou hackeři vytvářejíc nové ze starého.“*[19]

Tématem hackingu se zabývá množství autorů a vyšlo o něm řada knih a textů. Alespoň některé z nich zmiňuji. Jedná se v zásadě o dvě skupiny autorů, ti, kteří píší o komunitě „zevnitř“, byli tedy v určitou dobu přimo součástí subkultury, či se pohybovali v jejím těsné blízkosti. Druhá skupina jsou ti, kdo o fenoménu hackingu uvažují zvenku, a to především ti, kdo nebyli přímou součástí, ba naopak - byli dokonce i „na druhé straně“. Aspekt rozdělení na dvě vzájemně soupeřící skupiny – hackery, phreakery, crackery na jedné straně, a policii spolu se zástupci telekomunikačních společností na straně druhé, je v mnoha ze zaznamenaných příběhů právě ústředním motivem.

Mezi autory, kteří o hackingu píší na základě vlastní zkušenosti patří například Bruce Sterling s knihou “**Zátah na hackery“**[20]. Autor zde na pomezí non-fiction a literárního textu, ve světle zásahu proti americkému počitačovému podsvětí v roce 1990 objasňuje řadu detailních popisů tehdejších událostí, jejich účastníků a dobových kontextů o prostředí, kterému říkáme kyberprostor, ještě před nástupem internetu uprostřed 90. let 20. století. Především věnuje pozornost legendě hackerské scény v USA - známému uskupení **Legion of Doom**. Ne náhodou je Sterlingova kniha jednou z nejčtenějších v tomto okruhu,neboť její autor se sám podílel na vzniku žánru a posléze celého kulturního fenoménu s názvem cyberpunk, a právě on hackerskou subkulturu de-facto definoval. Podobným způsobem popisuje situaci na několika případech australanka Suelette Dreyfuss v “**Podsvětí“**[21], kde mapuje prostředí australské hackerské scény skrze vyprávění příběhů několika místních skupinek. Většina popisovaných reálných postav byli v době událostí ještě teenageři,

18 Wark, 2004
19 Wark, 2004, s.15
20 Sterling, 1992
21 Dreyfus, 1997

a nebylo tedy možné je odsoudit k vysokým trestům. Jedním z nich je i příběh níže zmiňovaného Mendaxe, který pronikl a ochromil mezinárovní počítačovou síť SPAN, stejně tak i jeho spolupracovníků Prime Suspect a Trax, kteří úspěšně pronikali do celosvětové sítě telefonních ústředen firmy Nortel. Další z příbehů pojednává o hackerech s přezdívkami Phoenix, Nom a Electron, kteří se stali v Austrálii prvními odsouzenými za vniknutí do počítačového systému.

Protikladem k beletriím o hackerech je zmíněná práce "**A Hacker Manifesto"**, formou připomínající Debordovu „**Společnost spektáklu**[22]" - klíčové situacionistické dílo, dělené do 221 krátkých tezí. McKenzie tuto formu využívá, a ve 389 tezích definuje vlastní chápání hacku jako institutu informační derivace. Tvrdí, že nejdůležitější je akt tzv. abstrakce : *„Jsme hackeři abstrakce, vytváříme nové koncepty, vnímání, senzace, vysekáváme je ze surových dat"*[23]. Chápe hack jako nástroj třídního boje, a definuje třídu tzv. vektoralistů – informačních magnátů, pojmenovanou podle množství vektorů, kterými se informace mohou šířit, zejména ve spojitosti s komodifikací informací : *„Vektoralistická třída ve vývoji vektorálních nástrojů produkce a distribuce vidí způsob, jak vytvořit rozhodný nástroj dosáhnutí globální komodifikace skrze komodifikaci informací"*[24].
Stephen Levy se v knize „Hackers: Heroes of the Computer Revolution" věnuje především generaci šedesátých a sedmdesátých let – tzv. **opravdovým hackerům**, především těm, pohybujícím se v okolí **TMRC**[25] – klubu příznivců železničních modelů. Je ironické, že skupina lidí, jež původně barvila železné modely na zelenožluto, stála na počátku nové technologické revoluce. Následně se také věnuje „hardware hackingu", popisuje například příběh Steva Wozniaka a okolnosti vzniku prvního osobního počítače který změnil svět – Apple II[26]. Softwarové hackery zahrnuje v podobě popisu nově vznikajícího herního průmyslu 80. let, především na příběhu Richarda Garriota, autora nejznámější série her na hrdiny - Ultima[27].

22 DEBORD, Guy. Společnost spektáklu. V Praze: Intu, 2007. ISBN 978-80-903355-5-4.
23 Wark, 2004, s. 14
24 Wark, 2004, s. 121
25 Tech Machine Railroad Club
26 Levy, 1994, s. 197
27 Levy, 1994, s. 312

V případě evropské hackerské scény bych rád zmínil publikaci “**Hacking Europe - From Computer Cultures to Demoscenes**“[28], která vykládá genezi hackingu na starém kontinentě jako sérii oddělených událostí, které se na sklonku 90. let spojily v kontinentální propojenou subkulturu, především za pomocí úspěchu internetového projektu. Autoři, mimo jiné, v této publikaci popisují níže zmiňovaný tzv. BTX hack německého **Chaos Computer Clubu**.

Vznik této subkultury je datován do období 60. let dvacátého století, kdy se okolo počítačových oddělení prestižních amerických univerzit – přededvším Machesussets Institute of Technology a UCLA[29] - začaly tvořit skupiny studentů s touhou objevovat možnosti nově vznikajících počítačových systémů, a znalosti aplikovat do praxe v podobě otevřených a všeobecně dostupných programů i fyzických nástrojů či „zlepšováků“. Tato malá skupina utvořila živou komunitu, jejíž základ byl především ve vzájemné touze objevovat, diskutovat a vytvářet nezvykle kreativní řešení, často vycházející z volnomyšlenkářských principů tehdejší pokrokové společnosti. To dalo vzniknout unikátnímu ethosu „globálního hackerského hnutí“, které opustilo hranice akademických institucí a stalo se kolébkou pro mnoho dalších generací technologických myslitelů. Je třeba říci, že z tohoto zárodku pochází většina technologických výdobytků, které vytvořily samozřejmou infrastrukturu pro naprostou většinu jakéhokoliv moderního počínání, ať se jedná o operační systém **UNIX** (autoři **Dennis Ritchie a Ken Thompson**), či sadu protokolů **TCP/IP** (**Bob Kahn, Vint Cerf**) ,na kterých je naprostá většina dnešních sítí založena.

Nutno podotknout, že hnutí nebylo nikdy homogenní. Levy komunitu rozděluje[30] na tři hlavní proudy:

1. **Původní hackeři** (tzv. True hackers) – Výše zmíňení pionýři z akademického sektoru, studenti, vědci. Hack je myšlen především jako způsob šikovného zásahu do kódu programu, často za pomocí algoritmů či softwarových rutin pro naprosto odlišné použití.

28 Alberts, 2014
29 University of California Los Angeles
30 Levy, 1984

2. **Hardware hackeři** - „bastlíři“, „telephone freaks“ – „phreakeři“ se silnou tradicí vzájemného setkávání a vyměnování zkušeností. Zde nezřídka znamenal hacking skutečné použití fyzické síly pro úpravu funkčnosti aparátu. V tehdejším Československu existovala tato subkultura v podstatě jako jediná z výše vyjmenovaných, pod označením „bastlíři“. Jedná se tedy o úpravu analogových zařízení, jako jsou různé „tuningy“ televizních a radiových přijmačů, apod.
3. **Software hackeři** – Jednotlivci usilující o pronikání do počítačových systémů, za pomocí hledání chyb v ochraně. Softwarový hacking lze rozdělit na několik podskupin, podle toho, jaký „klobouk“, či jaké úmysly jsou jejich motivací.
   - **White hat**
     - Především jde o bezpečnostní analytiky, kteří na znalosti chyb systému postavili své živobytí.Pak radí v soukromém či veřejném sektoru, jak se účinně bránit proti útokům níže zmíněných skupin. Část z nich se rekrutuje z řad bývalých grey-hat hackerů, kteří se istitucionalizovali, či si na své temné minulosti založili osobní značku, která jim zajišťuje publicitu. Tak se například dostal na „druhou stranu“ Kevin Mitnick,jenž je jedním z nejznámějších odsouzených etických hackerů.
   - **Grey hat**
     - tzv. šedá zóna, která pojímá jak internetový aktivismus, tak i část práce white-hatů, kteří se čas od času nebojí použí neortodoxní metody pro svou činnost. Zpravidla se však jedná o činnost průzkumnou, neinvazivní (ve smyslu menění systémů zevnitř). Sterling však upozorňuje[31], že vzhledem k důležitosti počítačových systémů ve zdravotnictví, dopravě, či průmyslu, může i malá změna, či krátká nedostupnost systému (např. v případě sítě tísňového volání) způsobit smrt toho, kdo je na elektronickém systému v onen okamžik závislý.
   - **Black hat**
     - Black-hat hackeři jsou především ti, kteří úmyslně tvoří škodu či poškození, a to jak na datech – krádeže osobních údajů, kreditních karet aj., tak přímo na zařízeních kde systémy běží. Pokud je někde

31 Sterling, 1992, s. 41

referováno o hackerech v negativním světle, jsou to především tyto skupiny opravdových zločinců, kteří vnikají do systémů pro vlastní obohacení či pro touhu poškození druhé strany z „pochybných“ důvodů.

