
Bruce Sterling
Zátah
na
hackery

Napsal: Bruce Sterling, <bruces@well.sf.ca.us>
Přeložil: Václav Bárta, 2:423/59.1
Upravil: Martin Hinner, <mhi@penguin.cz>

Toto je výtah překladu knihy Bruce Sterlinga "The Hacker Crackdown" z časopisu Natura (12/1995 - 07/1996).
Originál překladu najdete na adrese: http://www.penguin.cz/~mhi/crackdown/

Vydáno jako knižní příloha ZX Magazínu.
Ke stažení na adrese: http://zxm.speccy.cz

Literární freeware

Bruce Sterling

Zátah na hackery

Hackers manifesto

Another one got caught today, it's all over the papers. "Teenager Arrested in Computer Crime Scandal", "Hacker Arrested after Bank Tampering"... Damn kids.

They're all alike.

But did you, in your three-piece psychology and 1950's technobrain, ever take a look behind the eyes of the hacker? Did you ever wonder what made him tick, what forces shaped him, what may have molded him? I am a hacker, enter my world... Mine is a world that begins with school... I'm smarter than most of the other kids, this crap they teach us bores me... Damn underachiever.

They're all alike.

I'm in junior high or high school. I've listened to teachers explain for the fifteenth time how to reduce a fraction. I understand it. "No, Ms. Smith, I didn't show my work. I did it in my head..." Damn kid. Probably copied it.

They're all alike.

I made a discovery today. I found a computer. Wait a second, this is cool. It does what I want it to. If it makes a mistake, it's because I screwed it up. Not because it doesn't like me... Or feels threatened by me... Or thinks I'm a smart ass... Or doesn't like teaching and shouldn't be here... Damn kid. All he does is play games.

They're all alike.

And then it happened... a door opened to a world... rushing through the phone line like heroin through an addict's veins, an electronic pulse is sent out, a refuge from the day-to-day incompetencies is sought... a board is found. "This is it... this is where I belong..." I know everyone here... even if I've never met them, never talked to them, may never hear from them again... I know you all... Damn kid. Tying up the phone line again.

They're all alike...

You bet your ass we're all alike... we've been spoon-fed baby food at school when we hungered for steak... the bits of meat that you did let slip through were pre-chewed and tasteless. We've been dominated by sadists, or ignored by the apathetic. The few that had something to teach found us willing pupils, but those few are like drops of water in the desert. This is our world now... the world of the electron and the switch, the beauty of the baud. We make use of a service already existing without paying for what could be dirt-cheap if it wasn't run by profiteering gluttons, and you call us criminals. We explore... and you call us criminals. We seek after knowledge... and you call us criminals. We exist without skin color, without nationality, without religious bias... and you call us criminals. You build atomic bombs, you wage wars, you murder, cheat, and lie to us and try to make us believe it's for our own good, yet we're the criminals. Yes, I am a criminal. My crime is that of curiosity. My crime is that of judging people by what they say and think, not what they look like. My crime is that of outsmarting you, something that you will never forgive me for. I am a hacker, and this is my manifesto. You may stop this individual, but you can't stop us all...

After all, we're all alike.

+++The Mentor+++

Obsah

Úvod

Toto je kniha o policajtech, o divokých zázračných dětech, o advokátech, o anarchistech s krhavýma očima, o technicích, o hippies, o milionářích podnikajících s moderními technologiemi, o náruživých hráčích, o odbornících na počítačovou bezpečnost, o agentech Tajné služby USA, o podvodnících a zlodějích. Je to kniha o elektronickém pohraničí 90. let. Zabývá se činnostmi, které se odehrávají v počítačích a na telefonních linkách.

Jistý sci-fi spisovatel vytvořil užitečný termín "cyberspace" v roce 1982. Ale území, které toto slovo popisuje, "elektronické pohraničí", je staré asi sto třicet let. Cyberspace je "místo", kde se odehrává telefonní rozhovor. Ne ve vašem telefonním přístroji na vašem psacím stole. Ne v telefonu vašeho partnera v nějakém jiném městě. *Mezi* telefony. Tam, kde se vy dva, dvě lidské bytosti, setkáváte a komunikujete.

I když přísně vzato není "reálný", má cyberspace mnohé atributy "území". Dějí se v něm věci, které mají velmi reálné následky. Není "skutečný", ale žádá si vážnou pozornost. Desetitisíce lidí v něm nalezly životní náplň - rozvíjení veřejných komunikačních služeb po drátě a s pomocí elektroniky.

Generace lidí pracovaly v tomto elektronickém "pohraničí". Některým přinesla jejich snaha na tomto území bohatství a slávu. Někteří si tam jen hráli. Jiní o něm hluboce přemýšleli, psali o něm, regulovali jej, jednali o něm na mezinárodních fórech, soudili se o něj v ohromných, léta trvajících soudních bitvách. A téměř od začátku se našli lidé, kteří v něm páchali zločiny.

Ale v posledních dvaceti letech se tento elektronický "prostor", kdysi těsný, tmavý a jednodimenzionální - ne o moc víc než ozvučná trubka od jednoho telefonu k druhému - rozevřel jako gigantický teleskop. A zaplavilo ho světlo; kouzelné světlo zářící počítačové obrazovky. Temné elektrické zásvětí se změnilo v kvetoucí elektronickou krajinu. Od šedesátých let se svět telefonů kříží s počítači a televizí, a ačkoliv cyberspace stále nemá žádnou "substanci", nic, co by se dalo uchopit, získal podivný druh fyzické existence. Dnes má smysl mluvit o cyberspace jako o samostatném prostoru.

Protože dnes v něm žijí lidé. Nejen pár jednotlivců, pár techniků a podivínů, ale tisíce docela obyčejných lidí. A nejen na chvíli, ale v několikahodinových směnách, pravidelně po celé týdny, měsíce a roky. Dnešní cyberspace je "Síť", "Vzor" mezinárodního rozsahu a stále rostoucí. Roste jeho velikost, bohatství i politická důležitost.

Lidé dělají kariéry v moderním cyberspace. Vědci a technici, samozřejmě; ti se v něm pohybují už dvacet let. Ale cyberspace se stále více zalidňuje novináři, lékaři, právníky, umělci, úředníky. Státní zaměstnanci dělají kariéru "on-line" v ohromných státních databankách; a také špióni - průmysloví, političtí i docela obyčejní šťouralové; a také policisté, přinejmenším někteří. A děti si tam hrají.

Jsou lidé, kteří se tam seznámili a uzavřeli sňatek. V cyberspace nyní žijí celé komunity: povídají si, pomlouvají, plánují, radí se a kují pikle, posílají si mluvené vzkazy a elektronickou poštu a vyměňují si abstraktní hromady cenných dat, získaných legálně či ilegálně. Pilně si posílají software, někdy s číhajícím počítačovým virem.

Dosud nám není úplně jasné, jak vlastně žít v cyberspace. Hledáme cestu a ztrácíme se. Na tom není nic divného. Naše životy ve fyzickém, "reálném" světě také nejsou dokonalé, byť v něm máme mnohem víc zkušeností. Lidské životy jsou ze samé své podstaty nedokonalé, a v cyberspace žijí lidé.

Život v cyberspace je křivým zrcadlem života v reálném světě. Jak své silné stránky, tak své problémy si tam bereme sebou.

Tato kniha je o problémech v cyberspace. Konkrétně je o jistých podivných událostech v roce 1990, který se stal bezprecedentním překvapením pro celý rostoucí svět počítačové komunikace.

V roce 1990 byl uskutečněn celoamerický zátah na hackery vyvíjející nezákonnou činnost, včetně zatčení, obvinění z kriminálních činů, jednoho dramatického procesu, několika přiznání viny a velkých konfiskací dat a vybavení po celých USA.

Zátah na hackery v roce 1990 byl větší, organizovanější, promyšlenější a odhodlanější než všechny předchozí snahy přivést zákon do nového světa počítačového zločinu. Tajná služba USA, bezpečnostní oddělení soukromých telefonních společností a policejní složky na federální i místní úrovni spojily své síly v rozhodné snaze zlomit páteř amerického počítačového undergroundu. Byl to fascinující pokus s velmi rozpornými výsledky.

Zátah na hackery měl i jeden neočekávaný efekt; přivedl příznivce "počítačové komunity" k založení Electronic Frontier Foundation ("Nadace elektronického pohraničí"), nové a velmi podivné zájmové skupiny, nekompromisně prosazující ustanovení a ochranu elektronických občanských práv. Zátah, sám o sobě pozoruhodný, vyprovokoval živou debatu o elektronickém zločinu a trestu, svobodě tisku, domovních prohlídkách a konfiskacích. Do cyberspace vstoupila politika. Politika následuje lidi všude, kam jdou. A toto je příběh lidí v cyberspace.

Pád systému

Krátká historie telefonu / Bellova alfa verze / Univerzální servis / Divocí chlapci a slečny z ústředny / Elektronické komunity / Nelaskavý gigant / Rozdělení / Strážci systému / Pitva kolapsu / Zemětřesení v cyberspace

15. ledna 1990 se síť AT&T pro dálkové hovory zhroutila. Byla to obrovská, podivná a zlověstná událost. Šedesát tisíc lidí zůstalo bez telefonního spojení. Během devíti hodin, které si vyžádaly pokusy o jeho obnovení, bylo přerušeno přibližně sedmdesát miliónů telefonních hovorů.

Výpadek spojení je pro telecom známým a akceptovaným rizikem. Oblast je zasažena hurikánem a tisíce telefonních drátů jsou přerušeny. Zemětřesení roztrhá podzemní optické kabely. Telefonní ústředna je zachvácena požárem a shoří do základů. To se stává. Pro tyto případy jsou připraveny nouzové plány, uplatňované a vylepšované už desítky let. Ale kolaps z patnáctého ledna byl bezprecedentní. Byl neuvěřitelně velký a objevil se bez zjevného fyzikálního důvodu.

Počátek kolapsu nastal v pondělí odpoledne v jediné ústředně na Manhattanu. Ale odtud se na rozdíl od živelných pohrom šířil dál a dál. V řetězové reakci se hroutila jedna ústředna za druhou, až zkolabovala polovina sítě AT&T a druhá byla těžce přetížena snahou nahradit nefunkční linky.

V devíti hodinách softwaroví inženýři z AT&T víceméně pochopili příčinu kolapsu. Po několika týdnech důkladného prohlížení softwaru ji byli schopni přesně rekonstruovat. Ale protože byla technicky komplikovaná a obtížně vysvětlitelná, nebyla tato příčina ani její možné důsledky široce publikovány. Zůstala tajemná, obklopená nezaručenými pověstmi a strachem. Pro management AT&T byl kolaps zahanbující. Jeho "viníkem" byla chyba v softwaru společnosti - nic, co by se telekomunikačnímu gigantovi chtělo přiznat, zejména ne tváří v tvář rostoucí konkurenci. Nicméně pravda *byla* zveřejněna - v nesrozumitelných technických termínech, které ji dokázaly popsat.

Ale toto vysvětlení nepřesvědčilo americké strážce pořádku a dokonce ani bezpečnostní odborníky telefonních společností. Tito lidé nebyli techničtí specialisté ani softwaroví kouzelníci a měli své vlastní teorie o příčině katastrofy.

Policie a bezpečnostní experti měli důležité zdroje informací, nedostupné obyčejným softwarovým inženýrům. Měli informátory v počítačovém undergroundu a léta zkušeností se zneužíváním moderních technologií, jehož rafinovanost byla stále hrozivější. Léta očekávali přímý, zlovolný útok proti americkému telefonnímu systému. A kolaps z 15. ledna - v prvním měsíci nové, opět "technologičtější" dekády - byl pro ně manifestací jejich předpovědí, obav a podezření v reálném světě. Ve světě, v němž se telefonní systém ne pouze zhroutil, ale byl nejspíš *shozen* - zničen "hackery".

Kolaps vytvořil velký, temný mrak podezření, ovlivňující myšlenky a činy některých lidí po celé měsíce. To, že se jednalo o poruchu softwaru, bylo na první pohled podezřelé. To, že k ní došlo v den výročí smrti Martina Luthera Kinga, jež je stále politicky nejcitlivějším americkým svátkem, ji činilo ještě podezřelejší.

Kolaps z 15. ledna dal Zátahu na hackery jeho rozhodnost a neodkladnou naléhavost. Přesvědčil veřejné činitele s důležitými pravomocemi, že situace je kritická. A co bylo nejhorší, povzbudil vyšetřovatele k mimořádným opatřením a přísnému utajení. Komplikovaná softwarová chyba stárnoucí telefonní ústředny v New Yorku spustila řetězovou reakci policie a soudního systému po celé zemi.

Stejně jako kolaps telefonní sítě, i tato reakce byla na spadnutí. Během 80. let byly v americkém právním systému provedeny rozsáhlé změny, umožňující postih nových počítačových zločinů. Například v roce 1986 byl přijat Zákon o soukromí v elektronické komunikaci (jedním prominentním policejním úředníkem výmluvně popsaný jako "smradlavý chuchvalec"). A také drakonický Zákon o počítačové zpronevěře a zneužití počítače, jednohlasně přijatý Senátem, ve kterém byla později objevena řada nedostatků. Byl vykonán velký a dobře míněný kus práce na udržení zákonů na výši doby. Ale v každodenním provozu reálného světa má i ten nejelegantnější software sklon k překvapivým projevům svých skrytých chyb.

Stejně jako jeden kolaps nezlikvidoval telefonní síť, nebyl ani americký právní řád zničen svou dočasnou ztrátou stability; ale život těch, kteří se dostali pod trosky hroutícího se systému, se stal sérií výpadků a nepříjemných překvapení.

K porozumění těmto podivným událostem, jak z technologického, tak z právního hlediska, nestačí chápat pouze technické okolnosti. I k těm se dostaneme; ale ze všeho nejdříve musíme zkusit pochopit princip telefonu, postavení telefonní společnosti a život komunity lidí kolem telefonů.

Technologie se vyvíjejí v životních cyklech, stejně jako města, instituce, zákony a vlády.

Prvním stadiem každé technologie je Velký otazník, u softwaru známý jako alfa verze. V této fázi je technologie čirý fantóm, pouhý záblesk v oku vynálezce. Jedním takovým vynálezcem byl logoped a tvůrce elektrických hraček Alexander Graham Bell. [...]

Když Bellova výhradní práva vypršela, konkurenční telefonní společnosti zahájily činnost po celé Americe. Vynálezcova společnost, American Bell Telephone, se brzo dostala do vážných potíží a v roce 1907 byla převzata finančním kartelem nechvalně známého J. P. Morgana, skupinou spekulantů ovládající Wall Street.

Od tohoto okamžiku se historie mohla vyvíjet různými cestami. Telefonní spojení v Americe mohlo být nadále zajišťováno mozaikou místních společností. Mnoho komunálních politiků a drobných podnikatelů to pokládalo za dokonalé řešení.

Ale noví majitelé, společnost American Telephone and Telegraph neboli AT&T, pověřili vedením nového muže, vizionářského manažera jménem Theodore Vail. Vail, bývalý ředitel poštovní služby, rozuměl velkým organizacím a měl vrozený cit pro komunikaci ve velkém měřítku. Postaral se o to, aby AT&T opět získala technologickou převahu. "Plné vinutí" Pupina a Campbella a deForestův "audion" jsou dnes mrtvé technologie, ale v roce 1913 daly Vailově společnosti nejlepší dálkové linky na světě. Jejich kontrola - kontrola spojení mezi, přes a nad místními společnostmi - dala AT&T nástroj k jejich oslabení a postupnému ovládnutí.

Vail reinvestoval zisky zpět do výzkumu a vývoje a založil v AT&T tradici podpory průmyslového výzkumu velkého rozsahu a s vynikajícími výsledky. Technicky i finančně AT&T postupně převálcovala své konkurenty. Nezávislé telefonní společnosti nezanikly úplně a stovky jich prosperují dodnes. Ale Vailova AT&T se stala vládnoucí telefonní společností. Svého času koupila i Western Union, tutéž společnost, která

odmítla Bellův telefon jako "hračku". Vail důkladně zreformoval zkostnatělou organizaci Western Unionu podle svých moderních zásad; ale když federální vláda projevila zneklidnění nad koncentrací spojových organizací v jeho rukou, zdvořile se Western Unionu vzdal.

Tato centralizace nebyla nijak jedinečná. Velice podobné procesy proběhly v ocelářství, železnicích a naftovém průmyslu. Ale AT&T si, na rozdíl od jiných velkých společností, zachovala svoji moc. Monopolisté v jiných oblastech byli omezeni a nakonec zlikvidováni vládními antitrustovými opatřeními. Vail, bývalý státní zaměstnanec, ochotně vyhověl požadavkům federální vlády; ve skutečnosti s ní zformoval aktivní spojenectví. AT&T se stala téměř státní organizací, téměř další poštou - ale ne tak docela. AT&T se ochotně podrobovala federální regulaci, ale současně používala federální úředníky jako svou vlastní policii, ztěžující život konkurenci a zajišťující AT&T výsadní postavení a monopolní zisky.

Prosazení jednotného amerického telefonního systému bylo stejně důležitou událostí jako samotný vynález telefonu. Vailovo uspořádání úspěšně fungovalo mnoho desetiletí, až do roku 1982. Jeho systém jakéhosi amerického průmyslového socialismu vznikl zhruba ve stejné době jako Leninův komunismus a existoval téměř stejně dlouho - a, nutno zdůraznit, s mnohem lepšími výsledky.

Vailova strategie byla úspěšná. Neexistovala technologie, možná s výjimkou kosmonautiky, ve které by Američané dominovali tak výrazně jako v telekomunikacích. Telefon byl od samého počátku vnímán jako typicky americká technologie. Bellova politika, stejně jako politika Theodora Vaila, by se dala shrnout do hluboce demokratického principu *univerzálního přístupu*. Vailův slavný reklamní slogan "Jedna strategie, jeden systém, univerzální služby" byl politickým heslem, heslem ve velice americkém stylu. Americká telefonní síť nebyla budována jako specializovaný nástroj vlády či byznysu, ale jako služba pro širokou veřejnost. Pravda, soukromé telefony si zpočátku mohli dovolit jen bohatí a Bellova společnost se orientovala hlavně na obchodní kruhy. Rozvoj telefonní sítě byl obchodní podnik a jeho cílem bylo vydělávání peněz, nikoli dobročinnost. Ale od samého počátku byly součástí téměř každé místní telefonní sítě veřejné přístroje. A mnoho obchodů - zvláště koloniály - nabízelo své telefony k veřejnému použití. I když jste neměli svůj vlastní telefon, mohli jste se dostat do telefonní sítě, pokud jste to opravdu potřebovali.

Rozhodnutí učinit telefony "veřejné" a "univerzální" nebylo nijak nevyhnutelné. Vailův systém vyžadoval zásadní důvěru k široké veřejnosti. Jeho přijetí bylo politickým aktem, inspirovaným základními hodnotami americké demokracie. Telefonní systém mohl být úplně jiný; a v jiných zemích s jinými tradicemi také jiný byl.

J. V. Stalin, například, vetoval plány na vybudování sovětské telefonní sítě krátce po Říjnové revoluci. Byl přesvědčen, že veřejně přístupné telefony by se staly nástroji antikomunistické konspirace a kontrarevoluce. (Pravděpodobně se nemýlil.) Když byly telefony v Sovětském svazu nakonec zavedeny, byly chápány jako nástroje stranické hierarchie a rutinně odposlouchávány. Novela Alexandra Solženicyna Kruh první popisuje snahy o vývoj telefonního systému vhodného pro stalinistické cíle.

Francie, se svou tradicí osvícené centrální vlády, se ostře stavěla i proti elektrickému telegrafu, který Francouzi považovali za anarchistický a frivolní. Francie 19. století po desetiletí komunikovala pomocí "telegrafních semaforů", státem vlastněného systému vysokých kamenných věží postavených na kopcích po celé zemi, které si předávaly zprávy pohyby velkých dřevěných ramen, podobných lopatkám větrného mlýna. V roce 1846 zformuloval jistý Dr. Barbay, oddaný stoupenec tohoto systému, jednu z prvních verzí toho, co by se dalo nazvat "argumentem bezpečnostního experta" proti otevřeným komunikacím.

"Ne, elektrický telegraf není rozumný vynález. Je a vždy bude vydán na milost a nemilost ztrátě spojení, divokým mladíkům, opilcům, vandalům a podobně. Elektrický telegraf odkrývá těmto destruktivním elementům jen několik metrů drátu, jež není možno střežit. Jediný muž může nepozorovaně strhnout telegrafní dráty vedoucí do Paříže a v průběhu jediného dne přerušit tutéž linku na deseti místech, aniž by byl chycen při činu. Na druhé straně telegrafní semafor má věž, vysoké zdi a bránu chráněnou zevnitř silnými ozbrojenými muži. Tvrdím, že nahrazení telegrafních semaforů elektrickým telegrafem je hrozivé opatření a akt neuvěřitelného idiotismu."

Dr. Barbay a jeho vysoce bezpečné kamenné sítě byly nakonec překonány, ale jeho argumentace - že komunikace existují pro bezpečnost a blaho státu a musí být pečlivě chráněny před nepřátelskou lůzou a nezodpovědnými mladíky, kteří by se mohli pokusit o jejich narušení - je opakována znovu a znovu.

Když konečně vznikla francouzská telefonní síť, stala se brzy pověstnou svou komplikovaností a neadekvátností. Příznivci Bellovy telefonní společnosti často doporučovali skeptikům výlet do Francie.

V edwardiánské Anglii byl rozvoj telefonizace spoután tradicemi výlučnosti a soukromí vyšší společnosti. Bylo považováno za urážku, že kdokoli - každý divoký hlupák z ulice - může s křikem vrazit do cizí kanceláře či domu a svůj příchod ohlásit pouhým zazvoněním. V Anglii byly telefony tolerovány pro obchodní účely, ale soukromé přístroje byly vytlačovány do komor, kuřáren či pokojů pro služebnictvo. Telefonní operátoři byli považováni za nevychovance, kteří nevědí, kde je jejich místo. A nikdo z dobré rodiny by si na svou vizitku nedal vytisknout telefonní číslo; bylo by to pociťováno jako neotesaný pokus o navazování důvěrných vztahů s cizinci.

Na druhé straně v Americe se přístup k telefonu stal právem každého občana, právem podobným volebnímu, pouze všeobecnějším. V dobách počátků telefonního spojení americké ženy ještě nemohly volit, ale již tehdy mohly a chtěly telefonovat. Cizinci často komentovali tuto "feminizaci" americké telefonní sítě. Telefony v Americe nikdy nebyly cenzurovány, nebyly upjaté a formální; byly společenské, osobní, soukromé a domácké. Zdaleka nejrušnějším dnem roku pro telefonní síť je v Americe Svátek matek. [...]

Koncem roku 1988 a po celý rok 1989 si představitelé telecomu stále hlasitěji stěžovali těm několika mužům zákona, kteří se snaží porozumět problémům lidí od telefonů. Bezpečnostní experti telefonních společností objevili počítačový underground, infiltrovali ho a byli zděšeni jeho rostoucími odbornými znalostmi. Objevili struktury, které byly nejen na první pohled odpudivé, ale také snadným terčem protiútoku.

Nesmiřitelní rivalové AT&T, MCI a Sprint a řada následnických společností Bellu - PacBell, Bell South, Southwestern Bell, NYNEX, USWest, stejně jako výzkumné konsorcium Bellcore a nezávislá společnost Mid-American - ti všichni se zúčastnili Zátahu na hackery. Po letech pasivity a porážek převzaly telefonní společnosti opět iniciativu, byť v malém měřítku. Po letech zmatků měli jejich představitelé opět hladce a úspěšně spolupracovat s vládními úředníky při obraně systému. Optimismus stoupal, všude vládlo nadšení. Očekávaná pomsta byla sladká.

Od samého počátku - ještě dříve, než padlo rozhodnutí o celostátní akci - bylo velkým problémem utajení. Pro konspirativní přípravu zátahu na hackery mluvilo mnoho důvodů. Hackeři a zloději přístupových práv byli mazaní protivníci, připravení stáhnout se do svých ložnic a sklepů a zničit důležité důkazy při první známce nebezpečí. Navíc jejich trestná činnost byla vysoce technická a obtížně popsatelná. Bylo těžké vysvětlit ji i policii, natož široké veřejnosti.

Zkušenosti dokonce ukazovaly, že srozumitelné seznámení veřejnosti s "telefonní" trestnou činností vede k jejímu dramatickému *zvýšení*. Spojaři si byli vědomi zranitelnosti svých sítí a velice jim záleželo na tom, aby nebyla propagována jejich slabá místa. Věděli, že jakmile se povědomí o těchto slabých místech rozšíří, zneužijí je bez váhání desetitisíce lidí - nejen profesionální podvodníci a undergroundoví hackeři a telefandové, ale i obyčejní, zákona víceméně dbalí občané, kteří považují krádež služeb beztvaré, bezduché telefonní společnosti za neškodnou domácí zábavu. Při ochraně zájmů telekomunikačních společností přestali jejich pracovníci už dávno spoléhat na sympatie veřejnosti k "Hlasu s úsměvem". "Hlas" se stal hlasem počítače, a Američané projevovali telecomu mnohem menší než náležitý respekt a

vděčnost za jeho nepostradatelné služby veřejnosti než za časů pánů Bella a Vaila. Jak se telekomunikační společnosti stávaly efektivnějšími, modernějšími, automatizovanějšími a neosobnějšími, v přístupu k nim se prosazoval mrzoutský kriticismus a amorální hamižnost.

Představitelé telecomu chtěli potrestat undergroundové telefandy co nejveřejněji, exemplárním způsobem. Chtěli udělat odstrašující příklady z největších provinilců, chtěli pozatýkat vůdce a zastrašit malé ryby, chtěli vyděsit amatérské hříšníky a dostat profesionální podvodníky za mříže. Pro takovou akci byla publicita nezbytná.

Ale utajení celé operace také. Kdyby se prozradilo, že se chystá celostátní zátah, hackeři mohli prostě zmizet; zničit důkazy, schovat počítače, zalézt a počkat, až se kampaň přežene. I nezletilí hackeři byli chytří a podezíraví a profesionální podvodníci mizeli za hranicemi státu při prvním náznaku potíží. Aby byl zátah úspěšný, museli být přistiženi s rukou v cizí kapse, překvapeni masivním útokem z čistého nebe. Utajení mělo i jiné motivy. V nejhorší variantě scénáře mohlo prozrazení kampaně vést k ničivému protiútoku hackerů proti telecomu. Pokud v Americe opravdu operovali hackeři, kteří způsobili kolaps z 15. ledna - opravdu schopní hackeři ovládající ústředny dálkových spojů, rozzuření nebo vyděšení zátahem proti nim - pokus o jejich zkrocení by mohl mít nepředvídatelné následky. A i kdyby byli chyceni, jejich talentovaní a pomstychtiví přátelé by mohli zůstat na svobodě. Takže konfrontace by mohla zajít daleko. Velice daleko. Bylo těžké si představit, kam až by v takovém případě mohla dospět. Pracovníci telekomunikací brali možnost hackerského protiútoku vážně. Ve skutečnosti se žádného takového protiútoku nikdy nedočkali. Ale v celém průběhu kampaně na tuto hrozbu systematicky upozorňovali a pronášeli ponurá varování.

Nicméně toto riziko bylo nutno přijmout. Lépe riskovat pomstychtivé útoky, než být vydán na milost a nemilost potenciálním ničitelům systému. Každý policajt vám řekne, že platit vyděračům za "ochranu" nemá budoucnost.

Jenže publicita byla tak užitečná. Bezpečnostní odborníci velkých společností, včetně telefonních, zpravidla pracují velice diskrétně. Nevydělávají svým zaměstnavatelům peníze. Jejich úkolem je *zabránit ztrátám*, což zdaleka není tak fotogenické jako přinést zisk. Když jste bezpečnostní odborník a odvádíte dokonalou práci, nemá vaše společnost žádné problémy s bezpečností. Takže se zdá, že jste úplně zbytečný. To je jeden z mnoha nelákavých aspektů práce na ochraně nějakého systému. Je vzácné, když mají bezpečnostní experti příležitost předvést svou práci veřejnosti.

Publicita byla výhodná i pro zainteresované policejní složky. Důležitost veřejných činitelů, včetně policejních, roste se zájmem a sympatiemi veřejnosti. Na brilantním zvládnutí slavné kauzy může veřejný žalobce udělat kariéru. Každý policista ví, že příznivá publicita vede legislativu ke zvýšení finančních zdrojů a může přinést pochvalu, povýšení nebo přinejmenším uznání a respekt kolegů.

Ale dosáhnout publicity a utajení zároveň je jako sedět na dvou židlích. V průběhu akce, jak ještě uvidíme, způsobil tento nemožný požadavek strůjcům zátahu velké potíže. Zpočátku se zdálo - dokonce to bylo považováno za pravděpodobné - že zátah může úspěšně spojit to nejlepší z obou světů. *Zatčení* hackerů bylo třeba udělat reklamu. Jejich skutečné *přečiny*, technicky obtížně vysvětlitelné a představující bezpečnostní riziko, bylo třeba ponechat decentně zahalené. Propagace se měla zaměřit na *hrozbu*, kterou hackeři představují pro společnost; otázka, jak děsivé zločiny skutečně spáchali, měla být ponechána představivosti publika. Měl být zdůrazněn růst počítačového undergroundu a jeho stále se zvyšující sofistikovanost; samotní hackeři, většinou obrýlení nezletilci z bílých středostavovských rodin, měli zůstat anonymní.

Nezdá se, že by některého bezpečnostního odborníka napadlo, že obvinění hackeři se budou chtít hájit před soudem; že novináři je přivítají jako "nové tváře"; že podnikatelé, kteří zbohatli na moderních technologiích, nabídnou obětem zátahu morální a finanční podporu; že usměvaví advokáti s příručními kufříky se chopí příležitosti k diskusi o ústavních právech. S tím nikdo nepočítal.