Hacking bývá často zaměňován na termín **cracking**, což je termín,který označuje činnost související se snahou o obejití softwarové ochrany proti kopírování počítačového programu, což je úkol vyžadující často „zlomení“ určitého zabezpečení, nezřídka šifrovacího klíče.

Historický kontext

Kořeny využití techniky v rámci sociálního nátlaku sahají do počátků průmyslové revoluce – doby, během které industrializace ohrožovala postavení dělníků a kdy se začaly objevovat první případy sabotáží[32] strojového vybavení továren a dílen. Jedno z hnutí které proklamovalo destrukci strojů byly skupiny tzv. luddittů[33], většinou textilních dělníků s mnohaletou pracovní zkušeností, kteří, v obavách o své živobytí, začali organizovaně poškozovat především tkalcovské stroje ze strachu o ztrátu předmětu obživy.

Tyto stroje byly první zařízení[34] jejiž pravidla chodu člověk programoval předem, a stroje pouze vykonávaly to, co bylo zaznamenáno na dvourozměrné matici vpichů do (tehdy již masově rozšířeného) papírového pásku[35], jednalo se tedy o jedny z prvních informačních systémů pro práci s daty.

Na konci 19. století se situace změnila vynálezem spolehlivě fungujícího přístroje na vzdálenou komunikaci - telefonu Alexandra Grahama Bella, a především jeho zavedení do praxe společností Bell Telephone Atlantic. Již v této době byly evidovány útoky na fungování sítě, v podobě spíše žertovné, vycházející z tehdejšího fungování, kdy mladí operátoři – spojovatelé – z dlouhé chvíle přepojovali hovory neznámo kam, aby způsobili zmatek. Jak Bruce Sterling zmiňuje[36], telefonní spojovatelny zaměstnávaly především mladé chlapce, původně kurýry, kteří z

32 Termín sabotáž je slovo jehož kořen vznikl ze slova sabot, což jsou francouzské dřevěné boty, jež měli právě dělníci házet do strojů aby zastavili provoz.

33 Luddité – Skupina technopesimistických, především texilních dělníků.

34 Pokud pomineme stroje na měření času, kde je však termín programování vzhledem k tehdejšímu statickému pojetí vnímání časoprostoru poněkud nevhodný.

35 Děrný pásek - díky jednoduchosti se stal na několik desítek let standardem v ukládání strojově čitelných dat.

36 Sterling, 1992, s. 18

přirozeného nepřátelství k síti jako takové, či pouze pro pobavení přepojovali hovory neznámo kam, vstupovali do konverzací, či je předčasně ukončovali, čímž způsobovali zmatení a vztek části tehdejší, především podnikatelské klientely. Na tradice těchto „zlobivých-kluků-na-drátě“ částečně hackerské hnutí navazuje, jelikož jde stejně tak o vlastní identifikaci s telefonní sítí. A to především na základě jejího prozkoumávání co, či kdo je na druhé straně, a nalézání čeho je síť schopna. Průzkumy takového rázu byly možné především kvůli způsobu fungování telefonní sítě. Tehdejší analogové ústředny používaly na spojování hovorů sérii relé, přičemž pro spojení hovoru bylo u automatických ústředen potřeba relé vzdáleně sepnout v určitém pořadí. Každá soustava relé reagovala na jný počet pulzů za sebou, a pro uskuečnění hovoru bylo třeba sepnout několik těchto soustav současně, tedy vyslání série těchto pulzů, princip velmi podobný telegrafu. Telefonní přístroj, který spojoval hovor jednoduše vygeneroval pomocí vlastní série relátek potřebný počet pulzů, a ústředna propojila hovor sestavením elektrického okruhu. Kromě pulzní volby byla možná i volba tónová, která se však tehdy používala především na přenos servisních signálů skrze linku. Vždy když bylo např. potřeba spojit hovor jako meziměsto z telefonní budky, po zadání dostatečného počtu drobných přistroj vyslal tón o určité výšce, aby tak ústředně sdělil, že se jedná o dálkový hovor. Faktem bylo však to, že vzhledem ke zjednodušení celého systému se servisní signály posílaly po stejném vedení jako hlas (tzv. In-band signaling[37]), bylo tedy možné tón vytvořit svépomocí, např. ho zapískat do telefonního sluchátka a spojit hovor bez drobných. Disciplíně, věnující se obcházení omezení analogové telefonní sítě, se říká **phreaking.**
Ironií osudu bylo, že jeden z původních phreakerů, **John Draper**, veterán z války ve Vietnamu**,** v roce 1971 objevil že není potřeba ani nahrávat tóny z varhan na kazety, učit se pískat, či trénovat zpěvné ptáky pro získání pár minut volného klábosení. Stačilo si zakoupit krabici cereálií, ve které byla zdánlivě neškodná hračka – píšťalka - po zapískání vydávala tón o stejné výšce používanou tehdejšími ústřednami - **2600 Hz**. Tento objev mu vynesl přezdívku **Capt‘n Crunch** podle názvu oné krabice s cereáliemi. Nejednalo se sice o technologický průlom, díky této píšťalce však začal Jhon Draper experimentovat se stavbou zařízení na generování série těchto signálů – tzv. **blue box** aby proces vytáčení automatizoval. Uveřejněním článku o blue-boxu

37 In band signaling – způsob přenosu signalizace po stejném kanálu jako data/hovory. Opakem je out-of band signaling, které pro signalizaci vyhrazuje samostatnou, fyzicky oddělenou linku.

v časopisu Esquire, byla výroba podobných zařízení v následných letech náramě výdělečným zbožím, zejména v univerzitních kampusech. Jedním z těch, kteří se rozhodi na tomto „trendy způsobu okrádání“ nenáviděné společnosti AT&T vydělat, byl též Steve Jobs. Ten díky prodeji těchto krabiček zjistil, že prodej elektroniky může být zábava, na které se dá dobře vydělat.[38]
Během 70. let se následně phreaking velmi rozšířil i mimo území USA a stal se všeobecnou dovedností pro technologicky založené mladé generace.
V roce 1971 došlo k masivní akceleraci vývoje výpočetní techniky vlivem uvedení prvního komerčního mikročipu Intel 4004. Nebylo to ale až do následujícího roku, kdy jeho následovník **Intel 8008** odstartoval revoluci v odvětví osobních počítačů. Tento fakt, a nárazové skokové zvýšení poptávky po mikroprocesorech během první poloviny 70. let, mělo za následek, že každý, kdo si mohl dovolit utratit několik tisíc dolarů, mohl mít doma svůj opravdu osobní počítač, jako např. Altair 8800. Na opačné straně spektra, v akademické sféře tehdy již probíhal slibný, původně armádní pokusný projekt jak propojit všechny vědecké sítě do jedné celosvětové – **ARPANET**, zárodek budoucího internetu.
V první polovině 80. let však s internetem měl v Evropě zkušenosti jen málokdo. Existovalo nicméně několik technologií, které se dokázaly, za pomocí využití existující telefonní síťe dostat do širšího užití, zejména díky propojení s telefonním přístrojem ve formě zobrazovacího terminálu se sluchátkem, obrazovkou a klávesnící, pomocí které uživatel zadával přístroji pokyny. Díky faktu, že byl přístroj silně dotován, a zároveň vysoké ceně tehdejších mainframe počítačů, které by byly těmto „hloupým terminálům“ schopné poskytovat služby šlo o technologie vysoce centralizované, v podstatě výhradně pod křídly telekomunikační společnosti.

Na sklonku 80. let 20. století bylo počítačové vybavení v zemích západního bloku poměrně hojně rozšířeno, nicméně bez výraznějšího vzájemného propojení. Způsob spojení s okolním světem byl z domova možný výhradně skrze telefonní linku pomocí modemu, vytočením určitého čísla a návázání digitálního přenosu s podobným zařízením na straně druhé. Vzhledem k neexistenci jakékoliv centrální sítě, která by uživatele a služby propojovala, bylo rozšířenou praxí, že jednotliví uživatelé tyto

38 [cit. 2016-08-31] http://www.i-programmer.info/history/people/104-steve-jobs-apple.html

centralizované služby nahrazovali. Jednou z prvních takto rozšířených služeb byla elektronická nástěnka – BBS . Každý mohl na nástěnku přidat text jako vzkaz ostatním. Vzhledem k tomu, že se jednalo o uzavřený okruh, kdy v jeden moment mohla být k modemu připojena pouze jedna stanice, ostatní uživatelé byli nuceni čekat až na ně přijde řada, tj. až telefonní číslo přestalo být obsazené. Z tohoto důvodu vytáčení fungovalo z velké části automaticky – uživatel si na nové příspěvky musel počkat někdy i hodiny. Jednalo se tedy o přímé napojení na službu[39], kterou poskytovala stanice ke které byl modem připojen.

Tento způsob přístupu ke vzdálenému systému se však používal i v případě napojení na univerzitní či firemní time-sharing[40] systémy, kdy se uživatelova stanice stala pouze rozhraním k většímu, neporovnatelně výkonnějšímu sálovému počítači. Díky přístupu na mainframe měl uživatel často možnost připojit se na další systémy s mainframem propojené, již ne vytáčenou telefonní linkou, ale formou pevného okruhu (např. X.25, DECnet, či Ethernet) ,propojující jednotlivé akademické instituce do většího celku tehdy převážně univerzitních sítí, které umožňovaly vzájemnou výměnu dat. Praxí bylo, že každý mohl o účet na počítačovém systému požádat na základě svých studijních předpokladů, což bylo zejména u oborů ze kterých se „experimentátoři“ rekrutovali. Tento fakt byl mnoha hackery – průzkumníky - využíván ke získávání zkušeností při oťukávání kyber-prostoru kolem sebe. Univerzitní mainframe jim sloužil jako „hnízdo“ odkud vylétali za dobrodružstvím. Dílem rozšíření subkultury vznikla i některá periodika, která se „podsvětím“ zabývala. Ústřední postavou evangelizace „hackerství“ byl zakladatel čtvrtletníku **2600**[41] (obr. 2) Eric Corley, známy pod přezdívkou **Emanuel Goldstein**. Časopis vychází v nepravidelných intervalech dodnes, přičemž Corley je stále jeho vydavatelem a hlavním přispěvatelem.

39 Narozdíl od tzv. vytáčeného připojení k internetu které slouží pouze jako přemostění telefoní sitě kdy poskytovatel připojení koncovému zařízeni poskytuje přístup do decentralizované sítě skrze protokol TCP/IP.

40 Time-sharing je koncept sdílení výpočetních zdrojů jednoho počítače mezi více uživatelů. Vznikl jako protiklad k dávkovému zpracování úloh, které umožňovalo odbavení požadavků pouze v jasně dané frontě, což znemožňovalo použití počítače více uživateli, často tedy docházelo k jeho neefektivnímu využití. Jedná se o myšlenkový základ systémů z rodiny UNIX, které jsou na současné práci uživatelů – procesů – založeny. Z dnešního pohledu je time-sharing každý počítač, až na mikrokontrolery typu Arduino apod.

41 [online] https://www.2600.com/

Technologické souvislosti

Pro nastínění technologických souvislostí uvádím několik faktů.
Za prvé – veškeré intervence jsou závislé na objevení určitého nepředpokládaného chování, či objevené chybě. Vzhledem k tomu, že v sofistikovaných systémech jako jsou telekomunikační sítě je celková funkčnost závislá na mnoha vzájemně komunikujících částech. Vždy existuje větší či měnší pravděpodobnost, že určitá kombinace stavů jednotlivých komponent v čase, způsobu jejich vzájemného propojení, a vstupních dat bude umožňovat využití v útočníkův prospěch. Konkrétnímu plánu na využití jedné či několika „příležitostí“ se nazývá *Attack vector*. V okruhu kyberaktivismu se setkáváme spíše s méně sofistikovanými metodami, jako je zejména využití velmi špatného zabezpečení, selhání lidského faktoru, či nekritického přístupu k technologiím jako takovým. Způsoby sofistikovaného útoku jsou však v dnešní době mnohem jednodušší než v minulosti, a to především díky institucionalizaci celého procesu, kdy existují služby, kde si lze jednoduše koupit nezveřejněnou kritickou zranitelnost (tzv. zero-day exploit[42]), např. pro operační systém Windows 7. Tu následně útočník „doručí“ oběti pomocí volně dostupných nástrojů pro penetrační testování – disciplínu která naopak kyberzločin potírá. Příklad takového útoku lze vidět na obrázku č. 7.

Ze nastiňuji princip síťových protokolů na několika příkladech.
Komunikace mezi dvěma počítačovými systémy je založená na sadě pravidel, které nazýváme protokoly. Tyto protokoly existují v několika vrstvách. Jiná pravidla platí pro určení jak jsou zařízení fyzicky spojena, jak jsou modulovány elektrické signály i na jakém základě komunikují aplikace, které přenos vyžadují. V roce 1984 pro tuto sadu protokolů vznikl standard **OSI** (schéma na obr. 3), který určil, že jednotlivých vrstev bude sedm. Každá z nadřazených vrstev přímo závisí na té předchozí.[43]

42 Zero-day exploit – zranitelnost, jíž lze velmi jednoduše zneužít, a zároveň dojde k jejímu veřejnému odhalení bez současného vydání odpovídající opravy, dochází tedy k tomu, že tuto zranitelnost v ten samý den vyzkouší mnoho útočníků s tím, že správce systému se může o chybě dozvědět až po jejím zneužití. Má tedy doslova – 0 dní (0 days) na to aby chybu opravil,

43 OSI Reference model implementation - [cit, 2016-09-01] https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-X.200-199407-I!!PDF-E&type=items

V případě služby WWW se jedná o protokol HTTP je tzv. *bezstavový*, tzn. spojení je co nejrychleji uzavřeno po přijmutí informace (obr. 4). Oproti tomu existují i tzv. *stavové* služby, kdy si každá strana uchovává v jakém stavu-kontextu je právě otevřené spojení.
Příkladem mohou být služby pro přístup na vzdálený terminál, např. telnet, či SSH. (obr. 5)

Hacking jako umělecká metoda

Hacking lze chápat jako způsob prosazení určité myšlenky nejen na technologickém základě, ale i v kulturním nebo uměleckém kontextu. Můžeme na něj pohlížet jako na metodu v rámci skupiny aktivistických přístupů - tzv. **Tactická média**, což je pojem z okruhu nových médií, který souvisí s občanským aktivismem a do jisté míry na něm staví. Jde o disciplínu, jejíž modus-operandi není jasně ohraničen – spojujícím faktorem je tendence nejen se vyjádřit, nýbrž i vyvolat určitou společenskou změnu, či odezvu na základě interakce s okolím za pomocí využití uměleckých postupů. Může mít podobu např. distribuce letáků, intervence do veřejného prostoru pomocí pirátské videoprojekce, nebo i hacktivistického přístupu, kdy využitím níže zmiňovaných postupů dochází k přenosu sdělení podobně jako u ostatních uměleckých přístupů.
V případě hackingu je taktika zásadním aspektem díla. Jednotlivé přístupy z hlediska způsobu přenosu myšlenky nyní zmiňuji.

Intervence

Intervence funguje především jako ofenzivní taktika vůči již existujícímu objektu či uměleckému dílu jak ve světě věcí, tak v kyberprostoru. Intervenci můžeme v kontextu uměleckého aktivismu chápat jako způsob performativní akce, během které dochází k pozměnění zdrojových dat, jako v případě níže uvedeného příkladu intervence do vědecké sítě SPAN. Jedná o nejrozšířenější způsob práce s kyberprostorem v uměleckém kontextu. Ačkoliv se může jevit, že každý akt operace nad elektronickou sítí je intervence, není tomu tak.