A i kdyby tato možnost někoho napadla, pravděpodobně by nijak nezpomalila nelítostný hon na ukradený dokument telefonní společnosti s luzným názvem "Struktura Kontrolního odboru pro rozšířené služby zvláštním službám a významným zákazníkům 911". V následujících kapitolách se budeme věnovat světům policie a počítačového undergroundu a šedé zóně, ve které se stýkají. Ale předtím musíme prozkoumat bitevní pole. Než opustíme svět telecomu, musíme ještě pochopit, co je vlastně telefonní ústředna a jak váš telefon ve skutečnosti pracuje. [...]

Moderní telefonní síť se stala naprosto a nezvratně závislou na softwaru. Kolaps systému z 15. ledna 1990 byl způsoben *vylepšením* tohoto softwaru. Lépe řečeno *pokusem* o jeho vylepšení.

Vlastní, původní problém byl následující. Jeden z telekomunikačních programů byl napsán v jazyce C, který je v této oblasti standardem. V tomto programu byl dlouhý cyklus "do... while". V cyklu "do... while" byla konstrukce "switch". V konstrukci "switch" byla klauzule "if". V klauzuli "if" byl příkaz "break". Příkaz "break" *měl* přerušit klauzuli "if" [spíše cyklus "do... while" - pozn. překl.]. Místo toho přerušil konstrukci "switch".

Toto tedy byla pravá, skutečná příčina toho, že se lidé, kteří 15. ledna 1990 zvedli sluchátko, nemohli dovolat.

Nebo přinejmenším to bylo prvotní, nepostřehnutelné jádro problému v abstraktním cyberspace. A takto se chyba dostala z hájemství programování do reálného světa.

Systém 7, software pro ústřednu 4ESS, tzv. "Obecný software pro centrální ústředny 44E14", byl důkladně testován a považován za velmi stabilní. Do konce roku 1989 bylo osmdesát telefonních ústředen AT&T po celých Spojených státech vybaveno novým softwarem. Na třiceti čtyřech zbývajících byl z opatrnosti ponechán pomalejší a méně výkonný Systém 6, protože odborníci z AT&T se obávali problémů s obsluhou nové, mnohem sofistikovanější sítě Systému 7.

Ústředny se Systémem 7 byly naprogramovány tak, aby se v případě jakýchkoli problémů přepnuly na záložní síť. V polovině prosince 1989 byla do všech ústředen 4ESS dodána úprava tohoto programu, umožňující ještě rychlejší přepnutí a činící tedy Systém 7 mnohem bezpečnější.

Bohužel, tato úprava obsahovala nenápadnou, ale o to nebezpečnější chybu.

V rámci správy sítě musí ústředny monitorovat stav ostatních ústředen - zdali normálně pracují, zda jsou dočasně mimo provoz, jsou-li přetížené a potřebují pomoci a podobně. Nový software se podílel na této kontrole zpracováním stavových zpráv od ostatních ústředen.

Když se ústředna 4ESS dostane do chybového stavu, dokáže se během čtyř až šesti sekund zbavit všech procházejících hovorů, všechno zapomenout a restartovat svůj software. Restartem ústředna zpravidla zlikviduje softwarové problémy, které se během provozu systému vyvinuly. Vzniklé chyby jsou prostě zahozeny. Je to chytrý nápad. Tento automatický restart se nazývá "normální rutina pro zotavení". Protože software AT&T je ve skutečnosti mimořádně stabilní, ústředny se zřídkakdy potřebují "zotavovat"; AT&T byla nicméně vždy hrdá na svoji "realisticky zajištěnou" spolehlivost a popsaná taktika vypadá skutečně neprůstřelně.

Ústředna 4ESS používala svůj nový software k monitorování toho, jak se ostatní ústředny zotavují z chybových stavů. Když restartovaná ústředna obnovila provoz, zaslala jí signál "OK". Přijímající ústředna si udělala poznámku ve své "stavové mapě" a vzala na vědomí, že druhá ústředna je opět v provozu, takže by měla dostat nějaké hovory a začít znovu normálně pracovat.

Bohužel, během doby, ve které ústředna aktualizovala stavovou mapu, se uplatnila chyba v novém softwaru. Způsobila, že ústředna reagovala neočekávaným a zcela chybným způsobem na přicházející normální telefonní hovory. Jestliže - a pouze když - do ústředny přišly dva nové hovory během jediné setiny sekundy, byl malý kousek jejích dat přepsán.

Ale ústředna byla naprogramována tak, aby neustále sledovala možná poškození svých dat. Když si všimla, že její data byla přepsána, re-

startovala se také, aby se zbavila chyby. Poslala ostatním ústřednám signál, aby jí nadále nepřepojovaly žádné hovory. Čtyři až šest sekund se zotavovala. Pak byla zase v pořádku a rozeslala svůj signál "OK, připravena".

Jenže signál "OK, připravena" bylo *právě to, co původně přimělo ústřednu k restartu*. A *všechny* ústředny Systému 7 měly ve svém softwaru stavové mapy tutéž chybu. Jakmile pozastavily normální činnost a začaly si poznamenávat, že restartovaná ústředna je OK, staly se také zranitelnými příchodem dvou telefonních hovorů v jedné setině sekundy.

V pondělí 15. ledna přibližně ve 14.25 se na jedné z ústředen AT&T v New York City objevila drobná technická závada. Proběhla rutina pro zotavení a ústředna vyslala signál "restartuji se" a vzápětí "už jsem OK". Tato optimistická zpráva se rozšířila po celé síti k mnoha dalším ústřednám 4ESS. Většina z nich tuto zprávu bez problémů akceptovala. Měly štěstí a nedostaly dva hovory v jedné setině sekundy. Jejich software pracoval dál - zatím. Ale tři ústředny - v Atlantě, St. Louis a Detroitu - měly smůlu a byly zastiženy s plnýma rukama. Zhroutily se. A za několik okamžiků obnovily provoz. A vyslaly ničivý signál "OK", aktivující softwarovou chybu v dalších ústřednách.

Čím více ústředen mělo smůlu a vypadávalo ze sítě, tím hustším se stával provoz na zbývajících ústřednách, přetížených náhlým náporem. A samozřejmě, jak hovory přicházely stále častěji, bylo *mnohem pravděpodobnější*, že dva z nich přijdou v jedné setině sekundy. Ústředna se dokázala vzpamatovat v pouhých čtyřech sekundách. Nebyla koneckonců nijak *fyzicky* poškozena. Z mechanického hlediska pracovala perfektně. Problém byl "pouze" softwarový. Nicméně nakažlivá vlna zmatku se šířila a ústředny 4ESS se zapínaly a opět vypínaly v několikasekundových intervalech po celé Americe, s naprostou, neúnavnou, mechanickou pravidelností. Automaticky *shazovaly* jedna druhou vysíláním nebezpečných signálů "OK". Během deseti minut zasáhla řetězová reakce celou síť. I poté se ústřednám dařilo periodicky obnovovat provoz. Mnohé hovory - milióny hovorů - byly spojeny. Ale další milióny nikoli.

Ústředny užívající Systém 6 nebyly přímo ovlivněny. Díky této staré části systému nezkolabovala celostátní síť AT&T úplně. Tento fakt také prozradil spojařům, že chyba je v Systému 7.

Odborníci z Bell Labs, pracující v New Jersey, Illinois a v Ohiu, nejprve na Systému 7 vyzkoušeli celý svůj repertoár standardních oprav nefunkční telefonní sítě. Žádná z nich pochopitelně neuspěla, protože k takovéto poruše systému ještě nikdy nedošlo.

Plným nasazením záložní sítě nakonec dokázali snížit frekvenci signálů "OK" asi na polovinu. Řetězová reakce se zpomalila a systém se začal uklidňovat. 15. ledna ve 22.30 se vzpamatovala i poslední ústředna a vyčerpaná noční směna si oddychla.

V úterý 15. ledna byl z ústředen 4ESS odstraněn veškerý nový software a nahrazen starší verzí Systému 7. Kdyby v ústřednách seděli místo počítačů živí operátoři, nakonec by prostě přestali křičet. Bylo by jim *jasné*, že situace není "OK", a zdravý rozum by jim poradil zmlknout. Živí lidé mají zdravý rozum - přinejmenším do jisté míry. Počítače ne. Na druhé straně počítače zvládnou stovky hovorů za sekundu. Lidé ne. I kdyby všichni obyvatelé USA pracovali pro telefonní společnosti, nedokázali by zajistit výkon digitálních ústředen: přímou volbu, třícestné hovory, bleskové hovory, spojení na výzvu, osobní čísla a další ovoce z digitálního rohu hojnosti. Nahradit počítače operátory už dnes nepřipadá v úvahu.

Nicméně my stále anachronicky očekáváme, že naše telefonní síť bude řízena lidmi. Je pro nás těžké pochopit, že jsme přenechali většinu iniciativy a kontroly bezduchým a mocným strojům. Když telefony nefungují, chceme, aby za to byl někdo zodpovědný. Chceme viníka.

Když došlo ke kolapsu z 15. ledna, nebyli Američané prostě ochotní připustit, že taková "zemětřesení" v cyberspace jednoduše mohou nastat, aniž by to byla něčí chyba. Bylo snadné, a možná i jistým způsobem uklidňující, uvěřit, že za kolapsem stojí nějaká nepřátelská osoba či skupina osob. Udělali to "hackeři". Nasadili do systému virus. Trojského koně. Softwarovou bombu. Došlo ke zločinnému spiknutí. Mnoho zodpovědných lidí uvěřilo tomuto scénáři. V průběhu roku 1990 tvrdě pracovali na jeho potvrzení.

Hledali na mnohých místech. Ale už v roce 1991 se z mlhy vynořily obrysy nové reality.

1. a 2. července 1991 způsobilo selhání softwaru telefonních ústředen výpadky spojení ve Washingtonu, Pittsburgu, Los Angeles a San Francisku. Drobné problémy při údržbě ústředny opět způsobily pád Systému 7. Kolaps z 1. července pocítilo okolo dvanácti miliónů lidí.

Newyorská tisková agentura vydala následující zprávu: "Podle představitelů telefonních společností a federálních orgánů nelze možnost sabotáže počítačovými hackery vyloučit, nicméně většina z nich zřejmě soudí, že problém byl způsoben nějakým defektem v softwaru řídícím provoz sítě."

A samozřejmě, do týdne se zahanbená softwarová společnost DSC Communications z Plano v Texasu přiznala k "nedostatkům" v softwaru pro "bod transferu signálu", který dodala společnostem Bell Atlantic a Pacific Bell. Bezprostřední příčinou kolapsu z 1. července byla záměna jednoho písmene: jediná tisková chyba na jednom řádku programu. Záměna jednoho písmene, jeden špatný řádek připravil hlavní město USA o spojení. Nebylo nijak zvlášť překvapivé, že tento řádek unikl pozornosti - typická ústředna se Systémem 7 používá *deset miliónů* řádků kódu.

V úterý 17. září 1991 došlo k dosud nejdramatičtějšímu výpadku v americké telefonní síti. V tomto případě nešlo o softwarovou chybu - aspoň ne přímo. Stalo se prostě to, že několika telefonním ústřednám AT&T v New Yorku byla přerušena dodávka elektřiny a ony se jednoduše zastavily. Jejich záložní baterie selhaly. Automatický varovný systém měl ohlásit vybití baterií, jenže tento systém selhal také.

Tentokrát bylo přerušeno hlasové i datové spojení Kennedyho letiště, letiště La Guardia i letiště Newark. Ironickou stránkou této nebezpečné události bylo, že hackerské útoky na letištní počítače jsou již dlouho standardním katastrofickým scénářem, před kterým s oblibou varují bezpečnostní experti obávající se počítačového undergroundu. I v Hollywoodu už natočili thriller o zlověstných hackerech ničících letištní počítače - *Die Hard II*.

Nyní sama AT&T ochromila svými počítači letištní provoz - a ne na jednom letišti, ale na třech najednou, a to na jedněch z nejrušnějších na světě.

Letecký provoz na území Velkého New Yorku byl zastaven, což vedlo ke zrušení více než 500 letů po celé Americe a dokonce i v Evropě. Dalších přibližně 500 letů bylo zpožděno, takže problémy se spojením mělo asi 85 000 pasažérů (jedním z nich byl i šéf Federální komunikační komise).

Cestující, kteří uvízli v New Yorku a New Jersey, zažili další nepříjemné překvapení, když zjistili, že meziměstské telefonní spojení nefunguje, takže nemohou vysvětlit své zpoždění svým blízkým či obchodním partnerům. V důsledku kolapsu se nepodařilo navázat kolem čtyř a půl miliónu vnitrostátních a půl miliónu mezinárodních hovorů. Newyorský kolaps ze 17. září nevyprovokoval na rozdíl od předchozích ani slovo o nebezpečných hackerech. Naopak, v roce 1991 se obviňování, dříve zaměřené na hackery, soustředilo na samotnou AT&T. Kongresmani si stěžovali. Státní i federální kontroloři také. A samozřejmě i tisk.

Konkurenční telekomunikační společnost MCI uveřejnila v newyorských listech výsměšné celostránkové inzeráty, nabízející její vlastní síť pro dálkové hovory, "až AT&T příště přeruší provoz". "Seriózní společnost jako AT&T by se nesnížila k takové reklamě," protestoval nepřesvědčivě ředitel AT&T Robert Allen. AT&T opět publikovala celostránkové sebekritické inzeráty, omlouvající "neomluvitelnou kombinaci lidského a mechanického selhání". (Tentokrát ovšem nenabídla žádné slevy jako kompenzaci. Nelaskaví kritikové usoudili, že AT&T se obávala vytvořit precedent náhrad za finanční ztráty způsobené výpadky spojení.)

Odborné časopisy se veřejně tázaly, zdali AT&T "neusnula za ústřednou". Americká telefonní síť, údajný div technické spolehlivosti, se třikrát v 18 měsících zhroutila. Časopis *Fortune* zařadil kolaps ze 17. září do seznamu "Největších obchodních krachů roku 1991" a paro-

doval reklamní slogany AT&T v článku "AT&T Vás potřebuje (bezpečně na pevné zemi)".

Proč se vlastně newyorské ústředny při přerušení proudu zastavily? Protože nikdo nekontroloval poplašný systém. Jak to, že si nikdo nevšiml, že poplašný systém hlásí varování? Protože tři technici, kteří si *měli* všimnout, nebyli na svém pracovišti v dispečinku. Byli v jiném patře a zúčastnili se školení - školení o poplašném systému dispečinku!

Pád systému přestal být v roce 1991 "bezprecedentní". Naopak, stal se normální událostí. Koncem roku 1991 už bylo jasné, že ani všichni policisté světa nedokáží "ochránit" telefonní síť před zhroucením. Ty zdaleka nejhorší kolapsy způsobil systém *sám sobě*. A nikdo už sebejistě netvrdil, že šlo o neuvěřitelnou náhodu, která se víckrát nebude opakovat. V tomto roce spatřili strážci systému tvář svého tajemného nepřítele - byl jím systém sám.

Digitální underground

Ukradni telefon / Telefandové a hackeři / Pohled z druhé strany / Boardy: jádro undergroundu / Zakázané vědění / Zrození desperáta / Tábory elity / Návnada na hackery / Horký brambor / Válka s Legií / Terminus / Dokument 911 / Fantastické světy / Pravý cyberpunk

Bylo 9. května 1990. Papež pořádal mši v Mexico City. Kšeftaři z Medelínského kartelu se na floridském černém trhu pokoušeli nakoupit rakety Stinger. V novinových komiksech umíral Doonesburyho Andy na AIDS.

A také došlo k události, která si svou neobvyklostí a propracovanou rétorikou získala udivenou pozornost novin po celých USA. Úřad státního zástupce ve Phoenixu v Arizoně vydal tiskovou zprávu, oznamující celostátní policejní zátah proti „ilegálním aktivitám počítačových hackerů“. Jeho oficiální název byl „Operace Sundevil“ („Sluneční ďábel“).

V osmi odstavcích podávala tisková zpráva holá fakta: sedmadvacet domovních prohlídek, uskutečněných 7. května, tři zatčení a sto padesát policistů v akci ve „dvanácti“ městech po celých Spojených státech. (Různé zprávy místního tisku uváděly „třináct“, „čtrnáct“ a „šestnáct“ měst.) Úřad odhadoval ztráty telefonních společností v důsledku kriminální činnosti „až na milióny dolarů“. Úspěch operace byl připisován Tajné službě USA, pomocnému státnímu zástupci ve Phoenixu Timu Holtzenovi a pomocné státní zástupkyni státu Arizona Gail Thackerayové.

Zvláštní zájem byl věnován výrokům Garryho M. Jenkinse, zveřejněným v tiskové zprávě Ministerstva spravedlnosti. Pan Jenkins byl zástupcem ředitele Tajné služby USA a nejvýše postaveným státním představitelem, který se v Zátahu na hackery přímo angažoval.

„Dnes vyslala Tajná služba jasný signál všem počítačovým hackerům, kteří se rozhodli porušovat zákony této země v mylné víře, že se mohou vyhnout dopadení úkrytem za své relativně anonymní počítačové terminály. (...) Vytvořili organizované skupiny za účelem výměny informací usnadňujících jejich kriminální aktivity. Tyto skupiny spolu často komunikují prostřednictvím systémů pro předávání zpráv mezi počítači, zvaných ‚bulletin boardy‘. (...) Naše zkušenosti ukazují, že mnozí z počítačových hackerů nejsou již pouhými svedenými nezletilci, zneužívajícími počítačů ve svých ložnicích ke zlomyslným hrám. Nyní jsou mezi nimi i vysoce kvalifikovaní počítačoví profesionálové, páchající pomocí počítačů trestnou činnost.“

Co byly zač tyto „organizované skupiny“ a „počítačoví profesionálové“? Odkud přišli? Co chtěli? *Kdo* byli? Byli „zlomyslní“? Byli nebezpeční? Jak se „svedeným nezletilcům“ podařilo zalarmovat Tajnou službu USA? Jak rozšířená byla celá tato záležitost? Ze všech skupin účastníků Zátahu na hackery - telefonních společností, policie, ochránců občanských práv a hackerů samotných - jsou hackeři tou zdaleka nejtajemnější, zdaleka nejnepochopitelnější a zdaleka *nejgrotesknější*.

Aktivity hackerů jsou z historického hlediska nové a oni sami se navíc dělí na množství obskurních subkultur s nejrůznějšími jazyky, motivy a hodnotami.

Prvními „protohackery“ byli pravděpodobně oni bezejmenní zlomyslní poslíčkové, které Bellova společnost hromadně propustila z telefonních ústředen v roce 1878.

Hackeři v původním smyslu slova, tedy svobodomyslní, nicméně zákona dbalí počítačoví nadšenci, považují za své duchovní předchůdce zpravidla studenty elitních technických univerzit, zvláště M.I.T. a Stanfordu, v 60. letech.

Ale skutečné kořeny moderního hackerského *undergroundu* lze sledovat nejspíše k dnes už dávno zapomenutému anarchistickému proudu hippies, známému jako Yippies („jipís“). Yippies, kteří vytvořili své jméno z názvu víceméně fiktivní „Youth International Party“ („Mezinárodní strany mládeže“), uskutečňovali radikální a dramatický program surrealistických sabotáží a drzých politických provokací. K jeho základům patřila skandální promiskuita, otevřené a časté užívání drog, svržení všech politikářů přes třicet let a okamžité ukončení války ve Vietnamu, a to všemi prostředky včetně odlevitování Pentagonu.

Dvěma nejviditelnějšími Yippies byli Abbie Hoffman a Jerry Rubin. Rubin se nakonec stal wallstreetským makléřem. Hoffman, intenzívně hledaný federální policií, se sedm let ukrýval v Mexiku, Francii a Spojených státech. Na útěku pokračoval v psaní a publikování, využívaje pomoci sympatizantů z amerického anarchisticko-levičáckého undergroundu. Většinou používal falešné doklady a živil se příležitostnými zaměstnáními. Nakonec si nechal udělat plastickou operaci obličeje a přijal úplně novou identitu jako jistý „Barry Freed“. V roce 1980 se přihlásil úřadům a po usvědčení z držení kokainu strávil rok ve vězení.

Jak slavné časy 60. let bledly, stávaly se Hoffmanovy názory mnohem pochmurnějšími. V roce 1989 údajně spáchal sebevraždu - za podivných a pro některé lidi dosti podezřelých okolností.

Říká se, že materiály o Abbie Hoffmanovi shromážděné FBI jsou tím nejrozsáhlejším vyšetřovacím spisem, jaký kdy byl o nějakém soukromém americkém občanovi založen. (I kdyby to byla pravda, zůstává otázkou, zda FBI považovala Abbieho Hoffmana za skutečné nebezpečí - je docela dobře možné, že jeho spis byl mimořádně velký prostě proto, že Hoffman kolem sebe na každém kroku vytvářel barvité legendy.) Byl nadaným publicistou a elektronická média považoval za prostor ke hrám i k boji. Aktivně se věnoval manipulaci televizních společností i jiných naivních a senzacechtivých médií pomocí různých divokých lží, fantastických pověstí, podvodů se záměnou osob a dalších nekalostí, spolehlivě narušujících duševní rovnováhu policistů, kandidátů na prezidenta a federálních soudců. Hoffmanovou nejslavnější prací byla kniha výmluvně nazvaná *Ukradni tuto knihu*, ukazující mladým a chudým hippies množství postupů, jak „podojit“ systém podporovaný zkostnatělými trubci. *Ukradni tuto knihu*, jejíž titul vyzýval čtenáře k narušení právě té distribuce, která jim k ní umožnila přístup, může být chápána jako duchovní předchůdce počítačového viru.

Hoffman, stejně jako mnoho jiných moderních spiklenců, intenzívně využíval veřejné telefony pro svoji agitační činnost - ovšem místo mincí zpravidla používal laciná mosazná těsnění.

Během války ve Vietnamu existoval zvláštní daňový příplatek za použití telefonu; Hofman a jeho společníci mohli tvrdit, a také tvrdili, že jejich krádeže telefonního spojení jsou aktem občanské neposlušnosti, že z principiálních důvodů odmítají přispívat na nezákonnou a ne-

mravnou válku. Ale tato morální zástěrka byla brzy odložena. Porušování pravidel našlo ospravedlnění v hlubokém odcizení a anarchistickém pohrdání konvenčními měšťáckými hodnotami. Důvtipné způsoby šizení s lehce politickým podtextem, cosi jako „anarchie podle potřeb“, se mezi Yippies staly velmi populárními, a protože šizení bylo tak užitečné, přežilo i samotné hnutí Yippies. Na počátku 70. let bylo poměrně snadné naučit se telefonovat bez placení, opatřit si elektřinu a plyn „zdarma“ nebo dostat z prodejních automatů či parkoměrů peníze na drobná vydání. Pro šíření těchto znalostí byla zapotřebí organizace a pro skutečné páchání drobných krádeží drzost a dobré nervy, ale Yippies žádný z těchto předpokladů nechyběl. V květnu roku 1971 začali Abbie Hoffman a telefonní nadšenec známý pod sarkastickou přezdívkou „Al Bell“ publikovat bulletin nazvaný *Youth International Party Line* („Politika Mezinárodní strany mládeže“). Bulletin se zabýval uspořádáváním a propagací metod šizení, zvláště šizení telefonů, pro radost nevázaného undergroundu a na vztek všem řádným občanům.

Krádež telefonního spojení jako politická taktika zaručovala příznivcům Yippies ničím nerušený přístup k dálkovým spojům bez ohledu na jejich chronický nedostatek organizace, disciplíny, peněz a dokonce i stálých adres.

YIPL vycházel několik let v Greenwich Village v New Yorku. Pak „Al Bell“ víceméně opustil ztenčující se řady Yippies a změnil jméno bulletinu na *TAP* neboli „Program technické asistence“. Po skončení války ve Vietnamu ztratil americký radikální disent své ostří. Ale v té době už se „Al Bell“ a další tucet kmenových přispěvatelů *TAPu* utrhli ze řetězu a přišli na chuť potěšení z čiré *technické moci*.

V nových článcích nahradil politické slogany nelítostný technický žargon, pocta či parodie na originální technické dokumenty Bellu, které redaktoři *TAPu* podrobně studovali, bez povolení reprodukovali a extrahovali z nich užitečné informace. Elita *TAPu* si libovala v pyšném vlastnictví vědomostí nezbytných k překonání systému.

„Al Bell“ rezignoval koncem 70. let a na jeho místo nastoupil „Tom Edison“; čtenáři *TAPu* (celkem asi 1400 lidí) se začali zajímat o telex a o nový fenomén počítačových sítí. V roce 1983 žháři zapálili „Tomu Edisonovi“ dům a ukradli jeho počítač. Pro *TAP* to byla smrtelná rána (ačkoli slavná značka byla vzkříšena v roce 1990 mladým počítačovým desperátem z Kentucky zvaným „Predat0r“.)

Jakmile telefony začaly vydělávat peníze, začali někteří lidé okrádat telefonní společnosti. Legie drobných telefonních zlodějíčků mnohonásobně převyšují počty „telefandů“ („phreaks“ - slovo složené z „phone“ a „freak“), kteří „studují systém“ jako intelektuální výzvu. V oblasti New Yorku, který je již dlouho centrem amerického zločinu, dochází každý rok k více než 150 000 fyzických útoků proti veřejným telefonům! Při pečlivém průzkumu se ukáže, že moderní veřejný telefon je ve skutečnosti malým trezorem, jehož design byl vylepšován po celé generace, aby odolal kovovým plíškům, elektrickým šokům, kusům ledu místo mincí, páčidlům, magnetům, paklíčům i bouchacím kuličkám. Veřejné telefony musí přežít v nepřátelském, chtivém světě a moderní veřejný telefon je stejně unikátním výsledkem evoluce jako třeba kaktus.

Protože telefonní sítě se objevily dříve než sítě počítačové, objevili se i delikventi známí jako „telefandové“ dříve než delikventi známí jako „hackeři“. V praxi je dnes rozdíl mezi činností těchto skupin velmi nezřetelný, stejně jako je nezřetelný rozdíl mezi telefony a počítači. Telefonní síť byla digitalizována a počítače se naučily „hovořit“ po telefonních linkách. Co horšího - jak varoval pan Jenkins z Tajné služby - někteří hackeři se naučili krást, a někteří zloději se naučili „hackovat“.

Navzdory všem nejasnostem lze stále rozlišit některé druhy chování typické jednak pro telefandy, jednak pro hackery. Hackeři se intenzívně zajímají o „systém“ sám o sobě a rádi se napojují na stroje. Telefandové, kteří jsou společenštější, manipulují se systémem s vynaložením minimálního úsilí, aby se jeho prostřednictvím dostali k jiným lidem - rychle, lacino a bez ohledu na pravidla.

Pro telefandy je tou nejlepší zábavou „most“, ilegální telefonická konference tuctu upovídaných spiklenců, od pobřeží k pobřeží, trvající mnoho hodin - a samozřejmě, účtovaná někomu jinému, nejraději nějaké velké společnosti. Jak konference telefandů pokračuje, jedni účastníci zavěšují (nebo jednoduše pustí sluchátko a odtančí do práce, do školy či hlídat děti), zatímco ostatní telefonují novým partnerům, pokud možno z jiného kontinentu, a zvou je, aby se přidali. Vychloubají se, chvástají, naparují, lžou, vyměňují si technické perličky, vymyšlené zážitky, divoké fámy a zlomyslné pomluvy.

Na nejnižší příčce telefandovských dovedností stojí krádež přístupového kódu. Naúčtovat hovor na číslo někoho jiného je samozřejmě primitivní taktika, nevyžadující prakticky žádnou odbornost. Tato činnost je velice rozšířená, zvlášť mezi osamělými lidmi, kteří nemají moc peněz a žijí daleko od domova. Krádeže kódů kvetou v internátech, kasárnách i mezi stavěči rockových skupin. Poslední dobou se krádeže přístupových kódů rychle rozšířily mezi americkými přistěhovalci ze zemí třetího světa, kteří produkují ohromné nezaplacené účty za dálkové telefonní hovory na Karibské ostrovy, do Jižní Ameriky a Pákistánu.

Nejjednodušším způsobem, jak ukrást telefonní kód, je podívat se své oběti přes rameno, když volí svůj vlastní na veřejném telefonu. Tato technika, známá jako „surfing“, je často uplatňována na letištích, autobusových zastávkách a vlakových nádražích. Ukradený kód je za několik dolarů prodán. Jeho kupec nepotřebuje k jeho zneužití žádné počítačové znalosti; zavolá jednoduše mamince do New Yorku, Kingstonu nebo Caracasu a beztrestně se vyhne zaplacení účtu za dálkový hovor.

Cena této primitivní telefandovské aktivity je mnohem, mnohem větší než finanční ztráty způsobené ilegálními průniky hackerů do počítačových sítí. Od poloviny do konce 80. let, než telekomunikační společnosti zavedly přísnější bezpečnostní opatření, bylo kouzelně snadné krást přístupové kódy *počítačem* a tato technika byla obecně používána v digitálním undergroundu, mezi telefandy i hackery. Spočívala v naprogramování počítače tak, aby zkoušel kódy jeden po druhém, dokud nenašel ten pravý. Jednoduché programy uskutečňující tuto činnost byly v undergroundu běžně dostupné; během jedné noci provozu mohl počítač získat asi tucet platných čísel. A program se dal spouštět znovu a znovu po celé týdny, až jeho majitel shromáždil celou knihovnu kradených kódů.

Dnes je možné zjistit automatické vytáčení stovek čísel během několika hodin a rychle vystopovat jeho zdroj. Stejně tak je možné zjistit opakované zneužívání ukradeného kódu. Ale v 80. letech bylo publikování ukradených kódů pro klubající se hackery věcí elementární etikety. Tou nejjednodušší cestou, jak prokázat své nájezdnické kvality, bylo ukrást pomocí opakovaného vytáčení čísel kód a nabídnout ho „veřejnosti“ k volnému použití. Kódy mohly být kradeny i používány z naprostého bezpečí vlastní ložnice, prakticky beze strachu z dopadení a trestu.