Dekonstrukce

Dekonstrukcí se rozumí rozložení původního objektu,či myšlenky na menší celky. Julian Oliver například provádí v rámci performance „Men in Grey“ dekonstrukci síťového provozu, aby jeho surrogát zobrazil na displeji LCD monitoru a zároveň prohazuje data mezi uživateli. Komplexní objekty, jako webové stránky, či e-mailové zprávy rozkládá na pakety, které následně upravuje, a následně sestavuje v jiném kontextu uživateli který nebyl původním přijemcem.

Postprodukce

Pojem definoval Nicolas Bourriard ve svém textu „Postprodukce“ : *„Od počátku 90. let 20. století se stále více a více umělců zabývá interpretací, reprodukováním, novým vystavováním či jiným využíváním děl ostatních umělců nebo kulturních produktů, které jsou k dispozici.*[44]*“, a pokračuje : „..umělci pracují s objekty, které již obíhají na kulturním trhu, tj. nesou informace, které do nich vložili jiní lidé.“*[45]

Trevor Palgen skrze Autonomy Cube postprodukuje umělecký objekt v galerii, především Haackeho „Condensation Cube“ do formy skrze internet dostupné občanské služby. Ta se vtěluje do uměleckého artiklu jakoby mimochodem – jde totiž především o mimikry, jelikož hlavním úkolem je poskytovat službu anonymizace, a to především těm na „druhé straně“ linky – uživatelům v zemích s opresivními pravidly regulate internetu.

Popis vybraných příkladů

Zločin pana Wau

V polovině 80. let, ještě před příchodem internetu zřídíla v tehdejším SRN spolková pošta síť pod názvem Bildschrimtext – zkráceně BTX. Jednalo se o výše zmíněnou sít založenou na přímém modemovém spojení s centrálou telefoní společnosti. Terminály (obr. 7) se výrazně rozšířily jak do domácností, tak jimi byly vybaveny i veřejná místa – pošty, úřady, nákupní domy, nádraží. Způsob zpoplatnění byl stejný jako v případě telefoní služby – za „hovor“, v tomto případě za zobrazenou stránku. Na veřejných místech za mince, doma na účet. Skutečnost že šlo poprvé o

44 Bourriard, 2004, s. 3
45 Bourriard, 2004, s. 3

takto masivně duplexní[46] datový kanál, nahávala přesunu mnoha z agend informační společnosti do této elektronické podoby. Ještě před příchodem této služby vznikl v Hamburku v létě roku 1981 spolek nadšenců, kteří se v předtuše toho, jak informační technologie promění životy obyčejných lidí, začali zabývat techno-aktivistickými implikacemi takového počínání. Spolek je do dneška znám jako Chaos Computer Club. Jedním ze zjištění jednoho ze zakladatelů – Wau Hollanda byl po uvedení tohoto systému fakt, že uživatelský BTX terminál je pouze ochuzenou verzí terminálu, který je používán pro vytváření obsahu. Inženýři IBM – dodavatele systému, si totiž nejspíše zjednodušili práci tím, že oba terminály odlišili pouze tak, že tomu klientskému chyběla dvě tlačítka pro zahájení a ukončení editačního módu, programové vybavení bylo stejné.

Wau postupně zjistil, že jednoduchou úpravou zevnějšku klientského zařízení lze dodatečně přidat chybějící tlačítka – nebylo tedy nutné ani porušit homologační pečeť, a vzhledem k centralizaci systému bez jakéhokoliv zabezpečení, bylo možné vytvořit vlastní on-line službu, či pozměnit službu již existující.

Wau následnými experimenty zjistil, že v případě nesprávného pozměnění stránky Hamburger Sparkasse dojte k přetečení zásobníku[47] které na obrazovku vypíše autentizační kódy do systému banky, který zadává platby. Toho následně se svými společníky využil k vytvoření vlastní BTX služby, která za 9,99 DM uživateli dovolila zahrát si hru s vláčkem sbírající mince ve tvaru loga spolkové pošty (obr. 8), přičemž však platbu nestrhávala jemu, ale právě Hamburger Sparkasse za pomocí zmíněných přístupových kódů. Pro větší efekt mládenci z CCC napsali jednoduchý program, který stále dokola volal číslo jejich pirátské služby, a během jedné noci se jim povedlo provést zhruba 13 500 spojení, což připravilo hamburskou spořitelnu zhruba o 135 000 západoněmeckých marek. Faktem je, že skupina nehledala obohacení, pouze se snažila poukázat na nekritické nahlížení na technologii skrze využití snadno nalezitelných zranitelností, a tak následující den uspořádala tiskovou konferenci, kde „peníze“ veřejně vrátila, aby tak veřejnosti demonstrovala,jak jednoduché je zneužít takový systém pod centrální správou. Skupina byla zprvu sice považována za partnera při řešení problémů s BTX, následně však naopak dostalo

46 Duplexní spojení – spojení, pomocí kterého je možné posílat zprávy oběma směry po jednom okruhu.

47 Buffer Overflow – jedna ze základních chyb v programování digitálních systémů, která má za následek překročení paměťového prostoru vyhrazeného aplikaci nesprávným odkazováním na bloky v paměti. Výsledkem může být získání přístupu k datům z bezprostředně následujícího pamětového bloku.

celé uskupení CCC do konfliktu a bylo vyšetřováno podle teroristického paragrafu. Případ ve výsledku „vyšuměl do ztracena“ kvůli nejistotě, zda CCC opravdu kódy odposlechlo přímo ze systému banky, či je získali jinou cestou. Hra s vláčkem byla v tomto příběhu ironickým nástrojem kritiky centralizovaných informačních systémů 80. let. Nejednalo se sice zdaleka o první případ krádeže peněz skrze elektronický systém, událost nicméně rozhýbala debatu o zranitelnosti nově vznikajících veřejně přístupných informačních systémů a nutnosti dát jejich zabezpečení určitý legální rámec. Ve výsledku by se dalo říci, že CCC udělalo hackerskému hnutí určitou medvědí službu, protože i v návaznosti na tuto událost (nutno podotkout, že nejen na ni) došlo v NSR k vytvoření §263a StGB[48] , které podobná vniknutí, i se snahou poukázat na špatné zabezpečení, postihuje odnětím svobody až na 5 let. Podobný zákon vznikl v roce 1984 i v USA, tzv. CFAA[49] - zákon velmi kontroverzní zejména z důvodu, že kriminalizoval hackery i v případě, že vniknutím do systému nevznikla hmotná škoda a neexistovaly žádné oběti. Nezřídka jim byl vyměřen trest odnětí svobody v trvání až několika let. Nejznámější je nejspíše případ Kevina Mitnicka, phreakera, který se na přelomu 80. a 90. let prolamoval do nejrůznějších systémů v privátním i veřejném sektoru. Jeho motivací nebyl nicméně ani zisk či politický statement, ale dle jeho vlastních slov - obsese a aktem prolamování systémů. Mitnick se po sériích her na kočku a myš dostal na útěk a před FBI se úspěšně několik let skrýval pod ukradenou identitou. Po jeho dopadení státní zástupce přesvědčil velkou porotu, že je Kevin Mitnick hrozbou pro národní bezpečnost a dokázal by se v přítomnosti telefonu doslova „propískat“ až k systému pro odpalování jaderných hlavic. Ta mu uložila čtyřletý trest v oddělené cele a 5 let zákazu používat jakékoliv elektronické komunikační sítě.