Než počítače s připojenými modemy zaplavily americké domácnosti, používali telefandové svůj vlastní telekomunikační hardware, slavnou „modrou skříňku“. Tento zlodějský nástroj (dnes, v digitálních telefonních systémech, už téměř nepoužitelný) dokázal přimět telefonní ústřednu, aby povolila volný přístup na dálkové linky. Dosahoval toho napodobením systémového signálu, tónu o frekvenci 2600 hertzů.

Steven Jobs a Steve Wozniak, zakladatelé firmy Apple Computer, si svého času přivydělávali prodejem modrých skříněk po kalifornských internátech. V té době řada lidí nepovažovala používání modré skříňky za krádež, ale spíše za zajímavý (byť poněkud podfukářský) způsob neškodného využití přebytečné telefonní kapacity. Konec konců, dálkové linky prostě *čekaly na použití*. Vážně, komu to škodilo? Když *nepoškozuješ* systém, *nespotřebováváš* žádné zdroje a nikdo *nezjistí*, co jsi dělal, tak co jsi udělal špatného? Co jsi vlastně *ukradl*? Když v lese spadne strom a nikdo ho neslyší, proč je ten hluk důležitý? I dnes je na takovou otázku těžké odpovědět.

Telefonní společnosti ovšem nepovažovaly modré skříňky za žádnou legraci. Když například radikální kalifornský časopis *Ramparts* („Zákopy“) v červnu roku 1972 publikoval schéma zapojení „němé skříňky“, byl zabaven policií a úředníky Pacific Bellu. Němá skříňka, varianta modré skříňky, dovolovala svému uživateli přijímat dálkové hovory, aniž by za ně volající platil. Tento nástroj byl podrobně popsán v článku v *Ramparts*, ironicky nazvaném „Domácí regulace telefonní společnosti“. Zveřejnění tohoto článku bylo považováno za porušení sekce 502.7 kalifornského trestního zákoníku, jež zakazuje vlastnictví nástrojů umožňujících telefonické podvody a prodej „plánů nebo in-

strukcí k jakékoli pomůcce, přístroji nebo nástroji určených k vyhnutí se placení telefonních poplatků“.

Distribuce tohoto čísla *Ramparts* byla zakázána a výtisky u prodejců zabaveny. Následná finanční ztráta napomohla ke krachu časopisu. Z hlediska svobody projevu to byl nebezpečný precedens, ale likvidace nevýznamného alternativního časopisu telekomunikační společností se tenkrát nesetkala s vážným odporem. I ve svobodomyslné Kalifornii 70. let převládal názor, že na znalostech telefonní sítě je cosi posvátného a že telefonní společnosti mají právní i morální nárok bránit se proti ilegálnímu šíření takových vědomostí. Telekomunikační informace byly většinou natolik specializované, že běžný občan by jim stejně nedokázal porozumět. Nebyly-li by publikovány, málokdo by je postrádal. Nezdálo se, že by publikace takových materiálů byla částí role svobodného tisku.

V roce 1990 inspirovali spojaři podobný útok proti telefandovsko-hackerskému elektronickému magazínu *Phrack*. Případ *Phrack* se stal centrálním právním sporem Zátahu na hackery a vyústil do ohromné kontroverze. Vydávání *Phracku* bylo též pozastaveno, přinejmenším dočasně, ale tentokrát za to jak telekomunikační společnosti, tak jejich policejní spojenci zaplatili mnohem vyšší cenu. Případ *Phrack* podrobně prozkoumáme později.

Telefonování bez placení je dnes stále velmi živou sociální aktivitou. Kvete daleko víc než známější a obávanější činnost „počítačových hackerů“. Rychle se šíří jeho nové formy, využívající nové slabiny sofistikovaných telefonních služeb.

Mobilní telefony jsou zvlášť zranitelné; jejich čipy lze reprogramovat, takže hlásí falešné číslo volajícího a znemožňují vyúčtování. Dalším důsledkem je zabránění policejnímu odposlechu, přispívající k oblibě mobilních telefonů mezi obchodníky s drogami. „Prodej hovorů“ z pirátských mobilních telefonů může být, a také je, provozován z aut, pohybujících se mezi retranslačními stanicemi místní telefonní sítě a prodávajících kradené služby. Jedná se o elektronickou verzi stejného principu, na jakém funguje pojízdný stánek se zmrzlinou. [...]

Označení „hacker“ má z historického hlediska smůlu. Tato kniha, *Zátah na hackery*, má jen málo co říci o „hackování“ v lepším, původním smyslu tohoto slova. Tento termín může označovat intelektuální průzkum nejvyšších a nejhlubších možností počítačových systémů. Může popisovat odhodlání učinit přístup k počítačům a informacím co možná nejširším a nejsvobodnějším. Jeho částí může být pevné přesvědčení, že v počítačích je možno nalézt krásu, že graciéznost dokonalého programu dokáže obohatit racionální i duchovní stránku člověka. Tak popsal životní názor hackerů Steven Levy ve své vysoce ceněné historii počítačových pionýrů *Hackeři*, vydané v roce 1984.

Hackeři všech druhů jsou až po okraj naplněni heroickým odporem k byrokracii. Touží po uznání svého archetypu jako postmoderního elektronického ekvivalentu kovboje a horala. Zaslouží-li si takovou reputaci, rozhodne teprve historie. Ale mnoho hackerů - včetně těch mimo zákon, kteří pronikají do cizích počítačů a jejichž aktivity jsou definovány jako trestný čin - se skutečně snaží dostát své reputaci počítačového kovboje. A vzhledem k tomu, že elektronika a telekomunikace jsou stále téměř neprozkoumanými teritorii, mohou hackeři objevit opravdu *cokoli*.

Pro některé lidi je absolutní svoboda akce stejně důležitá jako vzduch, který dýchají a spontánní činnost je jim životním smyslem a cílem, otevírá brány do zázračných krajin a ke zvýšení potenciálu každého člověka. Ale pro mnoho lidí - pro čím dál tím víc lidí - je hacker zlověstná postava, nenormální vychloubač a anarchista připravený vyrazit ze svého sklepního úkrytu a pro zábavu zničit životy jiných lidí.

Jakákoli forma moci bez zodpovědnosti, bez pevných a jasných omezení a protivah vyvolává strach - a právem. Měli bychom si upřímně připustit, že hackeři *vzbuzují* strach a že základ tohoto strachu není iracionální. Strach z hackerů je mnohem hlubší než strach z pouhé kriminální aktivity.

Útoky na telefonní síť a její manipulace mají zneklidňující politickou dimenzi. V Americe jsou počítače a telefony důležitým symbolem organizované autority a technokratické obchodní elity.

Ale Amerika má i tradici vzpoury proti těmto symbolům, proti všem velkým podnikovým počítačům a všem telefonním společnostem. Žíla anarchismu, pevně vrostlá do americké duše, se raduje ze zmatku a bolesti všech byrokracií, včetně technologických.

Tento přístup je často poznamenán zlomyslností a vandalstvím, nicméně je podstatnou a ceněnou částí americké národní povahy. Muž mimo zákon, rebel, drsný samotář, pionýr, jeffersonovský hrdina, občan usilující o své štěstí a vzdorující nátlaku - každý Američan zná tyto postavy, a mnozí vyzdvihují a hájí jejich odkaz.

Mnoho poctivých, zákona dbalých občanů vykonává dnes vysoce kvalifikovanou práci na počítačích - práci, jež má již nyní ohromné důsledky pro celou společnost a jež bude mít ještě mnohem větší důsledky v příštích letech. Popravdě řečeno, tito talentovaní, pracovití, zákona dbalí, dospělí, cílevědomí lidé jsou pro současný klid a pořádek mnohem nebezpečnější než jakákoli delikventní skupina romantických kluků. Zákona dbalí hackeři mají schopnosti, možnosti a odhodlání ke zcela nepředvídatelným zásahům do života jiných lidí. Mají prostředky, motiv i příležitost k drastickým experimentům s americkým sociálním pořádkem. Jsou-li omezeni požadavky kariéry ve státních službách, na univerzitách nebo ve velkých mezinárodních společnostech a nuceni chovat se podle pravidel a nosit kravaty a saka, je jejich svoboda akce ohraničena aspoň běžnými konvencemi. Ale mají-li volný prostor, sami nebo v malých skupinách, a hnáni imaginací a podnikavým duchem, dokáží pohnout horami - a svrhnout je přímo do vaší kanceláře či obývacího pokoje.

Tito lidé, jako sociální skupina, instinktivně chápou, že všeobecný politický útok proti hackerům bude nakonec rozšířen i proti nim; že termín hacker, je-li démonizován, může být použit k jejich odstavení od převodových pák moci a ohrozit samu jejich existenci. Existují hackeři, kteří vytrvale veřejně kritizují jakékoli znevažování vznešeného titulu hacker. Přirozeně a pochopitelně pociťují odpor k degradaci svých hodnot, která je implicitně obsažena v používání pojmu hacker jako synonyma pro počítačového zločince.

Tato kniha, podle mého názoru bohužel nevyhnutelně, přispívá spíše k devalvaci tohoto pojmu. Zabývá se zejména „hackery“ podle novější a běžnější definice, tj. těmi, kteří pronikají do počítačových systémů potají a bez povolení. Tito lidé jsou rutinně označováni jako „hackeři“ prakticky všemi policejními úředníky, kteří se profesionálně zabývají případy zneužívání počítačů. Americká policie nazývá téměř každý zločin spáchaný na, s, okolo nebo proti počítači „hacking“.

A co je nejdůležitější, „hacker“ je jméno, které dávají ilegální uživatelé počítačů *sami sobě*. Nikdo, kdo proniká do počítačových systémů, se dobrovolně neoznačuje za „zloděje přístupových práv“, „počítačového delikventa“, „piráta“, „divokého hackera“ či „technogangstera“. V naději, že tisk a veřejnost nechají původní smysl slova „hacker“ na pokoji, byla vymyšlena řada nelichotivých označení. Ale používá je málokdo. (Vynechal jsem pojem „cyberpunker“, který je ve skutečnosti užíván některými hackery i policejními úředníky. Tento termín pochází z literárních kruhů a má jisté zajímavé konotace, nicméně dnes se stal, stejně jako pojem hacker, slovem označujícím zloděje.)

V každém případě, ilegální užívání počítačů nebylo původním hackerům nijak cizí. Dýchavičné systémy 60. let vyžadovaly poměrně rozsáhlé chirurgické zásahy k pouhému udržení v provozu. Uživatelé pronikali do nejodlehlejších a nejtemnějších zákoutí svých operačních systémů téměř rutinně. „Počítačová bezpečnost“ v tehdejších primitivních systémech byla v nejlepším případě přívažkem. Důraz byl kladen na fyzickou bezpečnost - předpokládalo se, že každý, kdo má právo přiblížit se k drahému a složitému hardwaru, musí být plně kvalifikovaný profesionál.

Na vysokých školách to ovšem znamenalo, že asistenti, postgraduální studenti, řádní studenti a nakonec bývalí studenti a všichni jejich přátelé získali přístup do počítačových středisek, nebo je dokonce i vedli.

Cílem univerzit není a nikdy nebylo střežit bezpečnost cenných vědomostí. Naopak, univerzity, o stovky let starší než „trh s informacemi“, jsou neziskové kulturní instituce, jejichž (deklarovaným) smyslem a cílem je objevovat pravdu, vědeckými postupy ji kodifikovat a poslé-

ze učit. Mají *předávat pochodeň civilizace*, ne cpát studentům vědomosti do hlavy. Akademické hodnoty jsou neslučitelné s hodnotami obchodníků s informacemi. Příkladem může být všeobecné a neskrývané pirátské kopírování programů i dat učiteli na všech stupních, od mateřské školky výše.

Tento střet hodnot byl živnou půdou kontroverzí. Mnoho hackerů, kteří se učili ovládat počítače v 60. letech, vzpomíná na toto období jako na čas partyzánské války proti „informační aristokracii“ sálových systémů. Mladíci, kteří tehdy chtěli pracovat s počítači, museli o přístup k nim bojovat, a mnozí z nich nebyli povzneseni nad používání jistých, řekněme, „zkratek“. V průběhu let tato praxe vyvedla výpočetní techniku ze sterilních laboratoří technokratů v bílých pláštích a způsobila explozívní rozvoj využití počítačů v běžném životě - zejména *osobních* počítačů.

Některé z těchto mladíků přístup k technické moci doslova uhranul. Většina základních technik ilegálního přístupu do systémů - zjišťování hesel, zadní vrátka, maškarády, trojské koně - byla vynalezena v prostředí univerzit 60. let, v počátcích počítačových sítí. Příležitostné zkušenosti s pronikáním do systémů byly běžnou součástí neformálního curricula většiny „hackerů“, včetně mnoha budoucích šéfů mamutích společností. Málokdo vně malé subkultury počítačových nadšenců přemýšlel o následcích „vloupání do počítačů“. Tato aktivita nebyla nijak popularizována, tím méně kriminalizována.

V 60. letech nebyly ještě pojmy jako „vlastnictví“ a „soukromí“ v cyberspace definovány. Počítače nebyly pro společnost nezbytné. Neexistovaly žádné velké počítačové databáze citlivých obchodních informací, které by se daly bez povolení číst, kopírovat, mazat, měnit či sabotovat. V těch dávných časech byla jejich důležitost malá - ale rostla, exponenciálně, spolu s růstem počítačů.

V 90. letech se komerční a politické tlaky staly neudržitelnými a prolomily hranice hackerské subkultury. Činnost hackerů se stala příliš důležitou, než aby byla ponechána jim samým. Společnost musela vzít v úvahu ekonomické aspekty cyberspace a vymezit neuchopitelný, abstraktní cyberspace jako území se soukromými parcelami. Akce hackerů začaly být posuzovány v novém kontextu „informační společnosti“ 90. let, závislé na seriózním, zodpovědném používání počítačů.

Co tedy znamená proniknout ilegálně do počítače a používat jeho výpočetní kapacitu, nebo si prohlížet jeho soubory, a nepůsobit přitom žádné jiné škody? Co jsou hackeři vlastně zač, jak má společnost - a zákon - definovat jejich činnost? Jsou to jen neškodní *intelektuálové*, hledající informace? Jsou to *voyeuři*, čmuchalové, narušitelé soukromí? Měli by být přísně trestáni jako potenciální *špióni*, ať už političtí nebo průmysloví? Nebo jsou to jen obyčejní *delikventi*, podobní mladistvým vandalům? Je jejich činnost *krádeží služeb*? Konec konců využívají cizí počítače, bez povolení a bez placení. Je to *defraudace*? Možná spíš *používání falešných jmen*. Nejběžnější způsob ilegálního průniku je ukrást nebo odposlechnout cizí heslo a vstoupit do systému pod jménem jiné osoby - osoby, které často zůstane ostuda i účet.

Možná, že medicínský přístup je lepší - hackeři by měli být považováni za nemocné, za *počítačové narkomany*, kteří nejsou schopni kontrolovat své nezodpovědné, nutkavé chování.

Ale tyto seriózní úvahy znamenají pro lidi, které posuzují, velmi málo. Z hlediska hackerského undergroundu jsou všechny zmíněné postřehy legrační, mylné, hloupé nebo nesmyslné. Nejdůležitější přesvědčení undergroundových hackerů - od 60. let až do dneška - je přesvědčení, že jsou *elita*. Každodenní střety v undergroundu se netýkají sociologických definic - kdo by se o ně staral? - ale moci, znalostí a postavení mezi kolegy.

Když jsi hacker, pevné přesvědčení o tvém elitním postavení ti umožňuje porušovat, nebo řekněme raději „přesahovat“, pravidla. Neznamená to ovšem, že *všechna* pravidla jdou k čertu. Pravidla, která hackeři porušují, jsou *nedůležitá* - pravidla natvrdlých hrabivých byrokratů z telekomunikačních společností a ignorantských otrapů z vlády. Hackeři mají *vlastní* pravidla, rozlišující elegantní, elitní chování od chování, které je idiotské, zrádné a odporné. Tato pravidla jsou ovšem nepsaná a prosazovaná neautoritativně, vyžadováním respektu ke skupinovým tradicím. Jako všechny systémy závisející na nevysloveném přesvědčení, že všichni ostatní jsou fajn kluci, jsou i tato pravidla snadno zneužitelná. Hackerské mechanismy „kolegiálního nátlaku“ - „telefonní soudy“ a ostrakizování - jsou zřídkakdy užívány a zřídkakdy fungují. Při vyřizování účtů mezi hackery se spíše uplatňují jedovaté pomluvy, výhružky a elektronické obtěžování, ovšem tyto metody zřídkakdy donutí protivníka k totálnímu ústupu ze scény. Jediným způsobem, jak se opravdu zbavit nějakého hnusného, odporného a zrádného hackera je *předhodit ho policii*. Na rozdíl od mafie či Medelínského kartelu nemůže hackerská elita své zrádce, odpadlíky a potížisty prostě odpravit, takže vzájemné udávání je využíváno překvapivě často.

V hackerském podsvětí neexistuje žádná tradice mlčení či „omerty“. Hackeři mohou být uzavření, dokonce stydliví, ale když mluví, vychloubají se, chvástají a naparují. Téměř všechno, co hackeři dělají, je *neviditelné*. Kdyby se nevychloubali, nechvástali a nenaparovali, *nikdo by se to nikdy nedozvěděl*. Nemáš-li nic, čím by ses mohl vychloubat, chvástat a naparovat, nikdo z undergroundu se o tobě nedoslechne, nebude tě respektovat a spolupracovat s tebou.

Cestou, jak získat v undergroundu reputaci, je říci ostatním hackerům o věcech, které nejsou veřejně známé a dají se zjistit jen nějakým originálním podfukem. Základní měnou digitálního undergroundu, ekvivalentem mořských ulit mezi obyvateli Nové Guineje, je tedy zakázané vědění. Hackeři ho shromažďují, vášnivě zkoumají, zušlechťují, vyměňují a mluví o něm a mluví. Mnoho hackerů dokonce trpí podivným nutkáním *učit* - šířit étos a znalosti digitálního undergroundu. Dělají to, i když jim to nepřináší žádné zvláštní výhody a představuje vážné osobní riziko.

A když se jim jejich riskování nevyplatí, pokračují ve vysvětlování a kázání - k novým posluchačům, totiž k policistům, kteří je vyslýchají. Téměř každý zatčený hacker řekne všechno, co ví. Všechno o svých přátelích, učitelích, žácích, všechny legendy, pověsti, výhružky, strašidelné příběhy, pomluvy a halucinace. To je pro policii samozřejmě výhoda - pokud kriminalisté neuvěří hackerské mytologii.

Telefandové jsou mezi delikventy výjimeční svým odhodláním volat policistům - do kanceláře i domů - a seznamovat je se stavem své mysli. Je těžké neinterpretovat toto chování jako *koledování si o zatčení* - skutečně jde o nebezpečnou hru s ohněm. Policisty takové provokace samozřejmě podráždí, takže vyvinou značné úsilí, aby drzé provokatéry zkrotili. Chování telefandů lze však vysvětlit i jako důsledek elitářského pohledu na svět, tak výlučného a uzavřeného, že v něm elektronická policie není chápána jako policie v pravém slova smyslu, ale spíše jako *nepřátelští telefandové*, které lze kritizovat a „přivést k rozumu“.

Nejpompéznější hackerskou představou je víra, že jsou průkopnickou elitou nového elektronického světa. Snaha přimět je dodržovat demokraticky vytvořené zákony současné americké společnosti je chápána jako represe a perzekuce. Konec konců, argumentují, kdyby se byl Alexander Graham Bell smířil s pravidly telegrafování Western Unionu, nebyly by dnes žádné telefony. Kdyby byli Jobs a Wozniak uvěřili, že IBM je počátkem a koncem všech věcí, nebyly by dnes žádné osobní počítače. Kdyby se byli Benjamin Franklin a Thomas Jefferson snažili „pracovat v rámci systému“, nebyly by dnes žádné Spojené státy americké.

Toto je pro hackery nejen článek soukromé víry; je to idea, které zasvěcují vášnivé manifesty. Následuje několik typických příkladů z jednoho zvláště výmluvného hackerského manifestu, „TechnoRevoluce“, jehož autorem je „Dr. Crash“ („Krach“). Tento manifest byl publikován v elektronické formě v časopise *Phrack*, svazek 1, číslo 6, soubor 3.

„Abychom plně vysvětlili pravé motivy hackerů, musíme se nejprve krátce obrátit do minulosti. V 60. letech postavila skupina studentů MIT první moderní počítačový systém. Pro tuto divokou, nespoutanou skupinu mladých mužů byl poprvé použit titul ‚hacker‘. Systémy, které

vytvořili, měly sloužit k řešení světových problémů a ku prospěchu celého lidstva.

Jak každý ví, situace se vyvíjela jinak. Počítačové systémy byly uzurpovány velkými komerčními organizacemi a vládou. Zázračné zařízení, určené k obohacení života, se stalo zbraní používanou k odlidšťování člověka. Pro vládu a komerční organizace neznamenají lidé nic víc než prostor na disku. Vláda nepoužívá počítače, aby zorganizovala pomoc chudým, ale aby kontrolovala smrtící nukleární zbraně. Průměrný Američan má přístup jen k mikropočítačům, jejichž cena je pouze zlomkem toho, co za ně platí. Obchodníci udržují opravdu špičkové vybavení z dosahu lidí, za ocelovou zdí neuvěřitelně vysokých cen a byrokracie. Z tohoto stavu společnosti se zrodilo hackerství. (...)

Samozřejmě, vláda nechce, aby byl technologický monopol narušen, takže postavila hackery mimo zákon a trestá každého, kdo je chycen. Telefonní společnosti jsou dalším příkladem zneužívané technologie, k níž je lidem zamezován přístup pomocí vysokých cen. (...)

Hackeři často zjišťují, že jejich vybavení, v důsledku monopolní taktiky počítačových společností, není pro jejich účely dostatečné. Následkem vyděračsky vysokých cen je nemožné legálně zakoupit potřebné vybavení. Tato potřeba dala vzniknout dalšímu segmentu boje: kreditnímu nákupu. Kreditní nákup je způsob, jak získat nezbytné zboží bez placení. Příčinou toho, že kreditní nákup je tak snadný, je opět hloupost obchodníků, což ukazuje, že světový obchod je v rukou lidí s podstatně nižším technickým know-how, než máme my, hackeři. (...)

Hackerství musí pokračovat. Musíme učit nováčky tomuto umění. (...) Ať už děláš cokoli, pokračuj v boji. Ať už to víš, či nikoli, jsi-li hacker, jsi revolucionář. Nemáš se čeho bát, jsi na správné straně."

Obrana „kreditního nákupu" je vzácná. Většina hackerů považuje krádež z účtů kreditních karet za „mor" undergroundu, za opovrženíhodnou a nemorální činnost, jež, a to je ze všeho nejhorší, se člověku zpravidla nevyplatí. Nicméně manifesty propagující krádeže z účtů kreditních karet, úmyslné shazování počítačových systémů a dokonce akty fyzického násilí, například vandalismu a žhářství, je v undergroundu možno najít. Takové vychloubačné hrozby jsou policií brány poměrně vážně. A ne každý hacker je abstraktní, platonický počítačový aktivista. Pár z nich má značné zkušenosti s otvíráním zámků, vykrádáním veřejných telefonů a různými metodami vloupání.

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.

Hackeři jsou zpravidla žáci a studenti, kteří si sami nevydělávají na živobytí. Často pocházejí z poměrně dobře situovaných středostavovských rodin a mají výrazně přezíravý vztah k materiálním požitkům (tedy, s výjimkou počítačového vybavení). Každý, koho motivuje touha po pouhých penězích (na rozdíl od touhy po moci, znalostech a statusu), je rychle odepsán jako zabedněný pitomec, jehož hodnoty mohou být pouze zkorumpované a opovrženíhodné.

Dnešní bohémové digitálního undergroundu vyrůstali v 70. a 80. letech a považují společnost jako celek za bažinu plutokratické korupce, kde je každý od prezidenta dolů na prodej a pravidla určují ti, kdo si je zaplatí.

Je zajímavé, že na opačné straně barikády existuje pokřivený odraz stejného přístupu. Policisté jsou jednou z nejvýraznějších sociálních skupin americké společnosti, která nemá materialistické cíle a je motivována nikoli pouhými penězi, ale ideály služby, spravedlnosti, esprit de corps a, samozřejmě, svým vlastním druhem moci a specializovaných vědomostí. Je pozoruhodné, jak často ideologická válka mezi policajty a hackery obsahuje hněvivá obvinění, že druhé straně jde jen o špinavý dolar. Hackeři se vytrvale ušklíbají, že organizátoři jejich trestního stíhání touží po teplých místečkách právníků telekomunikačních společností a policisté vyšetřující počítačové zločiny se později hodlají napakovat jako dobře placení bezpečnostní konzultanti v privátním sektoru.

Ze své strany policisté běžně kladou rovnítko mezi všechny hackerské trestné činy a rozbíjení veřejných telefonů krumpáčem. Výčty „finančních ztrát" vzniklých v důsledku průniků do počítačů jsou notoricky přehnané. Neautorizované zkopírování dokumentu z cizího počítače je morálně postaveno na stejnou úroveň jako loupež, řekněme, půl milionu dolarů z majetku společnosti. Nezletilý hacker, který se zmocnil „důvěrného" dokumentu, ho za takovou sumu zaručeně neprodal, nemá pravděpodobně žádnou představu, jak jeho prodej zařídit, a ještě pravděpodobněji ani neví, co vlastně sebral. Nezískal ze svého zločinu ani cent zisku, nicméně morálně je postaven na roveň zloději, který vykradl kostelní pokladničku a zmizel do Brazílie.

Policisté chtějí věřit, že všichni hackeři jsou zloději. V americkém právním systému je nesnadné, téměř nemožné, odsoudit lidi do vězení jen proto, že se chtějí dozvědět věci, jež je jim zakázáno znát. V americkém kontextu je téměř každý důvod k potrestání lepší než věznit lidi kvůli ochraně jistých druhů informací. Nicméně *restrikce informací* je esencí boje proti hackerům.

***

Pěkným příkladem tohoto rozporu jsou pozoruhodné aktivity „Emanuela Goldsteina", šéfredaktora a vydavatele tištěného časopisu jménem *2600: Hackerský čtvrtletník*. Goldstein studoval angličtinu na Státní univerzitě na Long Islandu v New Yorku v 70. letech, kde se podílel na provozu místní univerzitní radiostanice. Jeho vzrůstající zájem o elektroniku ho přivedl do kruhů Yippies okolo magazínu *TAP* a tedy do digitálního undergroundu, kde se stal, podle svých slov, „techno-krysou". Jeho časopis publikuje techniky průniku do počítačů a „výprav" do telefonní sítě a také odhalení zločinných praktik telekomunikačních společností a neúspěchů vlády.

Goldstein žije tiše a velmi uzavřeně ve velké, hroutící se viktoriánské vile v Setauketu ve státě New York. Dům na mořském pobřeží je vyzdoben schématy telefonních obvodů, kusy vyplaveného dřeva a běžnými dekoracemi hippie squatu. Je svobodný, mírně zanedbaný a živí se převážně hotovými jídly a krocaní nádivkou jedenou přímo z krabice. Goldstein má výrazný šarm a eleganci, krátký, odzbrojující úsměv a nelítostnou, tvrdohlavou, vpravdě recidivistickou integritu, kterou americká elektronická policie pokládá za skutečně nebezpečnou.

Goldstein přijal své nom de guerre, v řeči hackerů „handle", podle postavy z Orwellova *1984*, což je výmluvným příznakem kritičnosti jeho politických postojů a názoru na společnost. Sám není praktikující hacker, ačkoli jejich akce s vervou podněcuje, zvláště jsou-li zaměřeny proti velkým společnostem nebo vládním organizacím. Není ani zloděj, naopak opovržlivě kritizuje pouhou krádež telefonních hovorů, dávaje přednost „průzkumu a ovládání systému". Pravděpodobně nejlépe ho lze popsat a pochopit jako *disidenta*.

Jakkoli podivně to může znít, Goldstein žije v moderní Americe ve velice podobných podmínkách, v jakých žili intelektuální disidenti ve Východní Evropě. Jinými slovy, otevřeně se hlásí k hodnotovému systému, který je hluboce a neodstranitelně neslučitelný se systémem těch, kteří vládnou, i policie. Hodnoty vyjadřované v *2600* jsou zpravidla zastávány ironicky, sarkasticky, paradoxně nebo přímo zmateně. Ale jejich základní tón je nepochybně antiautoritářský. *2600* trvá na tom, že technická moc a speciální vědomosti, jakéhokoli získatelného druhu, patří plným právem do rukou těch lidí, jež jsou natolik odvážní a odhodlaní, aby si je opatřili - všemi dostupnými prostředky. Nástroje, zákony nebo systémy, které brání volnému přístupu a šíření vědomostí, jsou provokacemi, jež by měl každý svobodný a sebevědomý hacker neúnavně ničit. „Soukromí" vlád, obchodních společností a jiných bezduchých technokratických organizací nesmí být chráněno ke škodě svobody a neomezené iniciativy individuální techno-krysy.

Jenže v našem současném prozaickém světě si jak vlády, tak obchodní společnosti dávají velice záležet na restrikci informací, které jsou tajné, obchodním tajemstvím, pro vnitřní potřebu, důvěrné, copyrightované, patentované, nebezpečné, nelegální, neetické, poškozující pověst či jinak citlivé. To dělá z Goldsteina nežádoucí osobu a z jeho filozofie hrozbu.

Velice málo okolností Goldsteinova každodenního života by překvapilo, řekněme, Václava Havla. (Mimochodem můžeme poznamenat, že

prezidentu Havlovi byl svého času zabaven jeho textový editor československou policií.) Goldstein publikuje *samizdat* a polootevřeně funguje jako informační centrum undergroundu a zároveň vyzývá vládní moc, aby dodržovala svá vlastní pravidla: svobodu slova a první dodatek ústavy.

Goldsteinův vzhled přesně padne k jeho image techno-krysy - nosí vlasy až na ramena a černou pirátskou čapku vyzývavě nasazenou na stranu. Často se objevuje na setkáních počítačových odborníků, podoben duchu zavražděného z Macbetha, kde tiše poslouchá, zasněně se usmívá a dělá si pečlivé poznámky.

Setkání počítačových odborníků jsou zpravidla veřejná, takže je pro ně velmi obtížné zbavit se Goldsteina a jemu podobných bez použití nezákonných a protiústavních opatření. Sympatizanti, z nichž mnoho je váženými občany na zodpovědných místech, obdivují Goldsteinovy postoje a potají mu předávají informace. Neznámý, ale zřejmě značný podíl Goldsteinových více než 2000 čtenářů tvoří bezpečnostní odborníci telekomunikačních společností a policisté, kteří jsou nuceni předplácet si *2600*, aby si udrželi přehled o nových hackerských aktivitách. Dostávají se tak do situace, kdy se skřípěním zubů *platí tomu chlapovi nájem*, což by jistě potěšilo Abbieho Hoffmana (jednoho z nemnoha Goldsteinových idolů).

Goldstein je dnes pravděpodobně nejznámějším reprezentantem hackerského undergroundu a zcela jistě tím nejnenáviděnějším. Policie ho považuje za veřejného nepřítele, kazícího mládež, a mluví o něm s nefalšovaným odporem. Jako ovád je maximálně úspěšný.

Například po kolapsu telefonního systému z 15. ledna 1990 Goldstein na stránkách *2600* zručně vetřel spojařům sůl do ran. „Byla to pro telefandy legrace, když jsme pozorovali, jak se systém hroutí," přiznal vesele. „Ale bylo to i zlověstné znamení věcí příštích... Někteří lidé z AT&T se snažili s pomocí seriózních, nicméně ignorantských médií šířit představu, že mnoho společností má tentýž software a může tedy se tedy střetnout se stejným problémem někdy v budoucnosti. To není pravda. Defektní software používá výhradně AT&T. Přirozeně, jiné společnosti se mohou střetnout se zcela *jinými* softwarovými problémy. Ale AT&T také."

Po technické diskusi o nedostatcích systému nabídla techno-krysa z Long Islandu stovkám kvalifikovaných inženýrů gigantické nadnárodní společnosti konstruktivní kritiku. „Nevíme, proč se významná telekomunikační společnost jako AT&T chovala tak neschopně. Kde byly zálohy? Jistě, počítačové systémy se hroutí každou chvíli. Ale lidé, kteří chtějí telefonovat, nejsou titíž jako lidé, kteří se připojují k počítačům. Rozdíl je v tom, že kolaps telefonní sítě či jiné základní služby není akceptovatelný. Budeme-li i nadále důvěřovat technologii, aniž bychom jí rozuměli, můžeme se těšit na mnohé další variace na toto téma.

Je povinností AT&T vůči jejím zákazníkům, aby byla připravena *okamžitě* přepnout na jinou síť, začne-li se dít něco podivného či nepředvídatelného. V tomto případě není novinkou ani tak selhání počítačového programu jako selhání celé struktury AT&T."

Samotná představa toho... té *osoby*... nabízející „rady" o „celé struktuře AT&T", je víc, než někteří lidé dokáží snést. Jak se tenhle napůl kriminálník odvažuje diktovat, jaké chování AT&T je „akceptovatelné"? Zvlášť když v tom samém čísle publikuje detailní schémata zapojení pro vytváření různých signálních tónů telefonní sítě, které jsou veřejnosti nedostupné.

„Všimněte si, co se stane, když pustíte tón nebo dva ze ‚stříbrné skříňky' do vaší místní sítě nebo do dálkového spojení od různých společností," radí jeden z přispěvatelů *2600*, „Mr. Upsetter" („Zneklidňovač") v článku „Jak vyrobit signální skříňku". „Když experimentujete systematicky a děláte si záznamy, určitě zjistíte mnoho zajímavého."

To je samozřejmě vědecký postup práce, zpravidla považovaný za chvályhodnou aktivitu a jeden z květů moderní civilizace. Člověk se skutečně může takovou cílevědomou intelektuální činností naučit ledacos. Zaměstnanci telekomunikačních společností považují tento druh „výzkumu" za ekvivalentní házení dynamitových patron do jejich rybníka, aby se zjistilo, co žije na dně.

2600 je publikováno pravidelně od roku 1984. Redakce založila i BBS, potiskovala trička *2600*, přijímala faxy... V čísle z jara 1991 je na straně 45 zajímavé oznámení: „Právě jsme zjistili, že k naší faxové lince je připojen jeden kabel navíc, vedoucí k telefonnímu sloupu. (Už byl odstraněn.) Vaše faxy k nám i ke komukoli jinému mohou být monitorovány."

Ve světě podle *2600* je malá skupinka technokratických bratří (a, zřídkakdy, sester) obklíčeným předvojem opravdové svobody a ctnosti. Zbytek světa je eldorádem zločinů komerčních společností a korupce vysokých vládních míst, čas od času zmírňovaných snaživou ignorancí. Přečíst několik čísel za sebou znamená vstoupit do noční můry podobné Solženicynovým, i když ne tak pesimistické, protože *2600* je často velice zábavný.

Goldstein se nestal terčem Zátahu na hackery, ačkoli proti němu veřejně, hlasitě a výmluvně protestoval a zátah podstatně přispěl k jeho slávě. Nebylo tomu tak proto, že není považován za nebezpečného - opak je pravdou. Goldstein měl potíže se zákonem v minulosti: v roce 1985 byla BBS *2600* zabavena FBI a část softwaru na ní byla formálně prohlášena za „lupičský nástroj ve formě počítačového programu". Ale v roce 1990 Goldstein unikl přímému postihu, protože jeho časopis je tištěn na papíře a uznáván za subjekt ústavního práva na svobodu tisku. Jak jsme viděli v případu *Ramparts*, není tato ochrana ani zdaleka absolutní. Nicméně z praktického hlediska by zastavení *2600* soudním příkazem vyvolalo takové množství právnických potíží, že je prostě technicky nemožné, přinejmenším v současnosti. Během roku 1990 Goldstein i jeho časopis drze prosperovali.

Zátah na hackery v roce 1990 se místo toho zaměřil na počítačovou formu zakázaných dat. Byl to, především a v první řadě, zátah na *bulletin boardy*. Bulletin board systems („nástěnkové systémy"), častěji známé pod ošklivým, nepluralizovatelným [v angličtině - pozn. překl.] akronymem „BBS", jsou živou vodou digitálního undergroundu. Boardy byly i nejdůležitějším prvkem taktiky a strategie policie při zátahu.

BBS může být formálně definována jako počítač sloužící pro výměnu informací a zpráv mezi uživateli, kteří ho volají telefonem pomocí modemu. „Modem", což je zkratka z modulátor-demodulátor, je zařízení převádějící digitální impulsy počítačů do slyšitelných analogových telefonních signálů a naopak. Modem spojuje počítač s telefonní sítí a tedy s jinými počítači.

Velké sálové počítače jsou propojeny už od 60. let, ale *osobní* počítače, kontrolované jednotlivými majiteli a umístěné v jejich domech, byly poprvé spojeny koncem 70. let. „Board" vytvořený Wardem Christensenem a Randy Suessem v únoru 1978 v Chicagu je obecně považován za první BBS na osobním počítači hodnou toho jména. Boardy fungují na mnoha různých typech počítačů a používají mnoho různých druhů softwaru. První boardy byly primitivní a plné chyb a jejich manažeři, známí jako „systémoví operátoři" neboli „sysopové", byli plně vytížení techničtí experti a autoři svého softwaru. Ale jako prakticky všechno ostatní ve světě elektroniky, staly se v průběhu 80. let i boardy rychlejšími, levnějšími, lépe navrženými a vůbec sofistikovanějšími. Rychle se také rozšířily od pionýrů do rukou široké veřejnosti. V roce 1985 bylo v Americe kolem 4 000 boardů. Výpočty z roku 1990 udávají přibližný počet okolo 30 000 v USA a další tisíce v jiných zemích.

BBS jsou neregulované podniky. Stát se majitelem boardu je operativní, ničím nebrzděná akce. V zásadě každý, kdo má počítač, modem, software a telefonní linku může založit vlastní board. S vybavením z druhé ruky a public-domain softwarem zdarma může být cena boardu velmi nízká - nižší než náklady na vlastní časopis nebo i jen solidní pamflet. Řada prodejců nabízí software pro BBS a trénuje sysopy-amatéry, kteří nemají odborné znalosti, v jeho používání.

Boardy nejsou „tisk". Nejsou to ani časopisy, ani knihovny, ani telefony, ani amatérská rádia, ani tradiční korkové nástěnky v místní prádelně, ačkoli mají jisté společné rysy se všemi těmito dřívějšími médii. Boardy jsou nové médium - možná dokonce *mnoho druhů* nových

médií.

Podívejme se na jejich jedinečné rysy: jejich provoz je laciný, i když mají celostátní či dokonce globální dosah. Kontakt s boardem může být navázán z kteréhokoli místa globální telefonní sítě a majitele boardu to *nic nestojí* - telefonní účet platí volající, a je-li volající místní, je hovor zadarmo [téměř, v Americe - pozn. překl.]. Na boardech se neobrací redakční elita k masám posluchačů. Sysop boardu není exkluzívním autorem ani editorem - je hostitelem v elektronickém salónu, kde se každý může obracet k veřejnosti, hrát roli veřejnosti či si vyměňovat soukromé zprávy s jinými účastníky. „Konverzace“ na boardech, jakkoli plynulá, rychlá a vysoce interaktivní, není mluvená, ale psaná. Je také relativně, a někdy zcela, anonymní.

A protože boardy jsou levné a všudypřítomné, jejich regulace a povinnost získat licenci je pravděpodobně prakticky neprosaditelná. Taková operace by byla srovnatelná s pokusem „regulovat“, „kontrolovat“ a „povolovat“ posílání dopisů - pravděpodobně ještě těžší, protože pošta je na rozdíl od telefonů řízena federální vládou. Boardy řídí jednotlivci, nezávisle a zcela podle svých zálib.

Pro sysopa není hlavním limitujícím faktorem cena provozu boardu. Po počáteční investici do počítače a modemu je jediným trvalým nákladem cena za telefonní linku (nebo několik telefonních linek). Hlavními limitujícími faktory jsou čas a energie. Boardy je třeba udržovat. Noví uživatelé jsou zpravidla „prověřováni“ - musejí obdržet individuální hesla a být kontaktováni telefonem ve svých domovech, aby byla potvrzena jejich identita. Obtížní uživatelé, jichž je mnoho, musejí být vychováváni či odstraněni. Rychle se množící zprávy musejí být vymazány, když zestárnou, aby nebyla překročena kapacita systému. Programy (pokud je board nabízí) musí být kontrolovány na přítomnost počítačových virů. Je-li za použití boardu vyžadován poplatek (což je čím dál tím běžnější, zejména na větších a propracovanějších systémech), musí být vedeno účetnictví a účty zasílány uživatelům. A když se board zhroutí - což je velmi běžná událost - musí být opraven.

Boardy lze třídit podle snahy, která je věnována jejich provozu. Za prvé může jít o zcela otevřený board, jehož sysop vytahuje plechovky piva na ex a sleduje reprízy televizních seriálů, zatímco jeho uživatelé časem zpravidla degenerují do anarchie a posléze ticha. Druhým typem je kontrolovaný board, jehož sysop se objevuje jednou za čas, uklidí, zklidní hádky, zveřejní oznámení a zbaví komunitu pitomců a potížistů. Třetí je silně kontrolovaný board, který trvá na dospělém a zodpovědném chování a cenzuruje všechny zprávy považované za urážlivé, impertinentní, ilegální nebo nesmyslné. A posledním typem je kompletně editovaná „elektronická publikace“, prezentovaná mlčícímu publiku, jemuž není dovoleno přímo reagovat.

Boardy se dají třídit podle stupně své anonymity. Existují kompletně anonymní boardy, kde každý používá pseudonym - „handle“ - a ani sysop nezná pravou identitu uživatelů. Na boardu tohoto typu je i sysop sám zpravidla anonymní. Druhým, běžnějším typem je board, kde sysop zná (nebo si myslí, že zná) pravá jména a adresy všech uživatelů, ale uživatelé neznají jména ostatních a nemusejí znát ani sysopovo. Třetí je board, kde každý musí používat pravá jména a anonymní hraní cizích rolí je zakázáno.

Boardy se dají roztřídit podle rychlosti odezvy. „Chat“ („pokec“) boardy simultánně spojují několik uživatelů na různých linkách, kteří čtou zprávy ostatních v tom samém okamžiku, kdy jsou psány. („Chat“ nabízí mnoho velkých boardů vedle svých ostatních služeb.) Boardy s pomalejší odezvou, které mohou mít jen jednu telefonní linku, ukládají zprávy postupně, jednu za druhou. Některé boardy jsou otevřeny pouze v průběhu dne nebo o víkendech, což jejich odezvu podstatně zpomaluje. *Síť* boardů, jako je třeba „FidoNet“, může přenášet elektronickou poštu z boardu na board, z jednoho kontinentu na druhý, přes neomezené vzdálenosti - ovšem šnečí rychlostí, srovnatelnou s rychlostí pošty, takže zprávě může trvat několik dní, než se dostane k adresátovi a vyvolá odpověď.

Boardy lze třídit podle soudržnosti komunity jejich uživatelů. Některé boardy zdůrazňují výměnu soukromé pošty, od jednoho odesílatele k jednomu příjemci. Jiné upřednostňují veřejné zprávy a mohou se dokonce zbavovat lidí, kteří pouze „číhají“, tj. čtou zprávy, ale sami se diskuse neúčastní. Některé boardy jsou intimní a sousedské, jiné chladné a vysoce technické. Některé jsou jen o málo víc než zásobníky softwaru, kde uživatelé „downloadují“ a „uploadují“ programy, ale mezi sebou navzájem komunikují jen málo, pokud vůbec.

Boardy mohou být roztříděny podle své přístupnosti. Některé boardy jsou naprosto veřejné. Jiné jsou soukromé, určené pouze pro sysopovy osobní přátele. Některé boardy přidělují svým uživatelům různý status. Na takových boardech jsou někteří uživatelé, zejména začátečníci, neznámí nebo děti, vpouštěni jen do veřejné části, případně je jim zakázáno psát zprávy. Na druhé straně sysopovi oblíbení uživatelé mohou psát bez omezení a zůstat „on-line“ jak dlouho chtějí, a to i za cenu omezení jiných lidí, kteří se chtějí přihlásit. Uživatelé s vysokým statusem mohou mít přístup do skrytých oblastí boardu, například k „nestandardním“ tématům, soukromým diskusím a/nebo cennému softwaru. Oblíbení uživatelé se dokonce mohou stát „vzdálenými sysopy“ s právem převzít logickou kontrolu boardu pomocí svého vlastního počítače. Poměrně často takoví „vzdálení sysopové“ převezmou veškerou práci i kontrolu boardu, fyzicky umístěného v cizím domě. Někdy sdílí moc několik „co-sysopů“.

Boardy mohou být tříděny i podle velikosti. Velké, celostátní komerční sítě, například CompuServe, Delphi, GEnie nebo Prodigy, pracují na sálových počítačích a zpravidla nejsou považovány za „boardy“, ačkoli sdílejí mnoho jejich charakteristik, jako je elektronická pošta, diskusní konference, softwarové knihovny a velké a stále rostoucí právní problémy s občanskými svobodami. Některé soukromé boardy mají až 30 telefonních linek a relativně sofistikovaný hardware. Jiné jsou maličké.

Boardy se liší svou popularitou. Některé jsou velké a přeplněné a uživatelé si na ně musí protlačit cestu trvalým signálem „obsazeno“. Jiné jsou velké a prázdné - je jen málo smutnějších věcí než kdysi prosperující board, kam už nikdo nevolá a kde na mrtvé konverzace zmizelých uživatelů usedá digitální prach. Některé boardy jsou maličké a intimní a jejich telefonní čísla jsou úmyslně držena v tajnosti, takže se k nim může přihlásit jen malý počet lidí.

A některé boardy jsou *podzemní*.

Boardy dokáží být tajemné. Aktivity jejich uživatelů mohou být někdy jen těžko odlišitelné od spikleneckých. Někdy *jsou* spiklenecké. Boardy sloužily, nebo byly obviněny, že slouží, všemožným extremistickým skupinám, a podněcovaly, nebo byly obviněny z podněcování, všech myslitelných společensky nepřijatelných, radikálních, špinavých či kriminálních aktivit. Existují satanistické boardy. Nacistické boardy. Pornografické boardy. Pedofilní boardy. Drogové boardy. Anarchistické boardy. Komunistické boardy. Homosexuální a lesbické boardy (těch je zvlášť velké množství a mnohé z nich jsou živé a populární a mají bohatou historii). Sektářské boardy. Evangelické boardy. Boardy pro čaroděje, hippies, punkery, skateboardisty a přívržence UFO. Klidně mohou existovat boardy pro masové vrahy, únosce letadel a nájemné zabijáky. Nikdo to nemůže vyvrátit. Neodhadnutelný počet boardů raší, kvete a uvadá v každém koutě rozvinutého světa. I na první pohled nevinné, veřejně přístupné boardy mohou obsahovat, a někdy skutečně obsahují, tajné oblasti, otevřené jen vyvoleným. A i na velkých, veřejných, komerčních sítích je soukromá pošta zcela soukromá - a velice snadno může být kriminální.

Boardy se věnují prakticky každému představitelnému tématu, jakož i tématům, jež si lze představit jen stěží. Pokrývají široké spektrum sociálních aktivit. Nicméně všichni jejich uživatelé mají cosi společného: jsou vlastníky počítačů a telefonů. Počítače a telefony jsou tedy přirozeně jedněmi z nejdůležitějších témat konverzace na téměř každém boardu.

A hackeři a telefandové, tito narkomanští nadšenci do počítačů a telefonů, žijí boardy. Rojí se kolem boardů a získávají na nich nové přívržence. Koncem 80. let se skupiny telefandů a hackerů, spojené boardy, fantasticky rozšířily.

Pro demonstraci použijme seznam hackerských skupin, zkompilovaný redaktory *Phracku* 8. srpna 1988.

The Administration („Administrativa“). Advanced Telecommunications, Inc. ALIAS. American Tone Travelers. Anarchy Inc. Apple Mafia.

The Association. Atlantic Pirates Guild („Řád atlantických pirátů“). Bad Ass Mother Fuckers („Matkomrdi se špatnou prdelí“). Bellcore. Bell Shock Force. Black Bag („Černá kapsa“). Camorra. C&M Productions. Catholics Anonymous. Chaos Computer Club. Chief Executive Officers. Circle Of Death („Kruh smrti“). Circle Of Deneb. Club X. Coalition of Hi-Tech Pirates. Coast-To-Coast. Corrupt Computing. Cult Of The Dead Cow („Kult mrtvé krávy“). Custom Retaliations („Odveta na míru“). Damage Inc („Porucha“). D&B Communications. The Dange Gang („Zatrápená banda“). Dec Hunters. Digital Gang. DPAK. Eastern Alliance („Východní aliance“). The Elite Hackers Guild. Elite Phreakers and Hackers Club („Klub elitních telefandů a hackerů“). The Elite Society Of America. EPG. Executives Of Crime. Extasy Elite. Fargo 4A. Farmers Of Doom. The Federation. Feds R Us. First Class („První třída“). Five O („Pětka“). Five Star („Pět P“). Force Hackers. The 414s. Hack-A-Trip. Hackers Of America. High Mountain Hackers („Vysokohorští hackeři“). High Society („Lepší společnost“). The Hitchhikers. IBM Syndicate („Mafie IBM“). The Ice Pirates („Diamantoví piráti“). Imperial Warlords. Inner Circle („Vnitřní kruh“). Inner Circle II. Insanity Inc. International Computer Underground Bandits. Justice League of America. Kaos Inc („Chaos“). Knights Of Shadow. Knights Of The Round Table („Rytíři kulatého stolu“). League Of Adepts. Legion Of Doom. Legion Of Hackers („Hackerská legie“). Lords Of Chaos. Lunatic Labs, Unlimited („Laboratoře šílenství“). Master Hackers. MAD! („Amok“). The Marauders („Nájezdníci“). MD/PhD (akademický titul). Metal Communications, Inc. MetalliBashers, Inc. MBI. Metro Communications. Midwest Pirates Guild. NASA Elite. The NATO Association. Neon Knights („Neonoví rytíři“). Nihilist Order. Order Of The Rose. OSS. Pacific Pirates Guild. Phantom Access Associates. PHido PHreaks. The Phirm („Firma“). Phlash („Záblesk“). PhoneLine Phantoms. Phone Phreakers Of America. Phortune 500. Phreak Hack Delinquents. Phreak Hack Destroyers. Phreakers, Hackers, And Laundromat Employees Gang („Gang telefandů, hackerů a zaměstnanců prádelen“) čili PHALSE Gang („Falešný gang“). Phreaks Against Geeks („Telefandové proti frajerům“). Phreaks Against Phreaks Against Geeks. Phreaks and Hackers of America. Phreaks Anonymous World Wide. Project Genesis. The Punk Mafia. The Racketeers. Red Dawn Text Files („Textové soubory rudého úsvitu“). Roscoe Gang. SABRE. Secret Circle of Pirates. Secret Service („Tajná služba“). 707 Club. Shadow Brotherhood („Bratrstvo stínů“). Sharp Inc. 65C02 Elite. Spectral Force. Star League („Hvězdná liga“). Stowaways. Strata-Crackers. Team Hackers ’86. Team Hackers ’87. TeleComputist Newsletter Staff („Redakce Telecomputistu“). Tribunal Of Knowledge. Triple Entente („Trojitá aliance“). Turn Over And Die Syndrome („Příznak Otoč se a zemři“) čili TOADS („Ropuchy“). 300 Club. 1200 Club. 2300 Club. 2600 Club. 2601 Club. 2AF. The United Soft WareZ Force („Jednotky softwarových pirátů“). United Technical Underground („Spojený technický underground“). Ware Brigade („Softwarová brigáda“). The Warelords. WASP.

Ponořit se do tohoto seznamu je hluboký, téměř mystický zážitek. Jako kulturní artefakt je vysloveně poetický.

Undergroundové skupiny - subkultury - lze rozlišit od nezávislých kultur podle jejich zvyku neustále se odvolávat na mateřskou společnost. Subkultury ze své podstaty musejí udržovat membránu, oddělující je od okolí. Vyzývavé šaty a účes, specializovaný žargon, charakteristické, oddělené oblasti měst, odlišná doba vstávání, práce a spánku... Digitální underground, který se specializuje na informace, klade velký důraz na jazyk jako nástroj ozvláštnění. Jak je vidět z předcházejícího seznamu, s oblibou používá parodii a výsměch. Je zajímavé všimnout si, kdo je terčem tohoto výsměchu.

Za prvé, velké společnosti. Máme tu Phortune 500 (Fortune 500 je seznam pěti set nejbohatších Američanů, publikovaný stejnojmenným časopisem), The Chief Executive Officers (titul ředitele velké společnosti), Bellcore (výzkumná laboratoř AT&T), IBM Syndicate, SABRE (počítačový rezervační systém používaný aeroliniemi). Pozoruhodné je časté užívání „Inc.“ - žádná z hackerských skupin není skutečnou korporací, ale zjevně je těší hrát si na ně.

Za druhé, vládu a policii. NASA Elite, NATO Association. Feds R Us (parodie na název hračkářské firmy, doslova „Policajti jsou my“) a Secret Service jsou pěkné příklady verbální odvahy. OSS neboli Office of Strategic Services („Úřad strategických služeb“) byl předchůdcem CIA.

Za třetí, zločince. Použití nelichotivých pejorativ jako zvráceného vyznamenání je klasickou taktikou subkultur: punkerů, pirátů, banditů, gangů a mafií.

Nestandardní ortografie, zejména užívání „ph“ místo „f“ a „z“ místo „s“ označujícího plurál, je nezaměnitelným charakteristickým znakem. Stejně tak používání číslice „0“ místo písmene „O“ - abecedy počítačů zpravidla odlišují nulu proškrtnutím, takže rozdíl je zřejmý.

Některé výrazy poeticky opisují ilegální pronikání do počítačů: Stowaways („Černí pasažéři“), Hitchhikers („Stopaři“), PhoneLine Phantoms („Fantómové telefonní linky“), Coast-to-Coast („Dálkoví“). Všimněte si také častého používání slov jako „elita“ a „mistr“. Některé názvy jsou vulgární, některé obscénní, další pouze kryptické - vše s cílem překvapit, urazit, zmást „normální“ lidi a nedovolit jim zůstat lhostejnými.

Mnoho hackerských skupin ještě dále šifruje svá jména používáním akronym: z názvu United Technical Underground se stává UTU, z Farmers of Doom („Pěstitelé zkázy“) FoD, the United SoftWareZ Force trvá na zkratce „TuSwF“ - a běda ignorantskému krtkovi, jež neví, která písmena mají být velká.

Dále je třeba si všimnout, že i jednotliví členové těchto skupin používají pseudonymy. Seznámíte-li se třeba s „PhoneLine Phantoms“, zjistíte, že jsou to „Carrier Culprit“ („Telefonní pachatel“), „The Executioner“ („Kat“), „Black Majik“ („Černá magie“), „Egyptian Lover“ („Egyptský milovník“), „Solid State“ („Stav pevný“) a „Mr Icom“ (název firmy poskytující zlevněné telefonní spojení). „Carrier Culprit“ bude pro své přátele pravděpodobně „CC“ - budou například mluvit o „číslech od CC z PLP“.

Je velice dobře možné, že celkový počet členů všech skupin ze seznamu je třeba jen tisíc lidí. Není to kompletní seznam undergroundových skupin - neexistuje žádný takový seznam a nikdy existovat nebude. Skupiny vznikají, prosperují, upadají, sdílejí členy a udržují si okruh obdivovatelů usilujících o členství a příležitostných známých. Lidé se zapojují a odpadají, jsou ostrakizováni, ztrácejí zájem, jsou nalezeni policií či zahnáni do kouta bezpečnostními odborníky telekomunikací, předkládajícími vysoké účty. Mnoho undergroundových skupin jsou softwaroví piráti, kteří mohou porušovat copyright a ilegálně šířit programy, ale neodváží se pronikat do cizích počítačových systémů. Odhadnout skutečnou velikost populace digitálního undergroundu je velice těžké. Hackeři přicházejí a odcházejí. Většinou začínají mladí, střídají období aktivity a pasivity a končí v 22, když absolvují střední školu. A velká většina „hackerů“ se připojuje na pirátské boardy, vymyslí si handle, šíří copyrightovaný software a možná zneužije jeden či dva telefonní kódy, aniž by kdy vstoupila do řad elity.

Někteří soukromí vyšetřovatelé, živící se poskytováním informací o undergroundu platícím zákazníkům z bezpečnostních složek soukromých společností, odhadli počet hackerů až na padesát tisíc. Toto číslo je pravděpodobně vysoce nadhodnocené, pokud člověk nepočítá každého nezletilého softwarového piráta a zlodějíčka vykrádajícího telefonní budky. Můj odhad je kolem 5 000 lidí. A řekl bych, že z tohoto počtu může být tak stovka skutečné „elity“ - aktivních hackerů, schopných proniknout do sofistikovaných systémů, opravdové hrozby, jíž by se měly zabývat soukromé bezpečnostní složky i policie.

Další zajímavou otázkou je, zdali toto číslo roste. Začínající nezletilí hackeři jsou si často jisti, že nástup hackerů je nezadržitelný a že brzy ovládnou celý cyberspace. Starší a zkušenější veteráni, v ctihodném věku 24 nebo 25 let, jsou přesvědčeni, že zlatý věk už dávno skončil, že policajti mají celý underground přečtený a že dnešní mládež je blbá jak tágo a má zájem akorát o hraní Nintenda.

Já sám bych řekl, že pronikání do počítačů jako nezisková zábava a akt přijetí intelektuální výzvy je na pomalém ústupu, přinejmenším ve Spojených Státech; ale že počítačová zpronevěra, zvláště prostřednictvím telekomunikací, dramaticky roste.

Lze vymezit zajímavou paralelu mezi digitálním undergroundem a drogovým undergroundem. Bývaly časy, v důsledku historického revizio-

nismu dnes už skoro zapomenuté, kdy se účastníci koncertů volně dělili o jointy a hippie prodavači marihuany nabízeli lidem cigaretu zdarma, jen aby si užili dlouhého zdrogovaného rozhovoru o Doors a Allenu Ginsbergovi. Dnes jsou drogy čím dál tím víc za hranicí přijatelného, s vyjímkou nebezpečného, kriminálního světa vysoce návykových drog. Léta negativní propagandy a tlaku policie přiměla neurčitě ideologický, svobodomyslný drogový underground opustit trh s drogami a přenechat ho mnohem brutálnějšímu, kriminálnímu tvrdému jádru. Není to příjemná vyhlídka, ale analogie je velmi přesvědčivá.