Červ WANK

17. Října 1989 měl být v NASA velký den. Dlouho připravovaná a už dvakrát odložená sonda Galileo měla v rámci mise STS-34 odstartovat na palubě raketoplánu Atlantis, který ji měl vynést na oběžnou dráhu Země aby se následně vydala směrem k Jupiteru jako první sonda, která se usadí na jeho oběžné dráze a následně na planetě přistane. Vzhledem ke vzdálenosti a nepříznivým podmínkám,

48 Deutsches Strafgesetzbuch [cit. 2016-09-01] http://www.gesetze-im-internet.de/englisch_stgb/englisch_stgb.html#p2187

49 Computer Fraud and Abuse Act – [cit. 2016-09-01] https://www.law.cornell.edu/uscode/text/18/1030

které na planetě panují, bylo rozhodnuto o použití zdroje energie založeném na tepelném rozpadu radioaktivního izotopu plutonia[238]. To vyvolalo v části společnosti značné znepokojení, vzhledem k tomu, že se jednalo o první misi raketoplánu po havárii Challengeru, a zároveň ke zkušenostem se sanací havárie ruského vojenského satelitu Cosmos 954 na nukleární pohon v roce 1978, kdy došlo k rozplýlení radioaktivního materiálu na ploše 124.000 km^2 – území které zhruba odpovídá rozloze Severní Koreje. Na mysu Caneveral byla situace vyostřená. Odpůrci dokonce uspěli se žalobou na neústavnost u obvodního soudu, který ale start pět dní předem povolil. To nicméně nezabránilo mnoha protestům ve dnech před startem.

Stejného dne ráno týmy vědců, tj. uživatele první celosvětové vědecké počítačové sítě SPAN velmi překvapilo, když se jim při zapínání vlastního počítače od firmy Digital Equipment Corporation zobrazil místo uvítací obrazovky mateřské organizace podivný ASCII-art[50] :

```
  W O R M S   A G A I N S T   N U C L E A R   K I L L E R S
 _____________________________________________________________
 \__  _____________  _____  _________  ____  ____   __  _____/
  \ \ \    /\    / /    / /\ \       | \ \  | |    | | / /    /
   \ \ \  /  \  / /    / /__\ \      | |\ \ | |    | |/ /    /
    \ \ \/ /\ \/ /    / ______ \     | | \ \| |    | |\ \   /
     \_\  /__\  /____/ /______\ \____| |__\ | |____| |_\ \_/
       \_____________________________________________________/
        \                                                   /
         \    Your System Has Been Officially WANKed      /
          \_________________________________________________/

  You talk of times of peace for all, and then prepare for war.
```

Nejednalo se nicméně o žádný žert místního administrátora, nýbrž o první virus, který napadl distribuovanou počítačovou síť. Virus je nepřesné označení, ve skutečnosti šlo o červa (worm), označení které má svůj původ právě v tomto incidentu. Vyznačuje se tím, že se nezadržitelně šíří po počítačové síti a používá jednu z kritických zranitelností (tzv. zero-day exploit).

Za červem podle dostupných informací stál jediný hacker s přezdívkou Mendax, jehož identita není známa, spekuluje se ale o Jullianu Assangovi, zakladateli serveru WikiLeaks[51]. Akt samotný měl upozornit na zmíněnou nukleární hrozbu související s vypuštěním samotné družice, a na obecné závody ve zbrojení. Klíčem k odhalení

50 ASCII-art je samostatnou disciplínou v oboru počítačového umění který jako své vyjadřovací prostředky používá paletu 128 platných znaků v tabulce ASCII – zkratka pro American Standard Code for Information Interchange.

51 Události v Assangově životopisu korelují s těmi popsanými v knize Underground viz. Dreyfuss, 1997

motivu byl fakt, že virus nenapadal jen jedinou oblast v sítí DecNET. Jediný adresní prostor 43 nebyl napaden. Jednalo se o Nový Zéland, který je tzv. Nuclear-free zónou.

Červ byl naprogramován tak, aby se na základě zjištěných okolností a nasbíraných dat sám modifikoval. Navíc každá jeho iterace se chovala mírně jinak. Některé z nich předstíraly mazání souborů, jejich vzájemné přepisování, apod. což astrofyziky. Virus se podařilo dostat po několika týdnech pod kontrolu díky nalezení způsobu jak ho odzbrojit. I když reálné škody virus nepáchal, píše se o několika tisících „promrhaných“ badatelských hodinách. Řada vědců nemohla provádět výzkumné úkoly. Tento červ těžil především z tehdejšího velmi špatného zabezpečení systémů od firmy Digital Equipment Corporation, která nechávala počítačům dodaným do veřejného sektoru obecně známé administrátorské účty se stejným heslem.

Virus za plexisklem

Dvojice **Eva and Franco Mattes** vytvořila pro Venice Biennale 2001 instalaci s názvem **bienale.py**. Název díla je současně názvem počítačového programu, který dílo definuje, a který nedělá nic jiného než se nekonečně množí. Virus - instalace se skládá ze dvou počítačů (obr. 9), každý ve svém obdelníkovém plexiboxu s obrazovkou v opačném směru. Tyto počítače střídavě navzájem infikují jeden druhého virem a následně se léčí. Vzniká tedy nekonečný cyklus, na který se skrze obrazovku LCD displaye díváme podobně jako na ledního medvěda za plexisklem v ZOO, snažícího se stále dokola vyšplhat na strmý útes. Autoři během vernisáže rozdali několik desítek kompaktních disků infikovaných tímto „virem“, aby se infikovaný soubor posléze rozšířil přes internet do milionů počítačů po celém světě. Vzniklo tak globální distribuované umělecké dílo, jehož součástí byla každá nakažená obět. Dílo zároveň vyvolalo hysterickou reakci médií, kterou lze chápat jako přetvoření původního díla v neočekávanou celosvětovou performanci. Eva Mattes na otázku jaká byla motivace k celosvětovému rozšíření viru opověděla : „Jako umělec cítím, že jedinou zodpovědnost kterou mám, je být nezodpvědná“[52]. Symantec – přední antivirová společnost označila ve svých definicích “bienale.py“ za virus, přičemž na všech počítačích, kde byl antivir instalován, došlo k následovnému automatickému odstranění.

52 [cit. 2016-08-31] http://rhizome.org/art/artbase/artwork/biennalepy/

Muži v šedém

Jullian Oliver je jedním z autorů, jehož díla se zaměrují na kritiku technologické podstaty současné civilizace. Dokumentace k performanci s názvem “Men in Grey“ na sebe bere podobu fiktivního standardizačního IETF[53] dokumentu, RFC14 „Manifestace síťové úzkosti“. Performance spočívá v pohybu dvou do šeda odděných mužů s kufříky ve veřejném prostoru, především po kavárnách a místech, kde se setkávají lidé, připomínající agenty blíže neurčené státní organizace. Podstata performance leží ve zmíněných kufřících (obr. 10), jejihž obsahem bylo zařízení na dissekci síťového Wi-Fi provozu, a LCD dispeje zapuštěného do těla kufříku tak, aby kolemjdoucí viděl co se na displeji děje. Zařízení odposlouchávalo provoz na veřejných Wi-Fi sítích a obsahy osobních zpráv, např. e-mailu, chatů, ale i článků, které zrovna návštěvníci kavárny četli a zobrazoval je na zmíněném LCD displeji. Zároveň se i aktivně zapojoval do komunikace tak, že data jednotlivých připojených zařízení prohazoval mezi sebou, lidé tedy najednou viděli místo “své“ komunikace, tu, která patřila tomu u vedlejšího stolu. Men in Grey tím upozorňovali na falešný pocit soukromí v kyberprostoru. Zároveň šířili nejistotu mezi kolemjdoucími právě tím, že si nikdy nemohou být jisti, kdo je „sleduje“ během komunikace. V dnešní době, zejména po zveřejnení informací o masovém sledování ze strany tajných služeb západních zemí, došlo ke skokovému nárůstu použití zabezpečeného spojení na webu[54]. Je tedy otázkou, zdali by podobná performance v dnešní době vyvolala stejný ohlas. Faktem je, že performance byla oceněna zvláštním uznáním poroty festivalu Ars Electronica v roce 2010.

Autonomy cube

Trevor Palgen se dlouhodobě zabývá problémem nelegálního masového sběru dat o uživatelích internetu pro vládní účely. Zejména v souvislosti s odhalením programu PRISM, který provozuje americká NSA za účelem uložení několika dní

53 IETF – Internet Engineering Task Force, výbor zajišťující standardizační proces jednotlivých síťových technologií v podobě tzv. RFC – Request For Comments dokumentů, které každý definují jeden standard. Nejedná se nicmméně o těleso které dodržování standardů vymáhá.