Jak vypadá takový undergroundový board? Čím se liší od obyčejného? Rozdíl nemusí být nutně v konverzaci - hackeři se často baví o tématech, které jsou na boardech běžné, tj. o hardware, software, sexu, sci-fi, současných událostech, politice, filmech a osobních vtípcích. Undergroundový board lze nejlépe poznat podle jeho souborů (v hackerské transkripci „philes"), tj. textů, které učí techniky a étos undergroundu, vzácných rezervoárů zakázaného vědění. Některé jsou anonymní, ale většina hrdě nese handle hackera, který je jejich autorem, a jeho skupinu, pokud se k nějaké hlásí. Následuje částečný seznam „philes" jednoho undergroundového boardu, kdesi uprostřed Ameriky, cirka 1991. Většina popisů nepotřebuje komentář.

```
5406  06-11-91  Hacking Bank America BANKAMER.ZIP
4481  06-11-91  Chilton Hacking CHHACK.ZIP
4118  06-11-91  Hacking Citibank CITIBANK.ZIP
3241  06-11-91  Hacking Mtc Credit Company CREDIMTC.ZIP
5159  06-11-91  Hackers Digest DIGEST.ZIP (sborník)
14031 06-11-91  How To Hack HACK.ZIP
5073  06-11-91  Basics Of Hacking HACKBAS.ZIP (základy)
42774 06-11-91  Hackers Dictionary HACKDICT.ZIP (slovník)
57938 06-11-91  Hacker Info HACKER.ZIP
3148  06-11-91  Hackers Manual HACKERME.ZIP
4814  06-11-91  Hackers Handbook HACKHAND.ZIP (příručka)
48290 06-11-91  Hackers Thesis HACKTHES.ZIP (diplomová práce)
4696  06-11-91  Hacking Vms Systems HACKVMS.ZIP
3830  06-11-91  Hacking Macdonalds (Home Of The Archs) MCDON.ZIP
15525 06-11-91  Phortune 500 Guide To Unix P500UNIX.ZIP
8411  06-11-91  Radio Hacking RADHACK.ZIP
4096  12-25-89  Suggestions For Trashing TAOTRASH.DOC (prohledávání popelnic)
5063  06-11-91  Technical Hacking TECHHACK.ZIP
```

Široký výběr „Udělej si sám" příruček o ilegálním pronikání do počítačů. Toto je pouze malý výsek z mnohem větší knihovny o hackerských a telefandovských technikách a historii. Nyní se přesuneme do jiné, možná trochu překvapivé oblasti - „Anarchie".

```
3641  06-11-91  Anarchy Files ANARC.ZIP
63703 06-11-91 Anarchist Book ANARCHST.ZIP
2076  06-11-91  Anarchy At Home ANARCHY.ZIP
6982  06-11-91  Anarchy No 3 ANARCHY3.ZIP
2361  06-11-91  Anarchy Toys ANARCTOY.ZIP
2877  06-11-91  Anti-modem Weapons ANTIMODM.ZIP
4494  06-11-91  How To Make An Atom Bomb ATOM.ZIP
3982  06-11-91  Barbiturate Formula BARBITUA.ZIP
2810  06-11-91  Black Powder Formulas BLCKPWDR.ZIP (černý prach)
3765  06-11-91  How To Make Bombs BOMB.ZIP
2036  06-11-91  Things That Go Boom BOOM.ZIP
1926  06-11-91  Chlorine Bomb CHLORINE.ZIP
1500  06-11-91  Anarchy Cook Book COOKBOOK.ZIP (recepty)
3947  06-11-91  Destroy Stuff DESTROY.ZIP
2576  06-11-91  Dust Bomb DUSTBOMB.ZIP
3230  06-11-91  Electronic Terror ELECTERR.ZIP
2598  06-11-91  Explosives 1 EXPLOS1.ZIP
18051 06-11-91  More Explosives EXPLOSIV.ZIP
4521  06-11-91  Ez-stealing EZSTEAL.ZIP
2240  06-11-91  Flame Thrower FLAME.ZIP (plamenomet)
2533  06-11-91  Flashlight Bomb FLASHLT.ZIP (bomba v baterce)
2906  06-11-91  How To Make An Fm Bug FMBUG.ZIP
2139  06-11-91  Home Explosives OMEEXPL.ZIP
3332  06-11-91  How To Break In HOW2BRK.ZIP (vloupání)
2990  06-11-91  Letter Bomb LETTER.ZIP (dopisová bomba)
2199  06-11-91  How To Pick Locks LOCK.ZIP (otvírání zámků)
3991  06-11-91  Briefcase Locks MRSHIN.ZIP (zámky kufrů)
3563  06-11-91  Napalm At Home NAPALM.ZIP
3158  06-11-91  Fun With Nitro NITRO.ZIP
2962  06-11-91  Paramilitary Info PARAMIL.ZIP
3398  06-11-91  Picking Locks PICKING.ZIP
2137  06-11-91  Pipe Bomb PIPEBOMB.ZIP (bomba z trubky)
3987  06-11-91  Formulas With Potassium POTASS.ZIP (nitráty)
11074 08-03-90  More Pranks To Pull On Idiots! PRANK.TXT (kanadské vtipy)
4447  06-11-91  Revenge Tactics REVENGE.ZIP (odveta)
2590  06-11-91  Rockets For Fun ROCKET.ZIP (rakety)
3385  06-11-91  How To Smuggle SMUGGLE.ZIP (pašování)
```

Ježíšku na křížku! Vždyť to jsou návody na *bomby*!

Tak co si s tím počneme?

Za prvé bychom měli uznat, že rozšiřovat znalosti o výbušninách mezi děti je vysoce odsouzeníhodný akt. Není ovšem nijak ilegální.

Za druhé bychom si měli uvědomit, že většina těchto souborů byla ve skutečnosti *napsána* dětmi. Většina dospělých Američanů, kteří si dokážou vybavit svá mladá léta, si vzpomene, že představa postavení plamenometu v rodinné garáži je prostě skvělý nápad. *Skutečně* postavit v garáži plamenomet je ale spojeno s odstrašujícími potížemi. Exploze nastražené baterky, do které jsi nacpal střelný prach, trhající ruku zástupce ředitele školy, může být temně krásný duševní obraz. Skutečný útok výbušninou ti vynese vytrvalou pozornost Úřadu pro alkohol, tabák a střelné zbraně.

Nicméně někteří lidé tyto návody vyzkoušejí. Americký nezletilec, který je pevně rozhodnutý někoho zavraždit, může nejspíš ukrást nebo koupit revolver mnohem snáz než připravit falešný napalm v kuchyňském dřezu. Nicméně je-li lidem předloženo nějaké pokušení, jistá část mu podlehne, a malá menšina se pokusí tyto plány realizovat. Velká většina této malé menšiny neuspěje nebo se dokonce zmrzačí, protože přesnost návodů není kontrolována, jejich autoři nemají profesionální zkušenosti a často si je prostě vymýšlejí. Ale hrozba těchto „philes“ nemůže být zcela přehlížena.

Hackeři nemusí brát bombové útoky „doopravdy“; kdyby tomu bylo jinak, slyšeli bychom mnohem víc o vybuchujících baterkách, podomácku vyrobených bazukách a středoškolských učitelích otrávených chlorinem či kyanidem. Ovšem hackeři se *doopravdy* zajímají o zakázané vědění. Nejsou vedeni jen zvědavostí, ale opravdovou *touhou po vědění*. Přání vědět něco, co ostatní neví, je stěží nové. Ale *intenzita* tohoto přání, demonstrovaná technofilickými dětmi Informačního věku, *může být nová*, může být příznakem zásadního posunu společenských hodnot, ukázkou toho, k čemu spěje svět, kladoucí čím dál tím větší důraz na vlastnictví, shromažďování a prodej *informací* jako základní komodity denního života.

Vždy existovali mladí muži, kteří se vášnivě zajímali o tato témata. Ale nikdy dříve nebyli schopni tak univerzálně a lehce komunikovat mezi sebou a bez potíží propagovat své zájmy mezi zbytkem společnosti. Středoškolští učitelé vědí, že v každé skupině se jeden najde, ale když onen jeden unikne kontrole přesunem do telefonní sítě a na boardu se spojí se stovkou sobě podobných, zjevně hrozí potíže. Nutkání autorit *něco podniknout*, dokonce i něco drastického, je těžké odolat. V roce 1990 autority něco podnikly. Podnikly toho docela dost. [...]

Pronikání do počítačů je hackery chápáno jako *hra*. To není úplně iracionální a psychopatický přístup. Hacker může vyhrávat či prohrávat, uspět či selhat, ale jeho činnost nikdy není „reálná“. Není to jen tím, že nezletilci s bujnou představivostí mají někdy potíže rozlišit zbožná přání od skutečného života. Cyberspace *není skutečný*! „Skutečné“ věci jsou hmotné objekty, stromy, boty, auta. Činnost hackera se odehrává na obrazovce. Slova nejsou hmotná, čísla (dokonce ani telefonní čísla a čísla kreditních karet) nejsou hmotná. Počítač a svět, to je jako nebe a dudy, něco úplně jiného. Počítače *simulují* realitu, tak jako počítačové hry simulují tankové bitvy, psí zápasy a vesmírné lodě. Simulace jsou jenom hra, a to, co je v počítačích, *není skutečné*.

Uvažujte: jestli je „hackování“ tak vážné a opravdové a nebezpečné, jak to, že *devítileté děti* mají počítače a modemy? Nikdo by nedal devítiletému klukovi do rukou auto, nebo pušku, nebo motorovou pilu - takové věci jsou *skutečné*.

Příslušníci undergroundu jsou si velmi dobře vědomi, že jejich „hra“ se těm nahoře nelíbí. Zprávy o akcích proti undergroundu se šíří rychle. Publikovat je je jedna z hlavních funkcí pirátských boardů, ovšem ty učí i svůj vlastní postoj k policejním zásahům, své charakteristické ideály spravedlnosti. Uživatelé undergroundových boardů si nebudou stěžovat, je-li někdo zatčen pro shazování systémů, šíření virů nebo elektronickou zpronevěru. Mohou kroutit hlavou s vědoucím úsměvem, ale nebudou takové praktiky otevřeně hájit. Ale je-li někdo obviněn z krádeže nějaké teoretické sumy, třeba 233 846 dolarů a 14 centů, protože se dostal do cizího počítače, něco si zkopíroval a schoval si to na svoji disketu ve svém domě - je to považováno za příznak bláznovství žalobců, za příznak jejich zmatení abstraktní hry s počítači se skutečným, nudným každodenním světem velkých peněz.

Jako by si velké společnosti a jejich ochočení právníci mysleli, že používání počítačů je rezervováno jen pro ně, že na něj mohou dát cenovky jako na krabice s pracím práškem! Ale počítat cenu informace je jako počítat cenu vzduchu nebo cenu snů. Každý na pirátském boardu ví, že použití počítačů může být, a mělo by být, *svobodné*. Pirátské boardy jsou malé alternativní ostrůvky v cyberspace, které nepatří žádným firmám, ale undergroundu. Nejsou „sponzorovány firmou Procter & Gamble“.

Připojit se k undergroundovému boardu může být osvobozující zážitek, vstup do světa, ve kterém peníze nejsou tím nejdůležitějším a dospělí nemají na všechno odpověď.

Podívejme se na další vášnivý hackerský manifest. Toto jsou úryvky ze „Svědomí hackera“ od „Mentora“, převzaté z *Phracku*, svazek 1, číslo 7, soubor 3.

„Dnes jsem učinil objev. Nalezl jsem počítač. Moment, to je skvělé. Dělá to, co chci. Když udělá něco špatně, je to proto, že já jsem udělal chybu. Ne protože mě nemá rád. (...)

A pak se to stalo... brána se otevřela... vyslaný elektronický signál se řítí telefonní linkou jako heroin žílou narkomana a hledá úkryt před ubíjející každodenností... nalézá board. To je to místo... sem patřím... Znám tu každého, i když jsem se s nimi nikdy nepotkal, nikdy s nimi nemluvil, možná o nich už nikdy neuslyším... Znám vás všechny... (...) Toto je náš svět... svět elektronů a ústředen, svět krásného baudu. Používáme již existující služby a neplatíme za to, co by mohlo být směšně laciné, kdyby to nebylo majetkem chamtivých nenažranců, a jsme pro vás zločinci. Zkoumáme, a jsme pro vás zločinci. Chceme se učit, a jsme pro vás zločinci. Jsme bez rozdílu barvy, národnosti, bez náboženských předsudků... a jsme pro vás zločinci. Vy stavíte atomové bomby, vedete války, vraždíte, podvádíte a lžete nám a chcete, abychom uvěřili, že je to pro naše vlastní dobro, ale my jsme pro vás zločinci.

Ano, jsem zločinec. Páchám zločin zvědavosti. Páchám zločin posuzování lidí podle toho, co říkají a co si myslí, ne podle toho, jak vypadají. Páchám ten zločin, že jsem chytřejší než vy, a to mi nikdy neodpustíte.“

Undergroundové boardy existují téměř od té doby, odkdy existují boardy. Jedním z prvních byla 8BBS, jež se stala základnou elity telefandů na západním pobřeží USA. 8BBS, která zahájila provoz v březnu 1980, podporovala „Susan Thunder“ („Hromovou Susan“), „Tuca“ a zejména „Kondora“. Kondor se může pochlubit vůbec nejhorší pověstí ze všech amerických telefandů a hackerů. Kondorovi undergroundoví spolupracovníci, navztekaní jeho zlomyslným chováním, ho předali policii i s omáčkou divokých hackerských legend. Důsledkem bylo, že Kondor byl držen sedm měsíců v samovazbě, aby nemohl zahájit třetí světovou válku odpálením strategických raket z vězeňského telefonu. (Po odsloužení trestu byl propuštěn na svobodu; třetí světová válka zjevně dosud nezačala.)

Sysop 8BBS byl radikálním příznivcem svobody slova, zastávající názor, že *jakýkoli* pokus omezit konverzaci uživatelů jeho boardu by byl neústavní a nemorální. Techničtí nadšenci hromadně vstupovali na 8BBS a vynořovali se jako telefandové a hackeři, až v roce 1982 jeden z vděčných absolventů nabídl sysopovi nový modem, zakoupený na cizí kreditní kartu. Policisté využili příležitosti a zabavili celý board, aby odstranili - podle svého názoru - lákavý zdroj potíží.

Plovernet byl velký pirátský board na východním pobřeží USA, operující v New Yorku a na Floridě. V roce 1983 měl pět set aktivních uživatelů. Emanuel Goldstein byl svého času „co-sysopem“ Plovernetu, společně s „Lexem Luthorem“, zakladatelem skupiny „Legion Of Doom“ („Legie soudného dne“), které se brzy budeme věnovat podrobně.

„Pirate-80“ neboli „P-80“, jejíž sysop byl znám pod jménem „Scan Man“ („Hledač“), začala jako jedna z prvních v Charlestonu a vytrvale pokračovala po celá léta. P-80 prosperovala tak nápadně, že to znervózňovalo i její nejostřílenější uživatele, a někteří z nich dokonce nactiu-

trhačně naznačovali, že Scan Man musí mít styky s bezpečnostními specialisty telefonních společností, což on rozhořčeně odmítal.

„414 Private“ byl domovem první *skupiny*, která se stala známou svou pochybnou činností, nezletilců s názvem „414 Gang“, jejichž průniky do Sloan-Ketteringova centra pro rakovinu a do vojenských počítačů v Los Alamos se v roce 1982 staly novinářskou senzací.

Tehdy se také začaly objevovat boardy softwarových pirátů, vyměňujících si kopie her pro Atari 800 a Commodore C64, zbavené ochrany proti kopírování. Většinu uživatelů těchto boardů tvořili pochopitelně nezletilí. A s uvedením hackerského thrilleru *War Games* („Válečné hry“) v roce 1983 undergroundová scéna explodovala. Zdálo se, že každý americký kluk chtěl a dostal k vánocům modem. Většina těchto náhodných zájemců uložila své modemy po pár týdnech do skříně, a většina zbytku se chovala slušně a vyhýbala se pochybným akcím. Ale někteří tvrdohlaví a talentovaní vytrvalci vzali toho malého hackera ve *War Games* jako skutečnou postavu. Prostě si nedali pokoj, dokud se nespojili s undergroundem; a když se jim to nepovedlo, vytvořili svůj vlastní.

***

V polovině 80. let se undergroundové boardy šířily jako digitální plíseň. ShadowSpawn Elite („Elita Synů stínu“). Sherwood Forest I, II a III. Digital Logic Data Service na Floridě, jejímž sysopem nebyl nikdo menší než „Digitální Logika“ sama; Lex Luthor, zakladatel Legion of Doom, byl jednou z hvězd tohoto boardu, který se nacházel v jeho telefonním okruhu. Lexův vlastní board, Legion of Doom, zahájil činnost v roce 1984. „Neon Knights“ založili síť boardů pro hackery na Apple: Severní, Jižní, Východní a Západní Neonové rytíře. Sysopem boardu Free World II („Svobodný svět II“) byl „Major Havoc“ („Major Zkáza“). Lunatic Labs je v době vzniku této knihy stále v provozu. Dr. Ripco v Chicagu, rozverný anarchistický board s bohatou a divokou historií, byl zabaven agenty Tajné služby USA v roce 1990 v rámci operace Sundevil, ale téměř okamžitě obnovil provoz, s novými stroji a starým elánem.

Scéna v St. Louis se nevyrovnala velkým střediskům amerických hackerů, jako je New York a Los Angeles. Ale v St. Louis sídlili „Knight Lightning“ („Rytířský blesk“) a „Taran King“ („Král Tarantule“), dva z předních undergroundových *žurnalistů*. Boardy v Missouri, například Metal Shop, Metal Shop Private a Metal Shop Brewery, neměly sice ten nejtěžší kalibr zakázaných vědomostí, ale byly to boardy, kde hackeři mohli společensky konverzovat a uvažovat o tom, co se děje v celostátním - a mezinárodním - měřítku. Konverzace z Metal Shopu byla shromažďována v souborech zpráv a poté editována do formy elektronické publikace *Phrack*, což je novotvar vytvořený z „phreak“ a „hack“. Editoři *Phracku* se zajímali o hackery stejně intenzívně, jako se hackeři zajímali o počítače.

Phrack, zajímavé čtení zdarma, se začal šířit undergroundem. Když přešli Taran King a Knight Lightning ze střední školy na vysokou, objevil se *Phrack* na sálových počítačích připojených k síti BITNET, a přes BITNET k Internetu, k oné obrovské volné neziskové síti akademických, vládních a komerčních strojů spojených unixovským protokolem TCP/IP. („Červí“ program „Internet Worm“, napsaný postgraduálním studentem Cornellovy univerzity Robertem Morrisem a vypuštěný 2. listopadu 1988, je dosud největším a nejznámějším případem počítačového skandálu. Podle Morrise měl jeho důvtipně napsaný program neškodně zkoumat Internet, ale v důsledku programátorské chyby se začal nekontrolovatelně množit a zastavil přibližně šest tisíc počítačů Internetu. Méně ambiciózní pronikání do Internetu v malém měřítku bylo pro undergroundovou elitu běžné.) Prakticky každý undergroundový board, který nebyl beznadějně krotký a zaostalý, měl kompletní archiv *Phracku* - a možná i méně známé undergroudové publikace: *Legion of Doom Technical Journal*, drsně obscénní soubory skupiny *Cult of the Dead Cow*, časopisy *P/HUN*, *Pirate*, *Syndicate Reports*, případně silně ideologizovaný anarchistický *Activist Times Incorporated*.

Přítomnost *Phracku* na boardu byla jasným důkazem pohrdání zákony. Zdálo se, že *Phrack* je všude, radící, provokující a šířící étos undergroundu. Něco takového nemohlo uniknout pozornosti bezpečnostních odborníků telekomunikačních společností ani policie.

Tím se dostáváme k citlivému tématu policie a boardů. I policie totiž vlastní boardy. V roce 1989 existovaly boardy sponzorované policií v Kalifornii, Coloradu, na Floridě, v Georgii, Idahu, Michiganu, Missouri, Texasu a Virginii: boardy jako „Crime Bytes“, „Crimestoppers“, „All Points“ a „Bullet-N-Board“. Policisté, jejichž soukromým koníčkem jsou počítače, vlastnili boardy v Arizoně, Kalifornii, Coloradu, Connecticutu, na Floridě, v Missouri, Marylandu, Novém Mexiku, Severní Karolíně, Ohiu, Tennessee a Texasu. Policejní boardy často prokazují svoji užitečnost pro styk s místními obyvateli. Někdy jsou na nich oznamovány i zločiny.

Někdy jsou na nich *páchány* zločiny. Občas se to stane nešťastnou náhodou, když naivní hacker zabloudí na policejní board a bezelstně začne nabízet kradené kódy. Daleko častěji se to ovšem stává na nyní již téměř tradičních *nastražených boardech*. První nastražené boardy byly založeny v roce 1985: „Underground Tunnel“ v Austinu v Texasu, jehož sysop seržant Robert Ansley vystupoval jako „Pluto“, „The Phone Company“ („Telefonní společnost“) ve Phoenixu v Arizoně, řízená Kenem MacLeodem ze šerifova úřadu v Maricopa County a board seržanta Dana Pasqualeho ve Fremontu v Kalifornii. Kolem sysopů těchto boardů, kteří vystupovali jako hackeři, se rychle vytvořil okruh aktivních uživatelů, bez zábran zveřejňujících kradené kódy, vyměňujících si pirátský software a vůbec pilně pracujících na svém vlastním neslavném konci.

Nastražené boardy, stejně jako všechny ostatní, pracují lacino, velice lacino ve srovnání s infiltračními akcemi policie. Jakmile jsou sysopové akceptováni místním undergroundem, jsou zváni na jiné pirátské boardy, kde mohou získat další informace. A když je nástraha zveřejněna a největší hříšníci zatčeni, dostane akce velmi užitečnou publicitu. Následná paranoia v undergroundových kruzích - někteří dávají přednost označení „odstrašující efekt“ - zpravidla místně zastaví porušování zákonů na nezanedbatelnou dobu.

Samozřejmě, policisté nemusí „dělat vlny“. Naopak, mohou tiše rozprostřít sítě. Z hackerů, kteří se do nich chytí, se dají vymačkat informace. Z některých se stanou užiteční pomocníci. Mohou zavést policisty do pirátských boardů po celé zemi.

A na boardech po celé zemi byly špinavé otisky prstů *Phracku*, stejně jako té nejhlasitější a nejdrzejší undergroundové skupiny: „Legion of Doom“.

Název Legion of Doom pochází z komiksů. Legie soudného dne, spiknutí kostýmovaných ultrapadouchů, vedených chromem obrněným zločineckým supermozkem Lexem Luthorem, se staralo Supermanovi o spoustu čtyřbarevných nebezpečných úkolů po několik desítek let. Samozřejmě že Superman, tento vzor Pravdy, Spravedlnosti a Amerických hodnot, nakonec vždycky zvítězil. Hackerům, kteří přijali jméno Legie, to nevadilo - název Legion of Doom neměl vzbuzovat žádné hrozivé či dokonce satanistické asociace, nebyl míněn tak vážně. Byl převzat z komiksů a měl být komický. Ovšem, toto jméno mělo kvalitní zvuk. Legion of Doom - znělo to opravdu dobře. Jiné skupiny, například „Farmers of Doom“, blízcí spolupracovníci LoDu, chápali tento bombastický tón a dělali si z něj legraci. Existovala dokonce hackerská skupina zvaná „Justice League of America“ („Americká liga spravedlnosti“), nazvaná podle Supermanovy strany spravedlivých a hrdinských ochránců zákona.

Ale tyto skupiny zanikly; Legie zůstala. Původní Legion of Doom, uživatelé Quasi Motova boardu Plovernet, byli telefandové. O počítače se nijak zvlášť nezajímali. Sám Lex Luthor (jemuž nebylo ani osmnáct, když založil LoD) byl expertem na COSMOS neboli „Central System for Mainframe Operations“, tedy na vnitřní spojařskou počítačovou síť. Nakonec dosáhl velmi solidní úrovně v pronikání do sálových počítačů IBM, ale přece jen, jakkoli měl Lexe každý rád a obdivoval jeho styl, nebyl obecně považován za opravdu špičkového počítačového kovboje. Nebyl ani autoritativním šéfem Legion of Doom - Legie si nikdy nepotrpěla na formální hierarchii. Jako častý host na Plovernetu a sysop vlastního boardu „Legion of Doom“ byl jejím bubeníkem a personalistou.

Legion of Doom vznikla na troskách dřívější telefandovské skupiny „Knights of Shadow“ („Rytíři stínu“). Později LoD přejala účastníky

hackerské skupiny „Tribunal of Knowledge“ („Tribunál vědění“). Lidé neustále přicházeli a odcházeli, skupiny se štěpily a formovaly se v nich frakce.

V počátcích LoD se jeho telefandovští členové seznámili s několika zájemci o počítače a jejich zabezpečení, kteří založili asociovanou skupinu „Legion of Hackers“. Později se tyto skupiny spojily do „Legion of Doom/Hackers“ neboli LoD/H. Když si původní členové hackerského křídla, pánové „CompuPhreak“ a „Phucked Agent 04“ našli jinou životní náplň, dodatečné „/H“ se z názvu zvolna vytratilo; ale v té době už telefandovské křídlo, pánové Lex Luthor, „Blue Archer“ („Modrý Lučišník“), „Gary Seven“ („Sedma Gary“), „Kerrang Khan“ („Chán Kerrang“), „Master of Impact“ („Mistr zásahů“), „Silver Spy“ („Stříbrný špión“), „The Marauder“ („Nájezdník“) a „The Videosmith“ („Kovář videí“), získalo spoustu zkušeností s ilegálním průnikem do počítačů a stalo se nezanedbatelnou silou.

Členové LoDu instinktivně chápali, že cesta k opravdové moci v undergroundu vede přes samizdatovou publicitu. Legie byla všude. Nejen že byla jednou z prvních skupin, ale její členové si dávali záležet na široké distribuci svých ilegálních vědomostí. Někteří, například Mentor, projevovali horlivost téměř misionářskou. *Legion of Doom Technical Journal* („Technický žurnál LoD“) se začal objevovat na boardech po celém undergroundu.

Název *LoD Technical Journal* je parodií starobylého a důstojného *AT&T Technical Journal*. I obsah těchto dvou publikací byl velice podobný - převzatý z veřejných tiskovin a diskusí mezi spojaři. Ale dravčí tón LoDu dával i těm nejnevinnějším údajům punc zlověstné výzvy a zjevného, akutního nebezpečí.

Abychom pochopili, jak takové přesvědčení vzniká, použijme dva následující (fiktivní) texty k myšlenkovému experimentu.

(A) „W. Fred Brown, viceprezident AT&T pro modernizaci a technický rozvoj, vystoupil 8. května ve Washingtonu na jednání Národní rady pro telekomunikace a Informace (NRTI) se zprávou o projektu RADERS, řešeném společností Bellcore. RADERS (Rozšířená automatizovaná distribuovaná elektronická regulační síť) je nástroj pro programování telefonních ústředen, umožňující vývoj nových telekomunikačních služeb, včetně dvoubodového spojení ve formátu definovaném uživatelem, z každého tlačítkového telefonu a dostupných v několika sekundách. Prototyp RADERS používá pro spojení s minipočítačem centrexové linky a na počítači operační systém Unix.“

(B) „Purpurový blesk 512 z Centrex gangu hlásí: Pánové, ten mrzák co mu Bellcore říká RADERS je prostě k sežrání! Už nepotřebujete ani mizerný Commodore, abyste mohli reprogramovat ústřednu - prostě se připojíte k RADERS jako technik, a můžete reprogramovat přímo z číselníku telefonu, z každé telefonní budky! Můžete mít dvoubodové spojení v uživatelsky definovaném formátu, a co je ze všeho nejlepší, celá ta věc je řízená po naprosto nechráněných centrexových linkách počítačem, na kterém je - držte se - standardní Unix! Jupí!“

Zpráva (A), zahalená v technokratickém newspeaku, je nudná až k nečitelnosti. Málokdo by ji považoval za zlověstnou či nebezpečnou. Na druhé straně zpráva (B) je přímo strašlivá, jednoznačný důkaz hrozivého spiknutí a rozhodně ne ten druh čtiva, jež byste doporučili svému potomkovi. *Informace* v obou zprávách je ale tatáž. Je to *veřejná* informace, předložená federální vládě na veřejném jednání. Není „tajná“. Není „patentově chráněná“. Není dokonce ani „důvěrná“. Naopak, vývoj sofistikovaných softwarových systémů je pro Bellcore věcí, jež má být hrdě prezentována veřejnosti. Ovšem, když Bellcore veřejně oznámí takový projekt, očekává od lidí jistý přístup - něco ve stylu *jů, vy jste ale pašáci, jen v tom pokračujte dál, ať už to je co chce* - a rozhodně ne drzou parodii jejich vlastního oznámení, opovržlivé odfrkávání a divoké spekulace o možných bezpečnostních nedostatcích.

Nyní si představte sami sebe na místě policisty, na kterého se obrátil rozhořčený rodič či představitel telekomunikační společnosti, mávající kopií verze (B). Tento vážený občan objevil ke svému zděšení místní BBS, na které jsou volně dostupné hrozivé materiály podobné (B), jež jeho syn zkoumá s hlubokým a nezdravým zaujetím. Kdyby bylo (B) vytištěno v knize či časopisu, věděl byste, jako ví každý americký strážce zákona, že udělat s tím něco by dalo zatracenou práci; ale člověk nemusí být technický génius, aby pochopil, že je-li ve vašem okrsku počítač s materiály typu (B), budou z toho potíže.

Ve skutečnosti vám každý počítačově gramotný policajt řekne, zeptáte-li se ho, že boardy s materiály typu (B) jsou *zdroj* potíží. A *nejhorší* zdroj potíží jsou vůdci, vymýšlející a rozšiřující materiály typu (B). Kdyby nebylo těchhle vtipálků, *nebyly* by žádné potíže.

A Legion of Doom byla na boardech jako nikdo jiný. Plovernet. Legion of Doom BBS. Farmers of Doom BBS. Metal Shop. OSUNY. Blottoland („Namol“). Private Sector. Atlantis. Digital Logic. Hell Phrozen Over („Zamrzlé peklo“).

Členové LoDu měli i své vlastní boardy. Silver Spy založil board „Catch-22“ („Hlava 22“), považovaný za centrum hackerů, kteří to myslí opravdu vážně. Mentor měl „Projekt Fénix“. Když neřídili vlastní boardy, objevovali se na boardech jiných lidí, vychloubali se, chvástali a naparovali. A kde se neobjevovali osobně, tam přicházely jejich „philes“, plné nebezpečných vědomostí a ještě nebezpečnějších postojů. Již kolem roku 1986 získala policie neurčitý dojem, že *každý* příslušník undergroundu je z LoD. Legie nikdy nebyla tak velká - byla například znatelně menší než „Metal Communications“ či „The Administration“ - ale měla prvotřídní publicitu. Zvláště ve *Phracku*, jež chvílemi vypadal jako fanzin LoDu; a *Phrack* byl všude, a zvlášť v kancelářích bezpečnostních odborů telekomunikací. *Nebylo* přistiženého telefandy, hackera či dokonce jen usmrkaného zloděje kódů nebo počítačového piráta, jehož by se policajti nezeptali, zda není v LoDu.