54 Zabezpečeným spojením se myslí především HTTPS – varianta HTTP protokolu za použití způsobu zapouzdření do šifrovaného přenosu realizovaného pomocí protokolu SSL (Secure Socket Layers), či nověji TLS (Transport Level Security). Oba dva způsobe se liší úrovní na které šifrování probíhá. TLS je protokol vrstvy 7 OSI, přičemž SSL je vrstva 6. Čím nižší je vrstva, tím je obecně její zabezpečení jednodužší, a tím snáze prolomitelné, zejména vzhledem k faktu že vrstva musí kromě šifrování pojmout i vrstvu vyšší jako “náklad“

celosvětového internetového provozu do vlastního „bufferu“, v kterém lze vyhledávat chování každého uživatele dle libosti. Jeho práce *Autonomy cube* artikuluje tento problém umístěním jednoho z výstupních a vstupních bodů do anonymizační sítě TOR do galerie – white boxu, v podobě mixed-media objektu v podobě umístění jednodeskového počítače spolu s Wi-Fi přístupovým bodem do epoxidové průhledné kostky (obr.11). Ta může připomínat „Condensation cube“ Hanse Haackeho. Umístěním na piedestal se ze zařízení pro boj s cenzurou stává interaktivní umělecké dílo, které slouží návštěvníkům jako nástroj pro svobodný přístup do internetu skrze vytvořenou Wi-Fi síť. Zároveň komukoli, kdo do internetu přistupuje z druhé strany skrze tento exit-node dává imunitu tím, že v internetu vystupuje pod identitou (IP adresou) instituce, v které je Autonomy cube umístěna. Palgen tak používá taktiku obalení aktivistického aktu do institucionální kritiky metod masového sledování - především v USA.

QUANTUMSQUIRREL

Pokud je řeč o NSA, rád bych zde zmínil aspekt týkající se této organizace, která z podstaty jejího fungování a mise, je entitou, tvořenou především white-hat hackery. Mise NSA sice má od hacktivismu daleko, nicméně vizualita jednoho elementu z uniklých dokumentů (obr. 14-15), které se dostaly v roce 2013 na veřejnost, jistě zaujala nejednoho hackera. Jde o dokumenty, které NSA používá pro školení o tajných programech, určených právě pro masové sledování. Např. tajný program QUANTUMSQUIRREL zneužívá způsobu fungování protokolu TCP/IP tak, že doslova „závodí s časem“ o to, jaký proud dat při stahování z internetu se k oběti dostane dříve – ten původní, pravý, či ten podvrhnutý, upravený dle přání NSA. Jejich součástí jsou často internetové memy[55] přímo či nepřímo parodující snahu ostatních zemí o kybernetickou bezpečnost. Používají formu vysmívání se „hloupým uživatelům“ jako „ovcím“ které žijí v najivní představě soukromí a bezpečí na sítích. Tento fakt hackerské komunitě osvětlil, že i v útrobách tajnůstkářské organizace jsou skupiny, které mají evidentně smysl pro černý humor.

55 Internetový mem je aktivita, koncept, či kus média které se. především jako forma mimikry, virálně šíří. Viz Wikipedia [cit. 2016-09-01] https://en.wikipedia.org/wiki/Internet_meme

Anonymous

Jeden z pilířů hnutí Anonymous je založen na předpokladu, že hacking není pro každého, neboť je třeba znát technologii, trendy, zranitelnost a komunitu. Značka Anonymous vyvrací předpoklad tím, že vytváří zdánlivě celosvětové homogenní hnutí fungující jako kolektiv jedinců – avatarů - bez centrální autority, řízený pouze tím co si společenství demokraticky odsouhlasí. Pro vykonávání úkolů zpravidla existuje sada jednoduchých nástrojů, které zvládne použít každý uživatel internetu (obr. 16). Tyto nástroje nezřídka fungují na principu nulové interakce, tedy že je uživatel na svém počítači spustí a program se připojí do celosvětového „úlu“ ,z kterého přijmá přikazy. Uživatel ze sebe – svého počítače – vytvoří dobrovolně součást řízeného *botnetu*[56], tím provede identifikací s hnutím Anonymous.Tím může být zároveň každý a nikdo. Důležitým prostředkem prezentace jsou pamflety, distribuované klasickou a především elektronickou cestou po sociálních síťích. Jejich vizualita paroduje různé symboly a ikonografii nadnárodních institucí apod. (obr. 17-18)

Electronic Intifada

Na Anonymous navazuje specifické hnutí, které lze souhrnně pojmenovat jako „Electronic Intifada“. Jde o název odkazující k sérií povstání v Palestině, které v několika vlnách celospolečensky aktivizovalo její obyvatele. V tomto konkrétním podání se jedná o povstání elektronické, s cílem zabírání především internetového izraelského „prostoru“. Jsou používány jak nástroje nízkoprahového aktivismu prostřednictvím informování v rámci vlastní mediální služby[57], sociálních sítí a bloggingu, tak i skrze hacking, či znetvoření – defacment – webových portálů souvisejících s izraelskými zájmy (obr. 19). Nejedná se o homogenní hnutí, spíše o distribuovanou myšlenku, ve jménu které různé skupiny s různými zájmy prezentují své postoje.

56 Botnet – Síť virem nakažených počítačů, které jsou útočníkem vzdáleně ovládány pro různé využití jako jsou DDoS útoky, či rozesíláni spamu nebo podvodných e-mailů.

57 Webová prezentace http://www.electronicintifada.net

Závěr

V práci jsem se snažil představit fenomén hackingu v historickém kontextu jako disciplínu v rozmanitých podobách. Východiska i impulzy jsou různorodé, od hackingu jako utilitární metody, přes hacking jako způsob chápání světa, po hacking jako metodu umělecké práce. Velkou výhodou bylo, že se jedná o velmi dobře zdokumentovaný aspekt technologického bytí a činnosti člověka. Z podstaty a povahy tohoto fenoménu však plyne, že jsou tyto zdroje informací často v neakademické formě textu. Problémem je též nedostatek zdrojů o hackerství jako „umělecké formě“ a aktivistický hacking jako forma umění. Moje práce je tedy jen malým příspěvkem k odhalení této specifické formy uměleckého vyjádření.

Vždy když se budeme zabývat technicistním tématem, neexistuje kompletní výklad z jednoho zdroje. Systémy jsou vzájemně propojeny, a to jak fyzicky, síťově tak historicky. Ani moje práce si tak nedává za cíl sloužit jako kompletní průvodce intervencí v kyberprostoru. Jedná se spíše o určitý subjektivní průřez milníky, definicemi a přistupy, který, dle mého názoru může sloužit jako materiál pro uvedení do problematiky hackingu, a pro jeho rámování jako umělecké disciplíny skrze vybrané příklady. Vzhledem k tomu, že čerpám především ze svých praktických zkušeností, uvedl jsem nástin technicistních postupů počátků hackingu a pokusil se uvést do vztahu se současným hnutím.

Seznam literatury

ALBERTS, GERALD – Hacking Europe, From Computer Cultures to Demoscenes, 2014, ISBN 978-1-4471-5492-1

BAZZICHELLI, TATIANA – Networked Distruption, Rethinking Oppositions in Art, Hacktivism and the Business of Social Networking, 2013, ISBN: 87-91810-24-8

BEY, Hakim. T.A.Z.: the temporary autonomous zone, ontological anarchy, poetic terrorism. Brooklyn, NY: Autonomedia, 1991. ISBN 0936756764.

CÍSAŘ, Ondřej. Politický aktivismus v České republice: sociální hnutí a občanská společnost v období transformace a evropeizace. Brno : Centrum pro studium demokracie a kultury, 2008. 187 s. ISBN 978-80-7325-168-0.

DREYFUS, Suelette. a Julian. ASSANGE. Underground: tales of hacking, madness, and obsession on the electronic frontier. Kew, Australia: Mandarin, 1997. ISBN 1863305955.

GIBSON, William. Neuromancer. New York: Ace Books, 1984. ISBN 0-441-56959-5.

JORDAN, TIM & TAYLOR, PAUL A. - Hacktivism and Cyberwars, Rebels with a cause?, Routlege, 2004, ISBN 0-203-49003-7

LEVY, STEVEN – Hackers, Heroes of the Computer Revolution, ISBN: 0-385-31210-5, 1994

MANOVICH, Lev. The language of new media. Cambridge, Mass.: MIT Press, 2000. Leonardo. ISBN 0-262-13374-1.

MCLUHAN, Marshall. Understanding media: the extensions of man. 8. print. New York: New American Library, 1964. Signet Books.

BOURRIAUD, Nicolas. Postprodukce: kultura jako scénář: jak umění nově programuje současný svět. Praha: Tranzit, 2004. Navigace. ISBN 80-903452-0-4.

REJZEK, Jiří. Český etymologický slovník. Třetí vydání (druhé přepracované a rozšířené vydání). Praha: Leda, 2015. ISBN 978-80-7335-393-3.

STERLING, Bruce. The hacker crackdown: law and disorder on the electronic frontier. New York: Bantam Books, 1992. ISBN 055308058X.

WARK, McKenzie. A hacker manifesto. Cambridge, MA: Harvard University Press, 2004.

Obrazová příloha

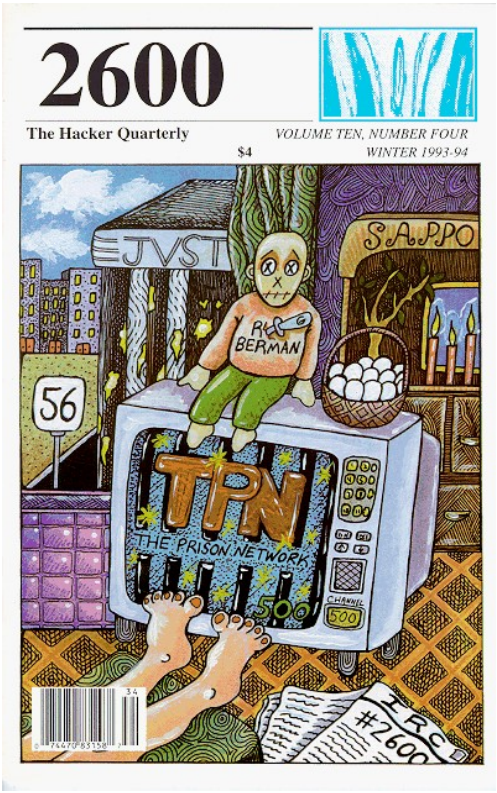
Obr. 2: Vůdce ludditů

Obr. 1: Dennis Ritchie a Ken Thompson

OSI (Open Source Interconnection) 7 Layer Model

Layer	Application/Example		Central Device/ Protocols			DOD4 Model
Application (7) Serves as the window for users and application processes to access the network services.	**End User layer** Program that opens what was sent or creates what is to be sent. Resource sharing • Remote file access • Remote printer access • Directory services • Network management		**User Applications** SMTP	GATEWAY Can be used on all layers		Process
Presentation (6) Formats the data to be presented to the Application layer. It can be viewed as the "Translator" for the network.	**Syntax layer** encrypt & decrypt (if needed). Character code translation • Data conversion • Data compression • Data encryption • **Character Set Translation**		JPEG/ASCII EBDIC/TIFF/GIF PICT			
Session (5) Allows session establishment between processes running on different stations.	**Synch & send to ports** (logical ports). Session establishment, maintenance and termination • Session support - perform security, name recognition, logging, etc.		**Logical Ports** RPC/SQL/NFS NetBIOS names			
Transport (4) Ensures that messages are delivered error-free, in sequence, and with no losses or duplications.	**TCP** Host to Host, Flow Control. Message segmentation • Message acknowledgement • Message traffic control • Session multiplexing	PACKET FILTERING	TCP/SPX/UDP			Host to Host
Network (3) Controls the operations of the subnet, deciding which physical path the data takes.	**Packets** ("letter", contains IP address). Routing • Subnet traffic control • Frame fragmentation • Logical-physical address mapping • Subnet usage accounting		**Routers** IP/IPX/ICMP			Internet
Data Link (2) Provides error-free transfer of data frames from one node to another over the Physical layer.	**Frames** ("envelopes", contains MAC address) [NIC card — Switch — NIC card] (end to end). Establishes & terminates the logical link between nodes • Frame traffic control • Frame sequencing • Frame acknowledgment • Frame delimiting • Frame error checking • Media access control		**Switch Bridge WAP** PPP/SLIP	Land Based Layers		Network
Physical (1) Concerned with the transmission and reception of the unstructured raw bit stream over the physical medium.	**Physical structure** Cables, hubs, etc. Data Encoding • Physical medium attachment • Transmission technique - Baseband or Broadband • Physical medium transmission Bits & Volts		**Hub**			

Obr. 4: Zachycuje vrstvení jednotlivých protokolů na sebe a jejich vzájemný vztah.



Obr. 3: Obálka časopisu 2600, hackerského čtvrtletníku založeného v druhé polovině 80. let.

Obr. 6: BTX terminál

Obr. 7: Stills ze hry a výsledné skóre vyjádřeno v západoněmeckých markách.

```
sh-4.3$ curl -kvvv http://nix.cz
* Rebuilt URL to: http://nix.cz/
*   Trying 195.47.235.3...
* Connected to nix.cz (195.47.235.3) port 80 (#0)
> GET / HTTP/1.1
> Host: nix.cz
> User-Agent: curl/7.47.1
> Accept: */*
>
< HTTP/1.1 301 Moved Permanently
< Date: Sat, 27 Aug 2016 23:22:44 GMT
< Server: Apache
< Location: https://www.nix.cz/
< Content-Length: 283
< Content-Type: text/html; charset=iso-8859-1
<
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>301 Moved Permanently</title>
</head><body>
<h1>Moved Permanently</h1>
<p>The document has moved <a href="https://www.nix.cz/">here</a>.</p>
<hr>
<address>Apache Server at nix.cz Port 80</address>
</body></html>
* Connection #0 to host nix.cz left intact
sh-4.3$
```

Obr. 5: Výpis požadavku na WWW stránku pomocí protokolu HTTP a výsledná odpoveď.

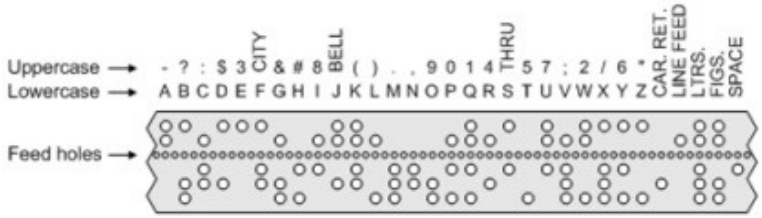
```
sh-4.3$ ssh sdf.org
Welcome to the SDF Public Access UNIX system, (est. 1987)

For quick help, type 'help'
For detailed questions and answers, type 'faq'
For user discussion boards and software requests, type 'bboard'
For interactive discussions, type 'com'
To setup your homepage, type 'mkhomepg'
to create your URL http://lsde.freeshell.org, type 'mkhomepg -a'

Explore and Enjoy!

$ ls -lsha
total 1.5M
4.0K drwx------     4 lsde  users  512B Aug 27 23:39 .
 28K drwxr-xr-x  1489 new   wheel   28K Aug 27 15:36 ..
4.0K -rw-------     1 lsde  users   12B Jul 14 23:01 .bash_history
 12K -rw-r--r--     1 lsde  users  8.1K Jul 10 15:02 .history
   0B -rw-------     1 lsde  users    0B Aug 27 23:32 .hushlogin
4.0K -rw-r--r--     1 lsde  users  2.8K Jul 10 16:48 .profile
4.0K -rw-------     1 lsde  users   60B Jul 10 14:09 .signature
4.0K drwx------     2 lsde  users  512B Jul 14 23:06 .ssh
4.0K drwx------     2 lsde  users  512B Jul 14 23:16 Mail
1.5M -rw-r--r--     1 lsde  users  1.5M Jul 16 18:17 irssi-0.8.19.tar.gz
$
$ Connection to sdf.org closed.
sh-4.3$
```

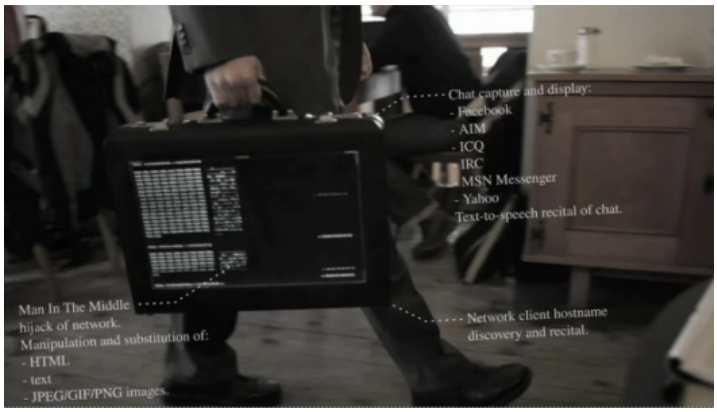
Obr. 8: Výpis komunikace při připojení pomocí protokolu SSH a následné vypsání obsahu vzdáleného adresáře.