Takové obvinění bylo obtížné vyvrátit, jelikož Legie nikdy nedistribuovala členské odznaky či legitimace. Kdyby se o to pokusili, pravděpodobně by brzy zanikli, protože odliv členů byl značný. LoD nebyl ani tak technologickým ekvivalentem pouličního gangu jako okamžitým stavem mysli. Byla to „Nesmrtelná banda“. V roce 1990 Legie *vládla* už desátým rokem, a policii připadalo neuvěřitelné, že všem přistiženým členům je teprve šestnáct let. A všichni ti pubescentní začátečníci opakovali tutéž únavnou hackerskou litanii: „prostě zvědavý, žádné kriminální úmysly“. Někde v centru spiknutí přece museli být opravdoví, dospělí šéfové, vedoucí zjevně nekonečný zástup obrýlených kluků z vilových čtvrtí s jedničkami na vysvědčení a legračními účesy.

Nebylo pochyb, že téměř každý zatčený americký hacker bude *znát* LoD. Znali pseudonymy přispěvatelů *Technického žurnálu LoD* a pravděpodobně se učili na boardech LoDu a z jeho zdrojů. Ale nikdy nepotkali žádného člena Legie. Dokonce i někteří lidé, kteří byli skutečně i formálně „členy LoDu“, znali jeden druhého pouze z elektronické pošty a pod pseudonymem. Pro zločinné spiknutí to byla velice neobvyklá organizace. Počítačové sítě a rychlý rozvoj digitálního undergroundu činili situaci velice nepřehlednou a zmatenou.

Navíc reputace v digitálním undergroundu neplynula z ochoty páchat „zločiny“. Reputace byla založena na chytrosti a technických znalostech. Důsledkem zpravidla bylo, že čím *nebezpečnější* hacker, tím *méně* ho bylo možno obvinit z nějakého běžného, snadno stíhatelného zločinu. Někteří hackeři opravdu uměli krást. A někteří hackeři opravdu uměli pronikat do systémů. Ale tyto skupiny se nepřekrývaly, nebo jen málo. Kupříkladu „Emanuel Goldstein“ z *2600* byl většinou lidí z undergroundu považován za hackerského poloboha. Ale Goldsteinovy publikační aktivity byly zcela legální - prostě vydával obskurní časopis a mluvil o politice, sám vůbec do počítačů nevnikal. Když jste se na to pořádně podívali, trávil vlastně Goldstein polovinu času stížnostmi, že počítačová bezpečnost *není dost dobrá* a měla by být drasticky zvýšena!

Opravdu dobří hackeři, kteří měli solidní technické znalosti a respekt undergroundu, nikdy nekradli peníze ani nezneužívali kreditní karty. Mohli telefonovat bez placení - ale často to vypadalo, že umějí získat veškeré spojení, které potřebují, aniž by zanechali jakékoli stopy.

Ti nejlepší hackeři, nejschopnější a nejsystematičtější, nebyli profesionální podvodníci. Běžně vstupovali do cizích počítačů, ale nic neměnili ani nepoškozovali. Nekradli ani hardware - většinou měli zaměstnání, která s ním souvisela, a mohli sehnat veškeré potřebné vybavení levně z druhé ruky. Schopní hackeři, na rozdíl od nezletilých amatérů, nebyli snobové do elegantního či drahého hardwaru. Jejich stroje

byly vyrobené podomácku, plné nestandardních přívěšků, zflikované ze starých beden, čipů a vázacího drátu. Někteří byli dospělí, živili se jako recenzenti softwaru a počítačoví konzultanti a vydělávali si tak slušné peníze. Někteří z nich dokonce *pracovali pro telefonní společnosti* - a *tito* hackeři, nalezení přímo pod sukněmi Ma Bell, nemohli při zátahu v roce 1990 počítat s žádným milosrdenstvím.

V undergroundu je již dlouho článkem víry, že ti nejlepší hackeři nikdy nejsou přistiženi. Jsou prý na to příliš chytří. Nejsou nikdy přistiženi, protože se nikdy nevychloubají, nechvástají a nenaparují. Tito polobohové mohou sledovat provoz na undergroundových boardech (se shovívavým úsměvem), ale sami se ho nikdy nezúčastní. Ti nejlepší hackeři jsou podle legendy dospělí počítačoví specialisté, například systémoví administrátoři sálových počítačů, kteří znají zabezpečení svého stroje skrz naskrz. Ani ti nejlepší hackeři se nemohou dostat do jakéhokoli počítače, který jim přijde do cesty; znalost slabin systému je příliš specializovaná a podstatně závisí na uvažovaném softwaru a hardwaru. Ale když se člověk na plný úvazek zabývá provozem sálového počítače s Unixem nebo VAX/VMS, zvládne jeho zabezpečení odshora dolů. Se svými znalostmi se pak může bez potíží a bez rizika dostat do téměř jakéhokoli jiného Unixu nebo VMS, když o to bude stát. A podle hackerských legend o to samozřejmě stojí, takže to samozřejmě udělá. Akorát kolem toho nedělá velký rozruch. Takže se to nikdy nikdo nedoví.

Stejně tak je v undergroundu článkem víry, že profesionální spojaři zneužívají telefony jako diví. *Samozřejmě* že poslouchají, s kým mluví Madonna telefonem - sakra, *ty bys to nedělal*? Samozřejmě, že si zařizují dálkové hovory zadarmo - cožpak *oni* budou platit, když celý ten krám řídí? Třetím článkem víry je, že každý chycený hacker se může vyhnout přísnému trestu, když se přizná, *jak to udělal*. Hackeři zřejmě věří, že vládní organizace a velké společnosti bloudí v cyberspace jako slepé ryby nebo jeskynní mloci. Myslí si, že tyto velké, ale pateticky hloupé organizace jim budou upřímně vděčné a možná dokonce nabídnou místo v bezpečnostním odboru a velký plat prvotřídnímu hackerovi, který jim zpřístupní geniální strategii svého modu operandi. V případě prominentního člena LoDu „Control-C“ se něco takového skutečně stalo. Control-C dal lovcům z Michigan Bellu pořádně zabrat, a když byl v roce 1987 dostižen, ukázalo se, že je to chytrý a zjevně neškodný mladý fanatik, fascinovaný telefony. Na tom božím světě nebyla šance, že Control-C někdy zaplatí ohromné a víceméně teoretické účty za dálkové hovory prostřednictvím Michigan Bellu. Snadno mohl být obžalován ze zpronevěry či ilegálního vniknutí do počítače, ale nezdálo se, že by to mělo nějaký smysl - fyzicky žádný počítač nepoškodil. Prostě by se přiznal, nejspíš by dostal obvyklé napomenutí, a Michigan Bell by měl spoustu starostí s přípravou obžaloby. Ale kdyby byl zaměstnán, mohl by své známé hackery od Michigan Bellu odradit.

Kající se Control-C byl užitečný. Vystupoval například na interních plakátech Michigan Bellu s důrazným varováním zaměstnancům, aby ničili papírový odpad. Své nejlepší vnitřní informace vždycky získával probíráním popelnic společnosti, ve kterých hledal neopatrně vyhozená užitečná data - tuto činnost nazývají hackeři „trashing“ („odpadování“). Na plakátech byl i jeho vlastnoruční podpis. Control-C se stal v podstatě maskotem Michigan Bellu. A *skutečně* odrazoval ostatní hackery. Malé ryby se bály Control-C a jeho slavných přátel z Legion of Doom. A velké ryby *byly* jeho přátelé a nechtěli mu působit potíže.

Názory na LoD se mohou různit, ale jejich solidarita je nezpochybnitelná. Když „Wasp“ („Vosa“), zjevně nebezpečný a agresivní newyorský hacker, začal ničit sálové počítače Bellcore, Control-C zajistil rychlou a účinnou dobrovolnou pomoc Mentora a georgijského křídla LoD, které tvořili „Prophet“ (čti „profet“ - „Prorok“), „Urvile“ a „Leftist“ („Levičák“). Na Mentorově boardu Projekt Fénix sestavili plán a pomohli spojařům chytit Waspa do pasti - nalákat ho na počítač se záznamníkem a zařízením na sledování volajících. Wasp prohrál, LoD zvítězil. A jak na to byli pyšní!

Urvile, Prophet a Leftist měli pro takovou činnost kvalifikaci, pravděpodobně ještě lepší než schopný Control-C. Pro chlapce z Georgie neměly telefonní ústředny tajemství. I když přišli do Legion of Doom relativně pozdě, byli považováni za jedny z nejlepších hackerů LoDu, za specialisty na ty nejobtížnější systémy. Měli štěstí, že žili v Atlantě či v jejím okolí, v oblasti spravované ospalou a zjevně tolerantní společností BellSouth.

Co se týče bezpečnosti následnických společností Bellu, BellSouth byla hračka. US West (v Arizoně, Skalistých horách a na severozápadním pobřeží) byl drsný a agresivní, pro hackery patrně nejnebezpečnější ze všech telefonních společností. Pacific Bell a kalifornská PacBell byli technicky na výši, moderní a zocelení veteráni válek s losangeleskými telefandy. NYNEX měl tu smůlu, že operoval v New York City, a byl neustále v pohotovosti a připravený skoro na všechno. Dokonce i Michigan Bell, divize následnické společnosti Ameritech, měl aspoň tolik rozumu, aby si najal hackera jako užitečného strašáka. Ale BellSouth, jakkoli jeho reklama tvrdila, že má „Všechno, co očekáváte od těch nejlepších“, nestál za nic.

Když se zprávy o hrátkách LoDu v georgijských ústřednách dostaly přes Bellcore a neformálními kanály bezpečnostních expertů do BellSouth, nejdříve jim odmítli uvěřit. Kdybyste si všímali každé pověsti o těchhle a od těchhle klukovských hackerů, museli byste se věnovat všem možným z prstu vycucaným nesmyslům: že National Security Agency (tajná služba, jejímž úkolem je analyzovat elektronické komunikace mimo USA, luštit vojenské i jiné šifry a garantovat bezpečnost amerických šifer) monitoruje všechny telefonní hovory v Americe, že CIA a DEA (tajná služba potírající obchod s drogami) sledují provoz na BBS pomocí programů analyzujících texty, že Kondor mohl zahájit třetí světovou válku z veřejného telefonu.

Jestli byli nějací hackeři v ústřednách BellSouth, jak to, že se nic nedělo? Nic nebylo poškozeno. Počítače BellSouth nepadaly. Ztráty BellSouth z defraudací nebyly nijak mimořádné. Zákazníci BellSouth si nestěžovali. Společnost BellSouth měla ředitelství v Atlantě, v ambiciózní metropoli amerického jihozápadu, který se profiloval jako nové technologické centrum; vylepšovala svoji síť na plný plyn a digitalizovala napravo nalevo. Nemohla být považována za lenivou či naivní. Experti BellSouth nepotřebovali, aby je někdo učil řídit telefonní síť, děkujeme pěkně.

A pak došlo k floridskému skandálu.

13. června 1989 zjistili volající do úřadu kurátora Palm Beach County v Delray Beach na Floridě, že kupodivu mluví se sexuální pracovnicí jménem „Tina“ ve státě New York. *Každé* zavolání do tohoto úřadu kurátora blízko Miami bylo jakýmsi magickým způsobem okamžitě přesměrováno přes hranice státu, bez přirážky pro volajícího, na pornografickou horkou linku vzdálenou stovky mil!

Takový kanadský vtip se na první poslech může zdát velice legrační, a telefandovské kruhy si ho také patřičně vychutnaly - přidalo se i číslo *2600* z podzimu 1989. Ale pro Southern Bell (divizi společnosti BellSouth, obhospodařující místní hovory na Floridě, v Georgii a v Severní a Jižní Karolíně) to byla krvavá stopa. Poprvé se stalo, že nějaký hacker pronikl do telefonní ústředny BellSouth a reprogramoval ji!

To si aspoň v BellSouth mysleli v červnu 1989. Ve skutečnosti si členové LoDu hráli v ústřednách BellSouth od září 1987. Žertík ze 13. června - propojení jednoho čísla na jiné úpravou softwaru ústředny - byla dětská hračka pro hackery tak schopné jako křídlo LoDu z Georgie. Propojit hovory přes hranice státu znělo hrozně složitě, ale ve skutečnosti si to vyžádalo pouhé čtyři řádky kódu. Stejně snadné, jen diskrétnější, bylo propojit cizí číslo ke svému vlastnímu telefonu. Když jsi byl pečlivý a opatrný a vyměnil posléze software za původní, nedozvěděla se o tom ani živá duše.

Kromě tebe. A těch, kterým ses s tím pochlubil.

Co se týkalo BellSouth, co oči neviděly, srdce nebolelo. Až na to, že teď někdo celou věc veřejně demonstroval, a v BellSouth uviděli. Probuzený a značně paranoidní BellSouth začal prohledávat ústředny jednu po druhé a pátrat po známkách ilegálních průniků, celé horké léto roku 1989. Ne méně než čtyřicet dva zaměstnanců BellSouth sloužilo dvanáctihodinové směny, čtyřiadvacet hodin denně po dva měsíce a

věnovalo se studiu záznamů, monitorování počítačů a hledání jejich ilegálního použití. Těchto čtyřicet dva přepracovaných expertů bylo známo jako „Intrusion Task Force“ („Operační skupina pro průniky“) společnosti BellSouth.

Výsledky vyšetřování byly pro spojaře neuvěřitelné. Neveřejné telefonní databáze byly modifikovány: odnikud se vynořila telefonní čísla bez jmen uživatelů a bez adres. A co bylo možná ještě horší, bez záznamů o používání a bez účtů. Nová digitální diagnostická služba ReMOB (zkratka z Remote Observation čili „vzdálené pozorování“) byla zmanipulována - hackeři se naučili upravovat software ReMOB, takže mohli poslouchat každý hovor procházející ústřednou, kdykoli se jim zachtělo! Používali majetek telekomunikací *ke špionáži*!

Senzační zpráva se v roce 1989 rozšířila do policejních jednotek. Nikoho v BellSouth nikdy nenapadlo, že jejich skvělé, zbrusu nové digitální ústředny mohou být *reprogramovány*. Spojaři zjevně upřímně žasli, že někdo může mít tu drzost. Samozřejmě že ústředny byly počítače, a každý věděl, že hackeři rádi vnikají do počítačů; ale počítače v telefonních ústřednách byly *jiné* než počítače normálních lidí.

Důvody, *proč* vlastně tyto počítače byly „jiné“, nebyly příliš dobře definovány. Určitě se nelišily zvýšenou bezpečností. Bezpečnost počítačů BellSouth nestála za nic. Počítače AIMSX, například, neměly ani hesla. Ale nebylo pochyb o tom, že v BellSouth si byli *jistí*, že jejich počítače jsou jiné. A jestli byli kolem nějací kriminálníci, kteří to nechtěli pochopit, byl BellSouth odhodlán přesvědčit je o tom.

Konec konců, ústředna 5ESS nebyla žádná databáze místního zahradnictví. Na těchto ústřednách závisely služby veřejnosti. Závisela na nich *bezpečnost státu*.

A číhající hackeři, naslouchající a reprogramující, mohli sledovat všechny hovory v daném místě! Mohli poslouchat hovory představitelů telekomunikací. Mohli poslouchat hovory z policejních stanic! Mohli poslouchat hovory místních úřadoven Tajné služby USA!

V roce 1989 začali policisté zabývající se telefony a lovci hackerů používat telefony kódující hlas a chráněné linky. Bylo to logické opatření. Nikomu nebylo jasné, kdo všechno pronikl do systému. Ať už byli kdokoli, šel z nich strach. Provozovali novou formu protispolečenské aktivity. Mohli to být západoněmečtí hackeři placení KGB. To také vypadalo jako groteskně přehnaná představa, dokud Clifford Stoll nepřiměl línou washingtonskou policejní byrokracii, aby zahájila šetření průniku do počítače, ze kterého se vyklubalo přesně tohle - *hackeři placení KGB*! Stoll, systémový administrátor internetovské laboratoře v Berkeley v Kalifornii, skončil na titulní straně New York Times jako národní hrdina prvního skutečného případu mezinárodní počítačové špionáže. Stollova kontrašpionážní akce, kterou v roce 1989 popsal v populární knize *Kukaččí vejce*, potvrdila, že činnost hackerů je skutečně potenciální hrozbou pro národní bezpečnost Spojených států. Tajná služba USA nepřešlapuje na místě, když zjistí nebezpečí akce cizí špionážní organizace. Telefony kódující hlas a chráněné linky Tajné služby USA představovaly vážnou překážku pro normální průběh policejních operací; překážku šíření informací, kooperace a předcházení nedorozuměním. Ale v roce 1989 se nezdálo, že je vhodná doba na polovičatá opatření. Jestliže policie a Tajná služba samy nepracovaly bezpečně, jak by mohly seriózně vyžadovat bezpečnostní opatření v soukromém sektoru? Potíže přinejmenším upozornily lidi na to, jak je hrozba vážná.

Bylo-li třeba poslední kapky, aby pohár klidu policie přetekl, stalo se jí zjištění, že i systém 911, tedy systém tísňového volání, je zranitelný. Systém 911 má vlastní specializovaný software, ale používá tytéž digitální ústředny jako zbytek telefonní sítě. Fyzicky se neliší od běžných telefonů. Ale samozřejmě se liší logicky; toto území v cyberspace je rezervováno pro policii a nouzová volání. Policista hlídající vaši ulici nemusí vědět mnoho o hackerech a telefandech. Lidi kolem počítačů jsou prostě divní; dokonce i *policajti* kolem počítačů jsou dost divní - je těžké si představit, čím se vlastně zabývají. Ale hrozba systému 911 je všechno, jen ne abstraktní. Jestliže selže systém 911, lidé mohou zemřít.

Představte si, že se dostanete z havarovaného vozu, dovrávoráte k telefonní budce, vytočíte 911 a uslyšíte „Tinu“, která zvedla sluchátko někde v New Yorku! Tahle situace už není nijak komická.

A mohlo se něco takového stát? Bezpochyby. Hackeři zaútočili na systém 911 už v minulosti. Telefandové dokáží shodit systém 911 prostě tím, že na něj poštvou několik modemů, koordinovaně vytáčejících jeho číslo, až se zahltí. To je velmi primitivní a hrubý postup, ale stále natolik funkční, aby vzbuzoval obavy.

Doba dozrála k akci. Nastal čas přijmout přísná opatření proti undergroundu. Nastal čas začít sbírat kostky skládačky, volné konce klubka, vychloubačné řeči při různých příležitostech. Nastal čas začít shromažďovat materiály a dát se do práce na novém případu. Hackeři nebyli „neviditelní“. *Mysleli si*, že jsou neviditelní; ale ve skutečnosti si jich jen příliš dlouho nikdo nevšímal.

Pod systematickým policejním tlakem v létě roku 1989 se digitální underground začal hroutit jako nikdy předtím.

První velký úspěch se dostavil velmi brzy: už za měsíc, v červenci 1989. Byl dopaden autor propojení na linku „Tiny“ a přiznal se. Jmenoval se „Fry Guy“ („Smažák“), bylo mu 16 let a pocházel z Indiany. Fry Guy byl skrz naskrz zkažený mladý muž.

Fry Guy si vysloužil svou přezdívku žertíkem v rychlém občerstvení. Ukradl heslo vedoucího místního MacDonaldu a připojil se na sálový počítač MacDonaldu v systému Sprint Telenet. Jménem vedoucího změnil záznamy MacDonaldu a zařídil několika svým nezletilým přátelům, přivydělávajícím si prodejem hamburgerů, velkorysé zvýšení platu. Nebyl přistižen.

Povzbuzen úspěchem, zkusil Fry Guy zneužívat kreditní karty. Měl značné konverzační schopnosti a navíc vlohy pro „sociální inženýrství“. Když ovládáte „sociální inženýrství“ - umění vydávat se za někoho jiného a rychlým a sebejistým projevem prodat nějaký podfuk - je zneužívání kreditních karet snadné. (Dlouhodobě se vyhnout dopadení je něco jiného.)

Na ALTOS Chat boardu v německém Bonnu se Fry Guy potkal s Urvilem z Legion of Doom. ALTOS Chat byl sofistikovaný board, přístupný přes globální sítě jako BITnet, Tymnet a Telenet. ALTOS byl oblíbeným boardem členů německé skupiny Chaos Computer Club. Dva hackeři z tohoto klubu, kteří se na ALTOSu často vyskytovali, „Jaeger“ („Lovec“) a „Pengo“, byli hlavními protagonisty Stollova případu „kukaččího vejce“. Ve Východním Berlíně se scházeli s agentem KGB, který jim platil za pronikání do amerických počítačů přes Internet. Když si členové LoDu přečetli ve Stollově knize popis Jaegerových akcí, nebyli z technického hlediska nijak ohromeni. Na tehdy oblíbeném boardu LoDu jménem „Black Ice“ („Černý led“) se vytahovali, že oni sami by zvládli to co Chaos Computer Club během jediného týdne! Nicméně reputace německé skupiny na ně přece jen udělala dojem; oceňovali divokou odvahu zkouřených anarchistických hackerů, jednajících s obávanými bossy mezinárodní komunistické špionáže. Členové LoDu si občas vyměňovali informace se sympatickými německými hackery na ALTOSu - například telefonní čísla zranitelných počítačů VAX/VMS v Georgii. Telefandové z Holandska a Anglie a také australské skupiny „Phoenix“, „Nom“ a „Electron“ byli na ALTOSu stálými hosty. V undergroundových kruzích byla přítomnost na ALTOSu známkou elitních kvalit, symbolem sofistikovaného hackera z mezinárodní lepší společnosti.

Fry Guy se rychle naučil získávat informace z agentur informujících o uživatelích kreditních karet. Ve svých poznámkách měl více než stovku ukradených čísel kreditních karet a tisíce kradených přístupových kódů pro dálkové telefonní hovory. Věděl, jak se dostat na ALTOS a jak mluvit řečí undergroundu. Začal na ALTOSu mámit znalosti o tricích s ústřednami od Urvila.

Kombinací těchto znalostí se Fry Guy vyšvihl k nové formě krádeže po telefonu. Nejprve dostal z počítačů společnosti nabízející kreditní karty jejich čísla. Zkopírovaná data obsahovala jména, adresy a telefonní čísla náhodně vybraných držitelů karet.

Pak Fry Guy, vydávající se za majitele karty, zavolal Western Union a požádal o vyplacení hotovosti z účtu „své“ kreditní karty. Western Union pro zajištění bezpečnosti zavolal zákazníka zpět domů a požádal o potvrzení transakce.

Ale stejně jako zaměnil úřad kurátora na Floridě za „Tinu“ v New Yorku, zaměnil Fry Guy číslo držitele karty za místní telefonní budku.

Pak se usadil za větrem a zahladil svoji stopu směrováním a přesměrováním hovoru přes vzdálené ústředny, třeba i v Kanadě. Když byl hovor spojen, suverénně přesvědčil zástupce Western Unionu, že je legitimním držitelem karty. Protože odpověděl na zavolání na správné telefonní číslo, nebylo to ani tak těžké. A peníze Western Unionu byly zaslány jeho společníkovi v jeho rodném městě v Indianě.

Fry Guy a jeho pomocníci ukradli pomocí technik LoDu Western Unionu od prosince 1988 do července 1989 šest tisíc dolarů. Přilepšovali si i objednáváním zboží na ukradená čísla kreditních karet. Fry Guy byl opilý úspěchem. Šestnáctiletý kluk se svým hackerským konkurentům vychloubal fantastickými příběhy, tvrdil, že si za nakradené peníze najal limuzínu a vyjel si na výlet po Spojených státech ve společnosti groupie své oblíbené heavymetalové skupiny Motley Crue. Rozjařený vědomostmi, mocí a lehce získanými penězi se Fry Guy pustil do obvolávání místních zástupců bezpečnostního odboru Indiana Bellu, aby se vychloubal, chvástal, naparoval a pronášel zlověstné předpovědi o tom, jak jeho mocní přátelé z nechvalně známé Legion of Doom dokáží shodit celostátní telefonní síť. Fry Guy jmenoval dokonce i datum plánované akce: státní svátek 4. července.

Důsledkem těchto flagrantních projevů koledování si o zatčení bylo jeho brzké zadržení. Když indianská telefonní společnost zjistila, kdo je Fry Guy, instalovala Tajná služba USA na jeho domácí linku tzv. záznamníky vytáčených čísel („Dialed Number Recorders“ čili DNR). Tato zařízení nejsou odposlouchávací, nemohou zaznamenat obsah telefonních hovorů, ale zaznamenávají všechna telefonní čísla, na která jsou spojovány hovory dovnitř i ven. Sledování těchto čísel prokázalo, že Fry Guy intenzivně používá kradené kódy pro přístup k dálkovým linkám, jeho rozsáhlé styky s pirátskými boardy a odhalilo i jeho četné osobní hovory s přáteli z LoDu v Atlantě. 11. července 1989 už měli i Prophet, Urvile a Leftist na svých linkách instalované DNR Tajné služby.

Tajná služba USA se objevila v domě Fry Guye 22. července 1989, k hrůze jeho nic netušících rodičů. Komando bylo vedeno zvláštním agentem z úřadovny Tajné služby v Indianapolisu. Ale bylo také doprovázeno a instruováno Timothy M. Foleym z úřadovny Tajné služby v Chicagu (což je muž, o kterém ještě hodně uslyšíme).

Podle standardního postupu federální policie při vyšetřování počítačového zločinu, etablovaného od počátku 80. let, prohledala Tajná služba důkladně celý dům a zabavila veškeré nalezené počítačové vybavení a záznamy. Veškerá technika Fry Guye byla odnesena pryč a převzata do úschovy Tajnou službou, což účinně znemožnilo jeho další výboje.

Tajná služba USA Fry Guye důkladně vyslechla. Jeho případ byl svěřen Deboře Danielsové, federální prokurátorce Severní Indiany. Fry Guy byl obžalován z jedenácti případů počítačových podvodů, neoprávněných přístupů k počítači a telefonických podvodů. Důkazy byly četné a nevyvratitelné. Fry Guy sám obvinil ze svého uklouznutí po šikmé ploše Legion of Doom a nabídl se, že proti nim bude svědčit.

Fry Guy trval na tom, že Legie měla v úmyslu shodit telefonní systém v den některého státního svátku. A když se AT&T zhroutila v den výročí Martina Luthera Kinga, získalo tím jeho tvrzení takovou důvěryhodnost, že skutečně zneklidnilo bezpečnostní odborníky telekomunikačních společností i Tajnou službu USA. Fry Guy se nakonec 31. května 1990 v plném rozsahu přiznal. 14. září byl podmínečně odsouzen s podmínkou na čtyřicet čtyři měsíců a čtyři sta hodin veřejně prospěšných prací. Mohl dopadnout mnohem hůř, ale žalobci považovali za rozumné nebýt na nezletilého hříšníka příliš přísní a místo toho se soustředit na nechvalně známé vůdce z Legion of Doom. Jenže případ proti LoDu měl vážné slabiny. Přes velkou snahu vyšetřovatelů bylo nemožné prokázat, že Legie způsobila kolaps z 15. ledna, protože ve skutečnosti s ním neměli nic společného. Vyšetřování v roce 1989 prokázalo, že někteří členové Legion of Doom měli větší schopnosti ovládat telefonní ústředny než všichni telefandové před nimi a že se aktivně angažovali ve spikleneckých aktivitách, jejichž cílem bylo získat schopnosti ještě větší. Vyšetřovatelé byli přesvědčeni, že Legie měla v úmyslu svých znalostí strašlivým způsobem zneužít, ale pouhé zlovolné záměry k jejich odsouzení nestačily.

A ačkoli Atlantská trojka - Prophet, Leftist a zvláště Urvile - naučila Fry Guye dost, sami nebyli podvodníci s kreditními kartami. Jediná věc, kterou „ukradli“, byly dálkové hovory - a protože většinou k tomu používali manipulaci s ústřednami, nebylo jednoduché posoudit, kolik „ukradli“, a dokonce ani jestli jejich činnost vůbec byla krádeží v běžném smyslu slova.

Fry Guy a jeho krádeže přístupových kódů přišly telefonní společnosti na pěkné peníze. Krádež dálkového spojení může být považována za čistě teoretickou „ztrátu“, ale zrušení všech ukradených kódů a vydání nových jejich nevinným majitelům stojí opravdový čas a opravdové peníze. I majitelé kódů mají potíže a ztrácejí takovou operací čas, peníze i duševní klid. Muselo být postaráno i o držitele zneužitých kreditních karet a o Western Union. Co se týkalo peněz, byl Fry Guy mnohem větší zloděj než LoD. Pouze z hlediska počítačových vědomostí byl Fry Guy malá ryba.

Pro atlantskou Legii byla většina pravidel cyberspace dobrá jen pro neschopné trouby, ale jistá pravidla *měli*. Nikdy nic nezničili a nikdy si nevzali peníze. To byla dost hrubá a nespolehlivá pravidla, neadekvátní pro etické jemnosti v cyberspace, nicméně umožňovala Atlantské trojce pracovat s relativně čistým svědomím (ale nikdy ne s klidnou myslí).

Když jsi nepronikal do počítačů pro finanční zisk, když jsi nekradl lidem skutečné peníze - tedy peníze z bankovního konta - nikomu se podle názoru LoDu *nic nestalo*. „Krádež služeb“ byl výmysl a „intelektuální vlastnictví“ špatný vtip. LoD se díval na podvodníky, „pijavice“ a zloděje s elitářským pohrdáním. Sami sebe považovali za čestné.