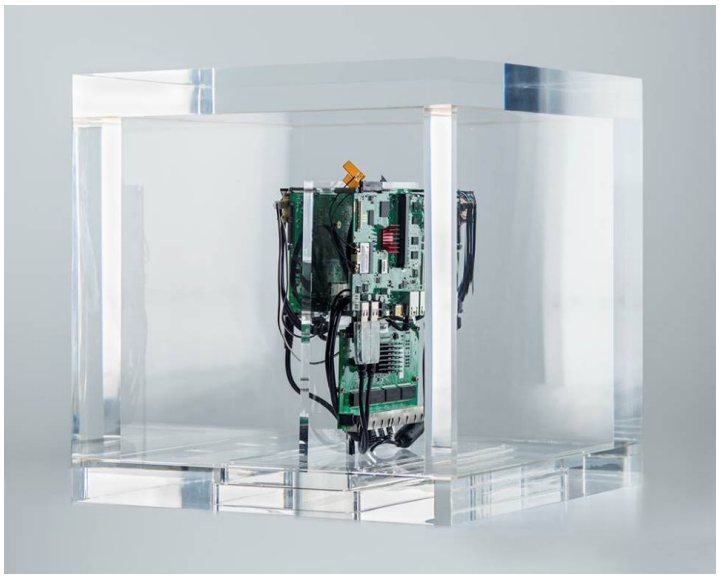
Obr. 9: Schéma kódování informací do děrné pásky

Obr. 10: Příklad cíleného útoku na obět pomocí nástroje Metasploit.

Obr. 11: bienale.py jako objekt v instalaci.



Obr. 12: Kufřík z performance Men in Grey

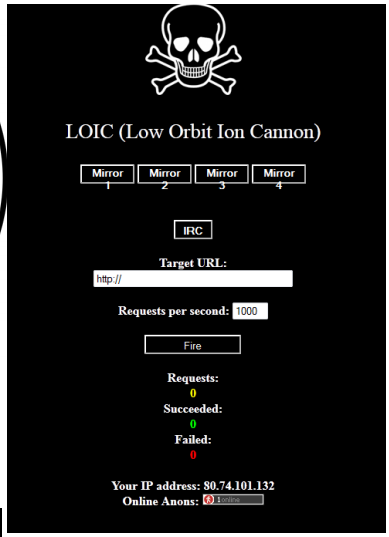


Obr. 13: Autonomy Cube

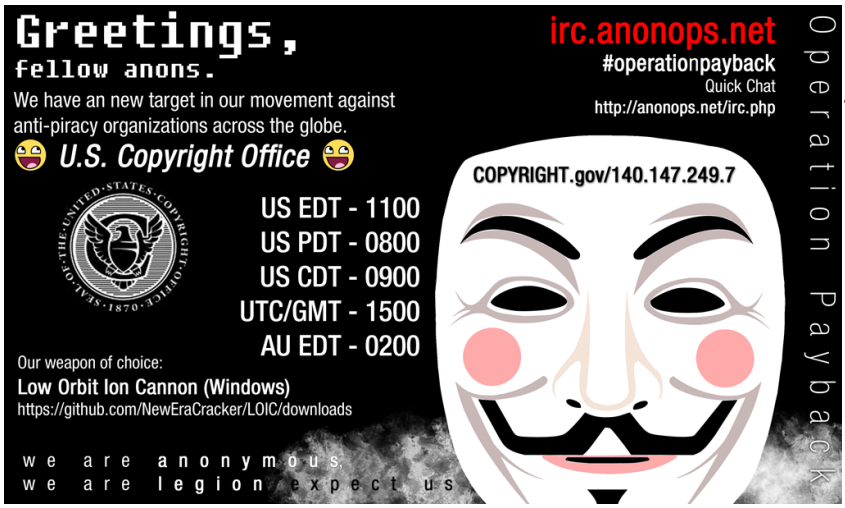
Obr. 14: Listy z prezentace NSA programu QUANTUMSQUIRREL

Obr. 17: List z prezentace NSA programu QUANTUMSQUIRREL

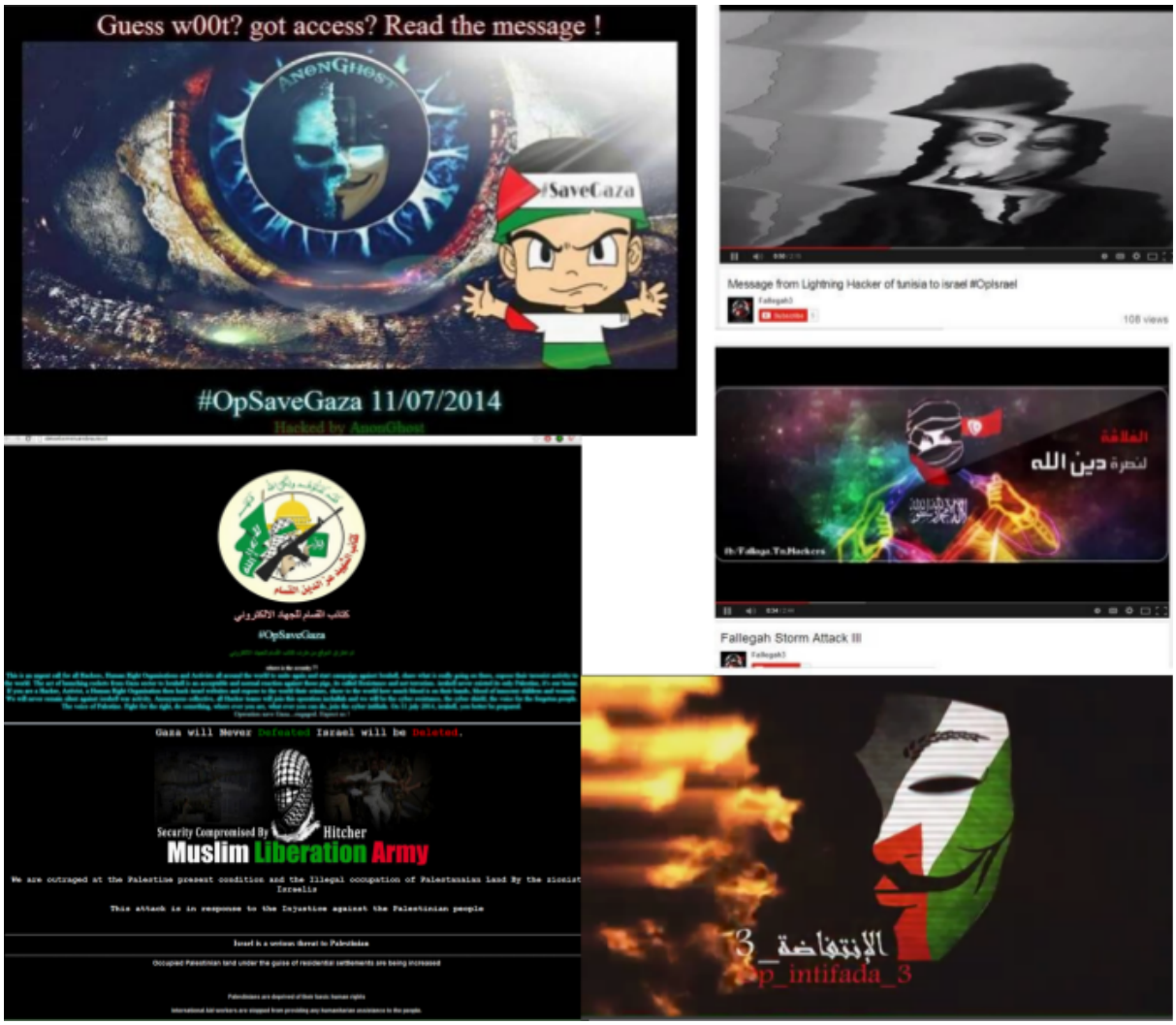
Obr. 15: Logo uskupení Anonymous



Obr. 16: Nástroj LOIC pro jednoduché zapojení do DDoS útoku.



Obr. 18: Banner Anonymous který zve do zapojení do akce.



Obr. 19: Příklady intervencí pod hlavičkou Electronic Intifada