Podle jejich názoru bylo nefér nazývat lidi, kteří neničili žádné systémy (tedy, ne úmyslně, vždycky se může vloudit chybička, zeptejte se třeba Roberta Morrise) „vandaly“ či „gangstery“. Když jsi se bavil on-line se svými „kámoši“ z bezpečnostního odboru, mohl ses na ně dívat svrchu, z vyšší úrovně hackerské morálky. A z policie sis mohl dělat legraci z - pro ně nedostupné - slonovinové věže hackerské touhy po čistém vědění.

Ovšem z hlediska mužů zákona a telekomunikační bezpečnosti nebyl doopravdy nebezpečný Fry Guy. Nebezpečná byla Atlantská trojka. Nešlo o zločiny, které páchali, ale o *nebezpečí*, o potenciální riziko, o sumu *technické moci*, kterou LoD nashromáždil a jež nemohla být ponechána bez povšimnutí.

Fry Guy nebyl členem LoD. Nikdy nespatřil nikoho z LoDu; jeho jediný kontakt s nimi byl elektronický. Členové jádra Legion of Doom pořádali přibližně každý rok svůj sraz - pozdravili se, společně se opili, dali si pizzu a v hotelovém pokoji uspořádali divoký mejdan. Fry Guy nikdy nic takového neudělal. Debora Danielsová ho výstižně popsala jako „aspiranta na členství v LoDu“.

Ale zločiny Fry Guye byly ve většině následné policejní propagandy připisovány LoDu. LoD byl popisován jako „těsně spolupracující skupina“, zabývající se „početnými ilegálními aktivitami“, včetně „krádeží z cizích kont a jejich modifikací“ a „podvodného získávání peněz a zboží“. Fry Guy to dělal, ale Atlantská trojka nikoli; o krádeže se prostě nezajímali, zajímali se o pronikání do počítačů. To vedlo k podivným konstrukcím ve strategii obžaloby. Členové LoDu byli obviněni z „šíření informací o útocích na počítače mezi ostatní počítačové hackery, aby tak přesunuli pozornost policie k těmto jiným hackerům, pryč od Legion of Doom“.

Toto poslední obvinění (převzaté přímo z tiskové zprávy „Chicago Computer Fraud and Abuse Task Force“) zní zvlášť vykonstruovaně. Po jeho přečtení můžeme dospět k závěru, že vyšetřovatelé by udělali velice dobře, kdyby opravdu „přesunuli pozornost“ od Legion of Doom. Možná, že by se *měli* soustředit na „tyto jiné hackery“ - na ty, kteří skutečně kradli peníze a nakupovali bez placení.

Ale Zátah na hackery v roce 1990 nebyl obyčejnou policejní akcí. Nešlo v něm jen o běžné udržování pořádku v cyberspace - byla to *razie*, akce vymyšlená k přistižení špiček undergroundu, k vyslání zřetelné a výhružné zprávy, která by zarazila undergroundový rej jednou provždy.

Z tohoto hlediska nebyl Fry Guy o moc víc než elektronický ekvivalent malého pouličního prodejce drog. Dokud byly mozky hackerských akcí z LoDu na svobodě a aktivní, rozhazující ilegální vědění napravo nalevo a povzbuzující radost z otevřeného porušování zákonů, byl zaručen *neomezený přísun* hříšníků, jako byl Fry Guy.

Protože si LoD dával záležet na své popularitě, zanechal stopy na mnoha místech. Policisté v New Yorku, Indianě, na Floridě, v Texasu, Arizoně, Missouri a dokonce i v Austrálii se po nich pustili. Ale v roce 1990 byla válka s Legií řízena z Illinois, skupinou Chicago Computer Fraud and Abuse Task Force.

Chicago Computer Fraud and Abuse Task Force („Chicagská operační skupina proti počítačové zpronevěře a zneužití počítače“), vedená federálním žalobcem Williamem J. Cookem, zahájila činnost v roce 1987 a rychle se stala jednou z nejiniciativnějších místních „jednotek pro boj s počítačovým zločinem“. Chicago bylo pro takovou skupinu přirozenou základnou. První BBS na světě byla vymyšlena v Illinois. Stát Illinois měl jedny z nejstarších a nejpřísnějších zákonů o počítačových zločinech v Americe. Policie v Illinois si byla velmi dobře vědoma nebezpečí „zločinů bílých límečků“ a počítačových podvodů.

A William J. Cook byl mezi lovci elektronických zločinců vycházející hvězdou. On a jeho kolegové z úřadu federální prokuratury USA v Chicagu měli úzké vztahy s Tajnou službou, zvláště s aktivním chicagským agentem Timothy Foleym. Cook a jeho kolegové z Ministerstva spravedlnosti plánovali strategii a Foley byl jejich mužem akce.

V průběhu 80. let vybavila federální vláda veřejné žalobce sadou nových, nevyzkoušených nástrojů pro potírání počítačového zločinu. Cook a jeho kolegové byli prvními, kdo použil nové paragrafy v praxi, ve skutečném boji ve federální soudní síni.

2. října 1986 Senát jednomyslně přijal Zákon o počítačové zpronevěře a zneužití počítače, ale existovalo politováníhodně málo rozsudků, které se na něj odvolávaly. Cookova skupina si zvolila jméno podle tohoto zákona, protože byla odhodlána transformovat tento mocný, ale spíše teoretický akt Kongresu do prakticky užitečného nástroje soudního boje proti počítačovým podvodníkům a delikventům.

Nešlo jen o pouhé odhalování zločinů, jejich vyšetřování a následné souzení a potrestání pachatelů. Chicagská skupina, jako téměř každý, kdo se o to zajímal, již *věděla*, kdo je jejím nepřítelem: Legion of Doom a autoři a redaktoři *Phracku*. Úkolem bylo najít legální prostředky, jak tyto osoby odstranit.

Takový přístup se člověku neobeznámenému s tvrdou realitou prokurátorské práce může zdát poněkud pochybný. Ale veřejní žalobci nedostávají lidi do vězení za zločiny, které spáchali; dostávají lidi do vězení za zločiny, které spáchali *a které jim před soudem mohou být prokázány*. Chicagská federální policie dostala do vězení Al Capona za daňový únik. Chicago je velkoměsto s tradicí drsných a účinných metod na obou stranách hrany zákona.

Fry Guy vyprovokoval vyšetřování a upozornil bezpečnostní odborníky telekomunikací na rozsah problému. Ale zločiny Fry Guye nemohly dostat za mříže Atlantskou trojku - a tím méně pochybné undergroundové žurnalisty z *Phracku*. Takže 22. července 1989, týž den, kdy byl dopaden Fry Guy v Indianě, se Tajná služba USA vrhla na Atlantskou trojku.

Takový vývoj byl pravděpodobně nevyhnutelný. V létě 1989 se policisté blížili k Atlantské trojce aspoň ze šesti směrů najednou. Za prvé k nim vedly stopy od Fry Guye, jehož sledování vedlo k instalaci DNR záznamníků na jejich telefonech. Tyto záznamníky samy o sobě by je dříve či později zlikvidovaly.

Ale za druhé, o svých známých z Atlanty věděl Control-C a jeho zaměstnavatelé z bezpečnostního odboru. Kontakty LoDu s bezpečnostními odborníky telekomunikací jim daly přílišnou sebedůvěru a ještě větší vychloubačnost, než byla pro ně obvyklá; mysleli si, že mají mocné přátele na vysokých místech a jsou telekomunikačními společnostmi otevřeně tolerováni. Ale Intrusion Task Force z BellSouth jim byla na stopě a nešetřila úsilím ani náklady.

Atlantská trojka měla také pod svými pravými jmény záznamy v rozsáhlých antihackerských souborech, které udržoval a prodával soukromý vyšetřovatel John Maxfield z Detroitu. Maxfield, který měl těsné vztahy s bezpečnostními odborníky telekomunikačních společností a mnoho informátorů v undergroundu, byl pro redakci *Phracku* veřejným nepřítelem číslo jedna, a jejich odpor byl vzájemný.

Atlantská trojka psala články pro *Phrack*. Takové vychloubání nemohlo uniknout pozornosti bezpečnostních odborníků ani policie.

„Knightmare“ („Rytířská můra“), hacker studující střední školu v Arizoně, byl blízký přítel a učedník atlantského LoDu, ale byl dopaden slavnou arizonskou jednotkou Organized Crime and Racketeering Unit. Knightmare byl uživatelem na několika oblíbených boardech LoDu - zejména na „Black Ice“ - a znal mnohá jejich tajemství. A být pronásledován Gail Thackerayovou, pomocným státním zástupcem státu Arizona, představovalo pro každého hackera strašlivé nebezpečí.

A co bylo možná nejhorší ze všeho, Prophet udělal velkou chybu, když předal ilegálně zkopírovaný soubor společnosti BellSouth Knight Lightningovi, který ho publikoval ve *Phracku*. Jak ještě uvidíme, byl to čin, jež měl fatální následky téměř pro všechny zůčastněné.

22. července 1989 navštívila Tajná služba USA Leftistův dům, kde bydlel se svými rodiči. Silný oddíl asi dvaceti mužů obklíčil budovu: Tajná služba USA, federální šerifové, místní policie, možná bezpečnostní odborníci BellSouth; v tom davu to bylo těžké poznat. Leftistův tatínek, pracující ve své suterénní kanceláři, si nejdříve ze všeho všiml svalnatého cizince v civilu běžícího přes zadní dvorek s pistolí v ruce. Když do domu vtrhli další cizinci, přirozeně předpokládal, že se stal obětí ozbrojené loupeže.

Jako většina rodičů hackerů, měli i Leftistova maminka a tatínek jen velmi matnou představu, co jejich syn celý čas dělá. Leftist měl práci jako opravář počítačového hardwaru. Jeho fascinace počítači se zdála trošku divná, ale docela neškodná a pravděpodobně vedoucí k dobře placené kariéře. Drasticky náhlá razie způsobila Leftistovým rodičům šok.

Leftist sám si vyšel po práci se svými spolupracovníky na pár skleniček tequily. Jak se na alkoholem poněkud znejistělých nohou a s taškou plnou disket v ruce blížil k domovu, všiml si velkého množství neoznačených aut zaparkovaných na příjezdové cestě. Všechny měly malé mikrovlnné anténky.

Příslušníci Tajné služby vyrazili dveře z pantů, přičemž málem zarazili jeho maminku do zdi.

Uvnitř byl Leftist uvítán zvláštním agentem Jamesem Coolem z atlantské úřadovny Tajné služby USA. Leftist nevěřil svým uším. Ještě nikdy se nesetkal s agentem Tajné služby. Vůbec si nedokázal představit, že někdy udělal něco hodného federální pozornosti. Vždycky si myslel, že stanou-li se jeho aktivity netolerovatelnými, některý z jeho kontaktů v telekomunikačních společnostech mu soukromě zatelefonuje a řekne mu, aby si dal pohov.

Ale místo toho byl Leftist s profesionální rázností prohledán, zda u sebe nemá zbraň, a jeho taška s disketami byla bleskurychle zabavena. On i jeho rodiče byli odvedeni do různých místností a důkladně vyslýcháni, zatímco houfy policistů hledaly po celém domě všechno, co mělo něco společného s elektronikou.

Leftist byl zděšen, když jeho milovaný osobní počítač IBM AT se čtyřicetimegabytovým pevným diskem, stejně jako jeho nedávno koupený klon IBM 80386 s fantastickými sto mega na disku zmizely v domovních dveřích do úschovy Tajné služby. Zabavili také všechny jeho diskety, poznámkové bloky a ohromnou haldu telekomunikačních dokumentů s oslíma ušima, které Leftist vytahal z různých popelnic.

Leftist si myslel, že celá věc je jedno velké nedorozumění. Nikdy se nezajímal o *vojenské* počítače. Nebyl *špión* ani *komunista*. Byl prostě starý dobrý georgijský hacker, a teď si jen přál, aby všichni ti lidi už konečně vypadli. Ale zdálo se, že nehodlají odejít, dokud jim něco neřekne.

Takže se jim svěřil. Což, jak později prohlásil ze svého federálního vězení v Talladeze v Alabamě, byla velká chyba.

Oblast Atlanty byla výjimečná tím, že v ní žili tři členové Legion of Doom na víceméně jednom místě. Na rozdíl od zbytku LoDu, který se scházel po telefonu a na počítačích, atlantští členové skutečně *byli* „těsně spolupracující“. Nebylo nic divného na tom, že agenti Tajné služby USA zadržující Urvila v počítačových laboratořích Georgijské technické univerzity našli v jeho společnosti i Propheta.

Urvile, jedenadvacetiletý student chemie polymerů na Georgijské technické univerzitě, byl pro policisty velmi neobvyklým případem. Urvile - známý také jako „Necron 99“ i pod jinými jmény, která měnil přibližně každý měsíc - byl jak zkušený hacker, tak fanatický hráč her na hrdiny.

Hry na hrdiny jsou neobvyklý koníček; ale hackeři jsou neobvyklí lidé, a jejich oblíbená hobby často nejsou běžná. Nejznámější americkou hrou na hrdiny je patrně „Dungeons & Dragons“ [v Čechách Dračí doupě - pozn. překl.], pokojová hra pro několik hráčů, hraná na papíře, s mapami, pery, statistickými tabulkami a několika podivně tvarovanými hracími kostkami. Účastníci představují hrdinské postavy, zkoumající vymyšlený fantastický svět. Hry na hrdiny se často odehrávají v pseudostředověkých světech „meče a magie“, s čaroději pronášejícími kletby, rytíři v brnění, jednorožci, draky, démony a skřety.

Urvile a jeho spoluhráči dávali přednost technologickým fantaziím. Používali herní systém „G.U.R.P.S.“ čili „Generic Universal Role Playing System“ („Obecný univerzální systém her na hrdiny“), vytvořený firmou „Steve Jackson Games“ (SJG).

„G.U.R.P.S.“ byl rámec pro vymýšlení široké škály fantastických světů. SJG publikovala široký výběr knih plných detailních informací a herních plánů, používaných pro vyplnění mnoha fantastických pozadí základní struktury GURPS. Urvile používal zejména dvě knihy SJG, *GURPS High-Tech* a *GURPS Special Ops* („Zvláštní agenti“).

Ve fantastickém světě *GURPS Special Ops* se hráči zúčastnili moderní „velké hry“ intrik a mezinárodní špionáže. Na počátku hry začínali malí a bezmocní, třeba jako pěšáci CIA nebo mrňaví obchodníčci se zbraněmi. Ale jak pokračovali v sérii her (jedna hra zpravidla trvala několik hodin a tvořila část dlouhého, promyšleného příběhu, který se mohl rozvíjet po celé měsíce), získávali nové dovednosti, nové vědomosti a novou moc. Učili se a trénovali nové schopnosti, například střelbu, karate, odposlouchávání telefonů, otvírání zámků. Mohli také získat imaginární objekty, třeba Beretty, šejkry na Martini či rychlé vozy s katapultovacími sedadly a kulomety ve světlometech. Jak se při komplexnosti těchto her dalo očekávat, Urvilovy herní poznámky byly velice detailní a rozsáhlé. Urvile byl „Pánem jeskyně“, tedy tvůrcem scénářů pro ostatní hráče. Psal ohromné hádanky ve formě dobrodružných příběhů, které ostatní hráči luštili. Urvilovy herní poznámky obsahovaly desítky stránek plných exotických výmyslů o útocích nindžů na Libyi a průnicích do tajných superpočítačů komunistické Číny. Jeho poznámky byly psány na starých listech papíru a ukládány v kroužkových blocích.

Nejdostupnějším starým papírem v Urvilově pokoji na koleji byly haldy výpisů a dokumentů společnosti BellSouth, které vybral z jejích popelnic. Jeho poznámky byly psány na zadních stranách papírů ukradených telekomunikační společnosti. Co bylo ještě horší, herní poznámky byly prokládány s Urvilovými ručně psanými záznamy o *skutečných průnicích do počítačů*, kterých se dopustil.

Nejen že bylo skoro nemožné oddělit Urvilovy scénáře fantastických her od „reality“ cyberspace, ale ani Urvile sám je téměř nerozlišoval. Není nijak přehnané říci, že pro Urvila bylo *obojí* hra. Urvile byl velmi inteligentní, měl bohatou fantazii a nijak zvlášť ho nezajímalo, co si jiní lidé myslí o vlastnických vztazích. Jeho poměr k „realitě“ nebyl věcí, které by věnoval zvláštní pozornost. Pro Urvila bylo pronikání do počítačů hra. Byla to zábava, zajímavá náplň volného času. A Urvile bral své zábavy vážně. Nemohl přestat pronikat do počítačů o nic snáz, než opustit z poloviny složenou skládačku či rozečtenou fantasy trilogii Stephena Donaldsona. (Jméno „Urvile“ pochází z úspěšné Donaldsonovy novely.)

Urvilův úsměvný, nenarušitelný klid jeho vyšetřovatele nepříjemně dráždil. Především si vůbec nepřipouštěl, že udělal něco špatného. Projevoval minimální stopy upřímné lítosti. Dokonce se choval, jako by byl přesvědčen, že ne on, ale naopak kriminalisté se pohybují ve svém vlastním, soukromém světě zdegenerované fantazie. Urvile byl příliš zdvořilý a dobře vychovaný, než aby to řekl rovnou, ale jeho reakce byly pokřivené a zneklidňující. Například co se týkalo schopností LoDu monitorovat telefonní hovory policie a Tajné služby USA. Urvile souhlasil s tím, že to bylo docela dobře možné a pro LoD to nebyl žádný nepřekonatelný problém. Vlastně o tom diskutoval se svými přáteli na boardu „Black Ice“, stejně jako o jiných zajímavých problémech, například o konstrukci osobního plamenometu a slepování bouchacích kuliček pro zvýšení jejich účinku. Měli stovky čísel státních institucí, získaných ověřováním atlantských telefonů nebo vybraných z počítačů VAX/VMS, do kterých pronikli.

V zásadě se nikdy nedostali k odposlouchávání policajtů, protože tato představa jim nepřipadala natolik zajímavá, aby jim stála za námahu. Kromě toho, kdyby monitorovali telefony Tajné služby USA, zjevně by nikdy nemohli být chyceni. OK?

Tajnou Službu tato neprůstřelná hackerská logika neuspokojila.

Pak se ho ptali na možnost shození telefonní sítě. Bez problémů, ujistil je Urvile s úsměvem. Členové LoDu z Atlanty mohli shodit atlantskou telefonní síť, kdykoli je napadlo. *I systém 911?* Na tom není nic zvláštního, vysvětlil trpělivě Urvile. Stačí shodit ústřednu, třeba chybou unixového příkazu „makedir“, a systém 911 spadne samozřejmě také. Upřímně řečeno, systém 911 nebyl příliš zajímavý. Mohl hrozně zajímat policajty (z nějakých jejich podivných důvodů), ale pokud šlo o technické výzvy, byl systém 911 nudný k uzívání. Samozřejmě, že Atlantská trojka by dokázala shodit systém. Nejspíš by dokázali shodit telefonní síť po celém teritoriu BellSouth, kdyby se tomu chvilku věnovali. Ale Atlantská trojka neničila systémy. Jen neschopní troubové ničili systémy. Atlantská trojka byla *elita*.

Urvile byl pevně přesvědčen, že čistě technická odbornost mu pomůže z jakýchkoli potíží. Co se jeho týkalo, elitní postavení v digitálním undergroundu ho definitivně vyčleňovalo mimo intelektuální sféru policajtů i všech ostatních „normálních“ lidí. Urvile se měl hodně co učit.

Ze tří špiček LoDu měl největší potíže Prophet. Prophet byl profesionální unixovský programátor, schopný kdykoli se dostat do Internetu a přes něj kamkoli jinam. Hackerskou kariéru zahájil asi ve čtrnácti letech pokusy s unixovým sálovým systémem na Univerzitě Severní Karolíny.

Prophet byl autorem užitečného souboru „Použití Unixu a jeho bezpečnost od základů“. Unix je mocný, univerzální počítačový operační systém pro počítače, na kterých současně běží více úloh pro více uživatelů. V roce 1969, kdy byl v Bellových laboratořích vytvořen, měly takové počítače pouze velké společnosti a univerzity, ale dnes běží Unix na tisících výkonných domácích počítačů. Unix byl zvláště vhodný pro telekomunikační programování a stal se v této oblasti standardem. V důsledku toho se stal standardem i pro elitní hackery a telefandy.

Poslední dobou nebyl Prophet tak aktivní jako Leftist a Urvile, ale zato byl recidivista. V roce 1986, když mu bylo osmnáct, byl usvědčen z „neautorizovaného přístupu do počítačové sítě“ v Severní Karolíně. Byl odhalen při průniku do Southern Bell Data Network, vnitřní unixovské sítě telekomunikací, která měla být pro veřejnost nepřístupná. Trest, který dostal, byl pro hackera typický: šest měsíců zákazu činnosti, 120 hodin veřejně prospěšných prací a tříletý ochranný dohled.

Po této ponižující prohře se Prophet zbavil většiny ze svých ilegálně získaných telefandovských a hackerských dat a zkoušel se chovat slušně. Ale na podzim roku 1988 bylo pokušení cyberspace pro Propheta příliš silné a on se po boku Urvila a Leftista pustil do těch nejobtížnějších systémů v dosahu.

Počátkem září 1988 se vloupal do centrálního systému pro automatické řízení společnosti BellSouth, do AIMSX neboli „Advanced Information Management System“ („Pokročilý systém informačního managementu“). AIMSX byla síť pro vnitřní organizační potřeby BellSouth,

kde jeho zaměstnanci skladovali elektronickou poštu, databáze, interní zpravodaje a kalendáře a zpracovávali texty. Protože AIMSX neměla veřejná telefonní čísla, byla považována za naprosto neviditelnou pro každého kromě oprávněných osob a nebyla nijak zvlášť zabezpečena - nevyžadovala dokonce ani hesla. Prophet se přihlásil místo nic netušícího zaměstnance společnosti „waa1“. Pod jménem majitele waa1 uskutečnil Prophet asi deset výletů do AIMSX.

Prophet v systému nic nepoškodil ani nevymazal. Jeho přítomnost v AIMSX byla neškodná a téměř neviditelná. Ale on se s tím nedokázal spokojit.

Jedním z textů zpracovávaných v AIMSX byl dokument, nazvaný „Standardní procedury Bell South 660-225-104SV, Struktura Kontrolního odboru pro rozšířené služby zvláštním službám a významným zákazníkům 911 z března 1988“.

Prophet nepátral speciálně po tomto dokumentu. Byl to pouze jeden ze stovek podobných dokumentů s neproniknutelnými tituly. Ale když o něj během svého ilegálního pobytu v AIMSX zakopl, rozhodl se, že si ho odnese jako trofej. Mohl se mu hodit v nějakém budoucím chlubivém, chvástavém a naparovacím představení. Takže někdy během září 1988 přikázal Prophet sálovému počítači AIMSX, aby tento dokument (napříště označovaný jednoduše jako „Dokument 911“) zkopíroval na jeho domácí počítač.

Nikdo si nevšiml, že to Prophet udělal. V jistém smyslu Dokument 911 „ukradl“, ale pojem vlastnictví může být v cyberspace ošidný. V BellSouth si ničeho nevšimli, protože originál dokumentu zůstal na svém místě. Nebyli „oloupeni“ o samotný dokument. Mnoho lidí bylo oprávněno kopírovat ho - konkrétně lidé pracující pro devatenáct „zvláštních služeb a významných zákazníků“ po celém jihovýchodě Spojených Států. To bylo ostatně účelem jeho existence a důvodem uložení v počítačové síti: být kopírován a čten - zaměstnanci telekomunikační společnosti. Ale nyní si tato data zkopíroval někdo, o kom se nepředpokládalo, že mu budou dostupná.

Prophet měl nyní svoji trofej. Navíc se rozhodl, že uloží ještě další kopii Dokumentu 911 na počítači jiné osoby. Touto nic netušící osobou byl počítačový nadšenec Richard Andrews, žijící nedaleko Jolietu v Illinois. Richard Andrews se živil jako unixovský programátor a vedl výkonný unixovský board zvaný „Jolnet“, umístěný ve sklepě svého domu.

Prophet získal pod jménem „Robert Johnson“ účet na počítači Richarda Andrewse. A do tohoto počítače uložil Dokument 911, do své vlastní, soukromé oblasti na něm.

Proč to Prophet udělal? Kdyby odstranil Dokument 911 ze svého vlastního počítače a držel svou kopii stovky mil daleko, na cizím stroji a pod falešným jménem, mohl si být celkem jist, že nebude objeven a potrestán - ačkoli jeho konspirativní opatření nepochybně postavilo nic netušícího Richarda Andrewse do riskantní situace. Ale jako většina hackerů, byl i Prophet na ilegálně získaná data jako křeček. Když došlo na lámání chleba, nedokázal se se svou trofejí rozloučit. Když bylo jeho bydliště v Decaturu v Georgii v srpnu 1989 prohledáno, byl Dokument 911, nezvratný důkaz, nalezen. A Prophet, v rukou Tajné služby USA, se ze všech sil snažil o „vysvětlení“.

***

Náš příběh nás nyní vede od Atlantské trojky a jejich konfrontace se zákonem v létě 1989. Musíme opustit Atlantskou trojku „plně spolupracující“ se svými četnými vyšetřovateli. A všichni tři spolupracovali, jak vyplývá z odůvodnění jejich rozsudku Státním soudem Severního distriktu Georgie - až do prosince 1990, kdy byli všichni tři odsouzeni do různých federálních věznic.

Teď se musíme věnovat jiným aspektům války s LoD. Válka s Legií byla totiž válkou v síti, konkrétně v síti tří sítí, komplexním způsobem propletených a navzájem se ovlivňujících. Sama Legie, včetně Atlantské trojky, a jejich obdivovatel Fry Guy, byla první sítí. Druhou sítí byl časopis *Phrack*, jeho redaktoři a přispěvatelé. Třetí sítí byla elektronicky spolupracující skupina kolem hackera jménem „Terminus“.

Válka proti těmto hackerským sítím byla uskutečňována policejní sítí. Atlantská trojka a Fry Guy byli pronásledováni agenty Tajné služby USA a federálními prokurátory z Atlanty, Indiany a Chicaga. Terminus zjistil, že mu je na stopě Tajná služba a federální prokurátoři z Baltimore a Chicaga. A válka proti *Phracku* byla téměř výhradně záležitostí Chicaga.

Vyšetřování případu Terminus bylo věnováno mnoho energie, zejména Chicagskou operační skupinou, ale tato operace je tou nejméně známou a nejméně zveřejňovanou z celého Zátahu na hackery. Terminus, žijící v Marylandu, byl unixovský programátor a konzultant, poměrně známý a uznávaný (pod svým rodným jménem) v unixovské komunitě jako expert na minipočítače AT&T. Terminus obdivoval AT&T, zejména Bellcore, a zakládal si na své reputaci unixovského experta; jeho nejvyšší ambicí bylo pracovat pro Bellovy laboratoře.

Ale Terminus měl podivné přátele a temnou minulost. Jednou byl objektem obdivného interview ve *Phracku* (svazek 2, číslo 14, soubor 2, datovaný květen 1987). V tomto článku ho jeden ze šéfredaktorů *Phracku* Taran King popsal jako inženýra, výška 5 stop a 9 palců, hnědé vlasy, narozen 1959. Osmadvacet let je na hackera poměrně vysoký věk.

Terminus byl kdysi sysopem telefandovsko-hackerského undergroundového boardu „MetroNet“, běžícího na Apple II. Později nahradil MetroNet undergroundovým boardem „MegaNet“, specializovaným na IBM. V dobách svého mládí napsal Terminus program na systematické zkoušení přístupových kódů pro IBM PC, jeden z úplně prvních a velice elegantní. Tento program byl v undergroundu široce rozšířen. Nepočítaně telefandů a hackerů vlastnících PC ho používalo ke krádežím telekomunikačních kódů. Tento úspěch neunikl pozornosti bezpečnostních odborníků telecomu; stěží jí mohl uniknout, protože dřívější handle Terminuse, „Terminal Technician“, byla hrdě vepsána do programu.

Když se stal počítačovým specialistou na plný úvazek (specializujícím se na programování telekomunikací), přijal handle Terminus („Konečný“), která měla vyjádřit, že jako hacker dosáhl konečného, dokonalého stadia. Pořídil si unixovský board „NetSys“ na počítači AT&T, se čtyřmi telefonními linkami a působivými 240 megabyty místa na disku. Na NetSysu byl dostupný kompletní *Phrack* od prvního čísla a Terminus udržoval přátelské styky s jeho šéfredaktory, Taran Kingem a Knight Lightningem.

Počátkem 80. let byl Terminus stálým hostem na Plovernetu, Pirate-80, Sherwood Forestu a Shadowlandu, což všechno byly známé pirátské boardy, často navštěvované členy Legion of Doom. Terminus vlastně formálně nikdy nebyl „členem LoD“, protože nikdy nedostal oficiální, obřadné požehnání od velkého náčelníka Legie Lexe Luthora. Terminus se nikdy fyzicky nesetkal s nikým z LoDu. Ale to stěží mělo nějaký význam - ani sama Atlantská trojka nebyla Lexem nikdy formálně uznána. Z hlediska policie byl případ jasný. Terminus byl dospělý profesionál, živící se programováním a se speciálními znalostmi softwaru a hardwaru AT&T - a přitom byl Terminus jedna ruka s Legion of Doom a undergroundem.

1. února 1990 - čtrnáct dní po kolapsu telefonní sítě AT&T - se agenti Tajné služby USA Tim Foley z Chicaga a Jack Lewis z Baltimore, doprovázení bezpečnostním odborníkem AT&T Jerry Daltonem, vydali do Middle Town v Marylandu. Terminus byl vyslýchán ve svém domě (k hrůze své manželky a malých dětí) a jeho počítače byly, jak bylo zvykem, zabaveny.

Zjistilo se, že počítač NetSysu obsahuje spoustu specializovaného unixovského softwaru - copyrightované zdrojové texty programů patřících AT&T. Například: UNIX System Five Release 3.2 (vlastní operační systém); UNIX SV Release 3.1; komunikační software UUCP; KORN shell (rozhraní pro ovládání systému z klávesnice); RFS; IWB; WWB; DWB; programovací jazyk C++; PMON; TOOL CHEST; QUEST; DACT; S FIND.

Podle starých pirátských tradic undergroundu poskytoval Terminus tento ilegálně zkopírovaný software malému okruhu svých známých unixovských programátorů. Velmi nemoudře skladoval na počítači NetSysu sedm let své elektronické pošty, dokumentující všechny jeho přátelské transakce s různými kolegy. Terminus nezpůsobil kolaps z 15. ledna. S potěšením ale řídil neziskovou pirátskou síť šířící software AT&T. To nebylo nic, co by AT&T dělalo radost. Bezpečnostní odborník AT&T Jerry Dalton ocenil „ukradený“ software na více než třista tisíc

dolarů.

Vstup AT&T do arény volného trhu byl komplikován novými a neurčitými pravidly informační ekonomiky. Až do rozdělení Ma Bell z rozhodnutí soudu bylo AT&T zakázáno prodávat hardware nebo software. Ma Bell byla telefonní společnost; nesměla použít své ohromné zisky z telefonů k financování vstupu na počítačový trh.

Nicméně AT&T vyvinula operační systém Unix. A podařilo se jí vydělat na něm nějaké peníze. Je poněkud absurdní, že Unix nebyl prodáván jako počítačový software, ale podle obskurní výjimky v regulačních omezeních povolující prodej přebytečného vybavení a odpadu. Jakýkoli velkorysejší pokus udělat Unixu reklamu a prodávat ho ve velkém by vyprovokoval žaloby počítačových společností. Místo toho byly licence na Unix za mírné poplatky přenechány univerzitám, kde kyseliny akademických svobod systematicky rozpouštěly copyrightová práva AT&T.

Po rozdělení si v AT&T byli vědomi, že Unix je potenciální zlatý důl. V té době už existovaly velké kusy unixovského kódu, které nepatřily AT&T a byly prodávány jinými. Celý konkurenční unixovský operační systém byl vyvinut v Berkeley v Kalifornii (jednom z nejdůležitějších zdrojů hackerské ideologie na světě). Dnes „hackeři“ zpravidla považují „Berkeley Unix“ za technicky pokročilejší než „System V Unix“ od AT&T, ale AT&T nenechala pouhou technickou eleganci zasahovat do racionálního byznysu prodeje copyrightovaného softwaru. AT&T úmyslně odstranila kompatibilitu svého vlastního kódu s Unixem jiných lidí a napsala kód, o kterém může dokázat, že je copyrightovaný, i když tento kód je poněkud nemotorný a „dřevorubecký“. Uživatelské licence AT&T jsou důkladné obchodní smlouvy, plné jasných upozornění na autorská práva a zákazů šíření třetím osobám.

AT&T neudržela Unix úplně pod pokličkou, ale aspoň v hrnci. Vzhledem k tomu, jak všudypřítomné a nekontrolované je softwarové pirátství, je zdrojový kód Unixu AT&T silně copyrightovaný, dobře střežený a poskytovaný za přísných podmínek. Unix se tradičně používal pouze na sálových počítačích, patřících velkým skupinám profesionálů s kravatami, a ne na strojích umístěných v ložnici, kde lidé snadno dostávají zlomyslné nápady.

A zdrojový kód Unixu AT&T je opravdové programování na vysoké úrovni. Počet schopných unixovských programátorů, kteří mají motiv ke krádeži zdrojového kódu Unixu, je malý. Velmi malý ve srovnání s desítkami tisíc lidí ochotnými získat bez placení například populární hry na PC jako třeba „Leisure Suits Larry“.

Ale v roce 1989 se ukázalo, že pirátský underground, konkrétně Terminus a jeho přátelé, vztáhl ruku na Unix AT&T. A vlastnictví, o které šlo, nebylo prodáváno za dvacet dolarů v místním supermarketu Bill; byl to komplexní, sofistikovaný, víceuživatelský a víceúlohový kód za desetitisíce dolarů.

Na tomto místě je třeba zdůraznit, že Terminus a jeho údajná skupina softwarových pirátů ve skutečnosti ze zločinů, ze kterých byli obviněni, nezískali žádné peníze. Zdůrazňovaná suma 300 000 dolarů, udávaná jako cena obsahu počítače NetSysu, neznamenala, že Terminus skutečně získal nezákonným způsobem třista tisíc dolarů patřících AT&T. Terminus poskytoval a přijímal software, soukromě, svým známým, a zdarma. Nekradl programy, aby je mohl prodávat. Nežádal o peníze a nedostával je. Žil docela skromně.

Zaměstnanci AT&T - a také nezávislí unixovští konzultanti, jako byl Terminus - běžně pracovali s „copyrightovaným“ softwarem AT&T, a to v kanceláři i doma na svých soukromých počítačích. AT&T zřídkakdy vysílala své bezpečnostní odborníky, aby pročesali pevné disky jejích konzultantů. Laciní nezávislí nájemní programátoři byli pro AT&T velmi užiteční; neměli zdravotní pojištění ani důchodové programy a už vůbec nebyli členy Odborového svazu amerických pracujících v telekomunikacích. Byli to námezdní poskokové, uklízečky ve Velkém technologickém chrámu AT&T; ale když se Tajná služba USA porozhlédla po jejich domovech, zdálo se, že jedí na stříbře společnosti a spí na jejích poduškách! Měli tu drzost chovat se, jako kdyby jim věci, se kterými pracovali každý den, patřily!

A nebyli to žádní nezletilí hackeři tahající papíry z popelnic, s nosy přitisknutými k oknům mrakodrapů vrcholového managementu. Tihle mladíci byli unixoví mágové, a nejen že měli data AT&T na svých počítačích a ve svých hlavách, ale s elánem se spojili k jejich studiu, a využili k tomu počítačů mnohem silnějších než cokoli, co bylo předtím představitelné v soukromých rukou. Jak zajistíte, aby lidé, kteří nejsou stálými zaměstnanci, měli uctivý respekt k vašemu vlastnictví? Bylo to dilema.

Rozsáhlé části unixovského kódu nebyly copyrightovány a daly se legálně získat zadarmo. Rozsáhlé části „copyrightovaného“ unixovského kódu byly důkladně přepracovány, změněny možná natolik, že se staly zcela novým produktem - nebo možná ne. Intelektuální vlastnictví softwarových vývojářů bylo, a je, neobyčejně složité a zmatené. A „softwarové pirátství“, podobně jako amatérské kopírování videokazet, je jedním z nejrozšířenějších „zločinů“ tohoto světa. Agenti Tajné služby USA nebyli odborníci na Unix a nebyli obeznámeni se zvyklostmi v jeho používání. Tajná služba USA, jako organizace, nezaměstnávala ani jednu osobu, která by dokázala programovat v prostředí Unixu - ne, ani jedinou. Tajná služba bohatě využívala služeb *externích* expertů, ale „experti“, které si vybrala, byli bezpečnostní specialisté AT&T a Bellcore, tedy přímé *oběti* vyšetřovaných zločinů, lidé, kteří měli maximální zájem na ochraně „copyrightovaného“ softwaru AT&T.

6. února 1990 byl Terminus zatčen agentem Lewisem. Nakonec byl odsouzen do vězení za ilegální užívání softwarových produktů AT&T.

Otázka pirátského šíření softwaru AT&T byla přítomna v pozadí během celé války s Legií. Asi půl tuctu lidí, se kterými Terminus udržoval elektronické kontakty - lidí žijících v Illinois, Texasu a Kalifornii - bylo důkladně vyslýcháno Tajnou službou USA ve spojitosti s ilegálním kopírováním softwaru. Ale Terminus zůstal jediným, kdo z něj byl obviněn. Nikdo z ostatních neměl jeho prominentní postavení v hackerském undergroundu.

To ale neznamenalo, že tito lidé neměli potíže nebo se jim mohli vyhnout. Transfer ilegálních dat je v cyberspace mlhavá a špatně popsatelná činnost, plná neočekávaných nebezpečí pro všechny zúčastněné: hackery, majitele přenosových kapacit, majitele boardů, policisty, veřejné žalobce i náhodné kolemjdoucí. Dobře míněná snaha vyhnout se potížím či potrestat porušování zákona může někdy způsobit více škody než obyčejná pasivita, lhostejnost nebo nekorektnost.

NetSys nebyl obyčejný „spotřební“ board, ačkoli měl většinu obvyklých funkcí BBS. NetSys nebyl izolovaný počítač, ale část celosvětově spolupracující sítě „UUCP“. Síť UUCP používá sadu programů Unixu, zvanou „Unix-to-Unix Copy“, umožňující unixovským systémům vyměňovat si data vysokými rychlostmi prostřednictvím veřejné telefonní sítě. UUCP je radikálně decentralizovaná, nezisková síť unixovských počítačů. Těchto počítačů existují desítky tisíc. Některé jsou malé, ale mnoho z nich je velkých a výkonných a také propojených s jinými sítěmi. Existují jisté poměrně komplikované vazby mezi UUCP a rozsáhlými sítěmi jako je JANET, EasyNet, BITNET, JUNET, VNET, DASnet, PeaceNet a FidoNet a také gigantický Internet. (Takzvaný Internet není ve skutečnosti ani tak síť sama o sobě, ale spíše standard rozhraní mezi různými sítěmi, umožňující mnoha celosvětovým počítačovým sítím komunikovat mezi sebou. Čtenáři, které zajímají složité a fascinující propletence moderních počítačových sítí, mohou ocenit autoritativní 719-stránkový výklad Johna S. Quartermana *The Matrix* („Vzor“), vydaný Digital Press v roce 1990.)

Schopný uživatel unixovského NetSysu mohl posílat a přijímat elektronickou poštu téměř z každé významné počítačové sítě na světě. NetSys nebyl nazýván board, ale spíše „node“ („uzel“). Nody jsou větší, rychlejší a sofistikovanější než pouhé boardy, a pro hackery je přítomnost na mezinárodně propojených nodech symbolem mnohem vyššího statusu než přítomnost na pouhých místních boardech. Terminus měl přes svůj node NetSys v Marylandu mnoho přímých spojení k jiným, podobným nodům UUCP, vedených lidmi, kteří měli stejné zájmy a aspoň částečně stejné svobodomyslné názory jako on. Jedním z těchto nodů byl Jolnet, vlastněný Richardem Andrewsem, který byl stejně jako Terminus nezávislým unixovským konzultantem. I Jolnet pracoval pod Unixem a dalo se s ním spojit vysokou rychlostí ze sálové-

ho počítače kdekoli na světě. Jolnet byl z technického hlediska poměrně sofistikovaný, nicméně stále byl řízen jednou osobou, jako soukromý, neziskový koníček. Většina uživatelů Jolnetu byli unixovští programátoři - používali ho pro poštu, ukládání dat a přístup k sítím. Jolnet zprostředkovával přístup k síti přibližně dvěma stům lidí a také místní střední škole. Mezi svými ostatními službami nabízel Jolnet i časopis *Phrack*.

Ze svých vlastních důvodů pojal Richard Andrews podezření, že s jeho novým uživatelem „Robertem Johnsonem“ není všechno v pořádku. Richard Andrews se rozhodl podívat se, co „Robert Johnson“ v Jolnetu skladuje. A našel Dokument 911.

„Robert Johnson“ byl Prophet z Legion of Doom, a Dokument 911 byl jeho kořistí ilegálně získanou z počítačů BellSouth.

Dokument 911, speciálně ilegální kousek digitálního vlastnictví, se opět pohnul po své dlouhé, složité a katastrofické cestě.

Andrewse zarazilo, že někdo, kdo není zaměstnancem telefonní společnosti, má dokument zabývající se systémem 911. I na dokumentu samém bylo jasné upozornění: „POZOR: NEPOUŽÍVAT A NEZVEŘEJŇOVAT MIMO BELLSOUTH A JEJÍ DCEŘINNÉ SPOLEČNOSTI BEZ ZVLÁŠTNÍHO PÍSEMNÉHO POVOLENÍ.“

Tato standardní varování jsou často připisována na všechny možné obchodní materiály. Zvláště spojaři jako živočišný druh jsou známi svou vášní orazítkovat všechno, co se jim dostane pod ruku, jako „důvěrné“. Ale přece jen, tento dokument se zabýval systémem 911. Richovi Andrewsovi se to nechtělo líbit.

Andrews nebyl ochoten ignorovat možné potíže. Rozhodl se, že by bylo rozumné poslat tento dokument jednomu příteli a známému z unixovské sítě a konzultovat ho s ním. Takže někdy v září 1988 poslal Andrews elektronicky další kopii Dokumentu 911 jistému zaměstnanci AT&T, Charlesi Boykinovi, který vedl unixovský node „attctc“ v Dallasu v Texasu.

„Attctc“ patřil AT&T a byl umístěn v jeho „Customer Technology Center“ („Zákaznické technologické centrum“) v Dallasu - odtud „attctc“. „Attctc“ byl spíše znám pod jménem „Killer“ („Zabiják“), což bylo jméno stroje, na kterém systém běžel. Killer byl velký, silný model AT&T 3B2 500, víceuživatelská, víceúlohová unixovská platforma s 32 megabyty operační paměti a obtížně představitelnými 3,2 gigabyty místa na disku. V roce 1985, kdy Killer přišel do Texasu, byla řada 3B2 jednou ze zářivých nadějí AT&T v připravované bitvě s IBM o trh počítačů pro velké společnosti. Killer byl umístěn v Zákaznickém technologickém centru v dallaském Nákupním centru informatiky, což byl v podstatě luxusní obchodní dům nabízející technologické novinky, a používán jako demonstrační vzorek.

Charles Boykin, dlouholetý zaměstnanec AT&T a specialista na hardware a digitální komunikace, byl členem místního týmu technické podpory pro systémy 3B2. Jako demonstrační vzorek v obchodním domě neměl Killer mnoho co na práci, a byla ostuda nechat jeho kapacitu zahálet. Takže Boykin dostal chytrý nápad - napsal pro Killera unixovský BBS software a zapojil stroj do místní telefonní sítě. Svým debutem koncem roku 1985 se Killer stal prvním veřejně přístupným unixovským počítačem ve státě Texas. Široká veřejnost byla vítána.

Stroj okamžitě vyvolal vznik elektronické komunity. Zapojil se do sítě UUCP a nabídl spojení na více než osmdesát dalších počítačů, jejichž přístup do neomezeného cyberspace závisel na Killerovi. A nesloužil jen velkým zvířatům; i uživatelé osobních počítačů skladovali v jeho ohromných 3200-megabytových prostorách volně šiřitelné programy pro počítače Amiga, Apple a IBM. Svého času měl Killer největší knihovnu volně šiřitelného softwaru pro Apple Macintosh v Texasu.

Časem Killer přitáhl kolem patnácti set živě komunikujících uživatelů, uploadujících a downloadujících programy, posílajících si poštu, vyměňujících si klepy a připojujících se k tajemným vzdáleným sítím.

Boykin nebyl za vedení Killera nijak placen. Považoval to za dobrou reklamu pro systém AT&T 3B2 (zisky z jeho prodeje nedosahovaly zrovna závratných výšek), ale také se mu prostě líbila živá komunita, kterou svými schopnostmi vytvořil. Zveřejnil svůj unixový BBS software a dal ho zdarma k dispozici případným zájemcům.

Mezi unixovskými programátory měl Charlie Boykin reputaci sympatického, upřímného a rozumného člověka. V roce 1989 ho skupina unixovských profesionálů z Texasu zvolila „Systémovým administrátorem roku“. Byl považován za muže, jehož radám je možno důvěřovat.

V září 1988 vtrhl Dokument 911, poslaný Richardem Andrewsem, do Boykinova života. Boykin okamžitě pochopil, že dokument je kradený. Nebyl odborník na hlasovou komunikaci a neznal neveřejné detaily o následnických společnostech AT&T, ale velmi dobře chápal, co je to systém 911, a rozčílilo ho, že se důvěrné informace o tomto systému dostaly do nepovolaných rukou. Tato záležitost jasně spadala do náplně práce bezpečnostního odboru. Takže 21. září 1988 pořídil Boykin *další* kopii Dokumentu 911 a poslal ji svému známému z práce, jistému Jerome Daltonovi z Odboru AT&T pro informační bezpečnost. Jerry Dalton byl tentýž člověk, který se později zúčastnil razie v domě Terminuse. Z bezpečnostního odboru AT&T byl Dokument 911 poslán do Bellcore. Bellcore neboli „BELL COmmunications REsearch“ („Bellův výzkum komunikací“) byl kdysi ústřední laboratoří Bellovy společnosti. Zaměstnanci Bellových laboratoří vyvinuli operační systém Unix. Nyní byl Bellcore formálně nezávislou společností s více vlastníky, fungující jako výzkumné středisko všech sedmi následnických společností Bellu. Bellcore měl výhodnou pozici i při koordinaci bezpečnostních technologií a konzultací pro následnické společnosti; muž pověřený vedením těchto snah byl Henry M. Kluepfel, celoživotní zaměstnanec Ma Bell, pracující pro ni přes čtyřiadvacet let.

13. října 1988 předal Dalton Dokument 911 Henrymu Kluepfelovi. Kluepfel, zkušený odborný svědek obžaloby v případech telekomunikační a počítačové zpronevěry, viděl už mnohem větší potíže než tuto. Přijal dokument jako to, čím skutečně byl: jako trofej z hackerského průniku.

Ovšem ať už onen průnik způsobil jakékoli škody, byl to nejspíš loňský sníh. Vypadalo to, že se v dané fázi celkem nedá nic dělat. Kluepfel si pečlivě poznamenal okolnosti případu a problém založil.

Uplynulo několik měsíců.

Byl únor 1989. Atlantská trojka se prohánělа v ústřednách BellSouth a nic netušila o svém brzkém konci. Legie jen kvetla. A stejně tak časopis *Phrack*. Uplynulo dobrých šest měsíců od Prophetova průniku do AIMSX. Propheta, jak je u hackerů obvyklé, omrzelo sedět na svých vavřínech. Knight Lightning a Taran King, šéfredaktoři *Phracku*, po něm neustále loudili materiál vhodný k publikaci. Prophet se rozhodl, že už nehrozí žádné podstatné nebezpečí a že se klidně může začít vychloubat, chvástat a naparovat.

Takže poslal kopii Dokumentu 911 - další kopii - ze stroje Jolnetu patřícího Richardu Andrewsovi na účet Knight Lightninga v BITnetu na Univerzitě v Missouri. Zopakujme si nyní, kde všude se nachází Dokument 911.

0. Originální dokument 911. Ten je v systému AIMSX na sálovém počítači v Atlantě a je dostupný stovkám lidí, kteří by ale všichni měli být zaměstnanci BellSouth. Někteří z těchto lidí - není známo kolik - mohou mít své vlastní kopie tohoto dokumentu, ale všichni jsou profesionální spojaři a mají důvěru telefonní společnosti.

1. Prophetova ilegální kopie, u něj doma na jeho osobním počítači v Decaturu v Georgii.

2. Prophetova záložní kopie, uložená na počítači Jolnetu Riche Andrewse ve sklepě jeho domu blízko Jolietu v Illinois.

3. Kopie Charlese Boykina na Killeru v texaském Dallasu, zaslaná Richem Andrewsem z Jolietu.

4. Kopie Jerryho Daltona v Odboru AT&T pro informační bezpečnost v New Jersey, zaslaná Charlesem Boykinem z Dallasu.

5. Kopie Henryho Kluepfela na ředitelství bezpečnostního odboru Bellcore v New Jersey, zaslaná Daltonem.

6. Kopie Knight Lightninga, zaslaná Prophetem ze stroje Richarda Andrewse, v Columbii v Missouri.

Je zřejmé, že „zabezpečení“ tohoto důvěrného dokumentu, jakmile byl vyloven z AIMSX, se rychle stalo dosti pochybným. Bez jakýchkoli

finančních transakcí a bez jakékoli zvláštní snahy byla tato data nejméně šestkrát reprodukována a rozšířila se po celém kontinentu. Ovšem to nejhorší mělo teprve přijít.

V únoru 1989 se Prophet a Knight Lightning elektronicky dohadovali, co s touto trofejí podniknou. Prophet se chtěl vytáhnout, ale zároveň si samozřejmě nepřál být chycen.

Na druhé straně Knight Lightning byl odhodlán publikovat z dokumentu co nejvíce. Knight Lightning studoval společenské vědy a zejména se zajímal o otázky svobody slova. Rád publikoval prakticky cokoli, co ukazovalo v příznivém světle schopnosti undergroundu a zahanbovalo telekomunikační společnosti. Ale Knight Lightning měl i kontakty s bezpečnostními experty, se kterými čas od času konzultoval, zda materiál, který získal, není příliš citlivý pro zveřejnění.

Prophet a Knight Lightning se rozhodli, že Dokument 911 proškrtají a odstraní tak většinu příznaků, podle nichž ho bylo možno identifikovat. Nejdříve ze všeho zmizelo nápadné varování „NEPOUŽÍVAT A NEZVEŘEJŇOVAT“. Odstranili i další kritická místa, například seznam pracovních telefonních čísel specialistů BellSouth na systém 911 na Floridě. Kdyby byla tato telefonní čísla publikována ve *Phracku*, byli by tito zaměstnanci BellSouth velmi pravděpodobně obtěžováni telefandy, což by BellSouth pořádně nadzvedlo a představovalo by jak pro Propheta, tak pro *Phrack* vážné riziko.

Takže Knight Lightning zkrátil Dokument 911 téměř na polovinu a odstranil telefonní čísla a některé citlivé specifické informace. Pak ho elektronicky vrátil Prophetovi; Prophet měl stále obavy, takže Knight Lightning vypustil ještě něco. Nakonec se shodli, že dokument je připraven k publikaci a že bude zveřejněn ve *Phracku* pod pseudonymem „Eavesdropper“ („Naslouchač“).

K publikaci došlo 25. února 1989.

Čtyřiadvacáté číslo *Phracku* obsahovalo rozverné interview se zástupcem šéfredaktora, telefandou „Chanda Leirem“ („Lustr“), tři články o BITnetu a jeho propojení s jinými počítačovými sítěmi, článek o číslech s předvolbami 800 a 900 (tato čísla si pronajímají obchodní společnosti pro reklamní kampaně, soutěže apod.) od „Unknown Usera“, článek „VaxCata“ („Dorůstající kočka“) o základech telekomunikací, elegantně nazvaný „Ma Bell za závojem tajemství“ a obvyklé „Phrack World News“.

V této sekci byla, ironickou náhodou, i rozsáhlá zpráva o odsouzení osmnáctiletého hackera z Chicaga jménem „Shadowhawk“, kterého dostal do federální věznice sám William J. Cook.

A toto číslo obsahovalo i dva články od „Eavesdroppera“. První byl upravený Dokument 911, nazvaný nyní „Struktura Kontrolního odboru pro rozšířené služby zvláštním službám a významným zákazníkům 911“. Eavesdropperův druhý článek byl glosář termínů, vysvětlující záplavu spojařských akronym a žargonu v Dokumentu 911.

Nešťastný dokument byl nyní distribuován na více než sto padesát míst, která pravidelně dostávala *Phrack*. Ne sto padesát *lidí*, nenechte se mýlit - sto padesát *míst*, z nichž některé byly unixové nody nebo boardy, samy o sobě mající desítky, dokonce stovky uživatelů.

To bylo v únoru 1989. Bezprostředně se nic nestalo. Přišlo léto, a Atlantská trojka byla zadržena Tajnou službou USA. Byl dopaden Fry Guy. Ale *Phracku* se nic nestalo. Vyšlo dalších šest jeho čísel, celkem třicet víceméně každý měsíc. Knight Lightning a jeho zástupce Taran King neměli žádné problémy.

Phrack měl ve zvyku přikrčit se, když začaly létat třísky. Během letních zátahů v roce 1987 (k zátahům na hackery dochází zpravidla v létě, možná proto, že hackery je snazší najít doma než na koleji) nevydal *Phrack* nové číslo několik měsíců a držel se stranou. Bylo zatčeno několik lidí kolem LoDu, ale redakci *Phracku*, elitním reportérům undergroundu, se nic nestalo. V roce 1988 převzal *Phrack* nový šéfredaktor „Crimson Death“ („Červená Smrt“), nevázaný mladík se zálibou v anarchistických souborech.

Rok 1989 vypadal pro underground plodně. Knight Lightning a jeho zástupce Taran King se znovu ujali vlády a *Phrack* se po celý rok úspěšně rozvíjel. Atlantský LoD v létě 1989 neslavně skončil, ale *Phrack* pokračoval vesele dál. Nezdálo se, že by Prophetův Dokument 911 měl *Phracku* způsobit nějaké potíže. V lednu 1990 byl ve *Phracku* dostupný už téměř rok. Kluepfel a Dalton, zástupci bezpečnostního odboru AT&T, měli dokument šestnáct měsíců - dostali ho ještě dříve než samotný Knight Lightning - a nevyvinuli žádnou snahu zastavit jeho distribuci. Dokonce ani neřekli Richi Andrewsovi a Charlesi Boykinovi, aby smazali kopie na svých unixovských nodech, na Jolnetu a Killerovi. Ale pak, 15. ledna 1990, v den výročí smrti Martina Luthera Kinga, došlo k monstróznímu kolapsu.

Pouhé tři dny na to, 18. ledna, přišli do domu studentského bratrstva, kde bydlel Knight Lightning, čtyři návštěvníci. Byli to Timothy Foley a Barbara Goldenová, agenti Tajné služby USA z chicagské úřadovny, spolu s bezpečnostním specialistou Univerzity v Missouri a Reedem Newlinem z bezpečnostního odboru Southwestern Bellu, následnické společnosti Bellu v Missouri. Foley obvinil Knight Lightninga, že způsobil celostátní kolaps telefonní sítě.

Knight Lightning byl tímto obviněním zděšen. Na první pohled takové podezření nebylo úplně nepravděpodobné - ačkoli Knight Lightning věděl, že on sám to neudělal. Ale na druhé straně spousta hackerů vytahujících se svými schopnostmi tvrdila, že dokážou shodit systém. Například Shadowhawk, chicagský hacker, kterého William Cook nedávno dostal do vězení, se na boardech několikrát chlubil, že umí „zastavit veřejnou síť AT&T“. A teď se něco takového, nebo přinejmenším něco, co přesně tak vypadalo, doopravdy stalo. Kolaps nasadil Chicagské operační skupině ostruhy. A dosud okolkující Bellcore a AT&T byly nyní připraveny k akci. Bezpečnostní odborníci telekomunikací - již předtím zděšení schopnostmi hackerů v teritoriu BellSouth - se shodovali v tom, že digitální underground se vymkl kontrole. LoD a *Phrack* museli být odstraněni.

A publikováním Dokumentu 911 poskytl *Phrack* policii vytouženou příležitost k legálnímu zásahu. Foley se dotázal Knight Lightninga na Dokument 911.

Knight Lightning ztratil nervy. Okamžitě začal „plně spolupracovat“, jak bylo v digitálním undergroundu tradicí.

Dal Foleymu všechna čísla *Phracku*, vytištěná a svázaná v kroužkových blocích. Předal svůj elektronický seznam stálých odběratelů *Phracku*. Foley a jeho pomocníci vyslýchali Knight Lightninga čtyři hodiny. Knight Lightning přiznal, že Dokument 911 mu předal Prophet, a připustil, že věděl, že byl ukraden při hackerském průniku do systému telefonní společnosti. Knight Lightning podepsal v tomto smyslu prohlášení a písemně potvrdil, že bude spolupracovat s vyšetřovateli.

Další den - 19. ledna 1990 - se agenti Tajné služby USA vrátili s povolením k domovní prohlídce a důkladně pročesali pokoj Knight Lightninga v domě jeho studentského bratrstva. Sebrali všechny jeho diskety, ale kupodivu mu nechali jeho počítač i modem. (Počítač neměl žádný pevný disk a nemohl tedy podle Foleyho názoru obsahovat žádný důkazní materiál.) Ale pro Knight Lightninga to byl jen velmi malý jasný bod uprostřed rychle rostoucích nepříjemností. Měl potíže nejen s federální policií, ale také se staršími svého studentského bratrstva, které rozčílila představa, že nevědomky poskytovali útočiště federálnímu počítačovému zločinci.

V pondělí byl Knight Lightning předvolán do Chicaga, kde byl opět vyslýchán Foleym a zkušenou agentkou Tajné služby USA Barbarou Goldenovou, tentokrát za přítomnosti advokáta. A v úterý byl formálně obviněn federální velkou porotou.

Proces Knight Lightninga, který probíhal 24. až 27. srpna 1990, byl klíčovým soudním sporem Zátahu na hackery. Důkladně se mu budeme věnovat ve čtvrté části této knihy. Nyní odhodlaně pokračujme po stopě Dokumentu 911.

V lednu 1990 už muselo být jasné, že Dokument 911, ve verzi, kterou publikoval *Phrack* v únoru 1989, se rozšířil rychlostí světla nejméně sto padesáti různými směry. Pokoušet se nacpat tohoto elektronického džina zpátky do láhve bylo prostě nemožné.

Nicméně Dokument 911 byl z formálního právního hlediska stále *kradený*. Jakýkoli elektronický přenos tohoto dokumentu, kýmkoli, kdo nebyl autorizován k manipulaci s ním, mohl být interpretován jako zpronevěra s použitím telefonu. Přeprava kradeného materiálu mezi státy USA, včetně elektronického materiálu, je federálním zločinem.

Chicagská operační skupina proti počítačové zpronevěře a zneužití počítače byla ujištěna, že Dokument 911 má velkou finanční cenu. Přesněji řečeno, měli od bezpečnostních odborníků BellSouth konkrétní sumu: 79 449 dolarů. Takové peníze ospravedlňovaly rozsáhlou akci. I kdyby spáchané škody už nemohly být napraveny, byla tak velká částka přinejmenším dobrým právnickým argumentem pro exemplární potrestání zlodějů. Bylo pravděpodobné, že udělá dojem na soudce a poroty. Mohla být využita ke zlikvidování Legion of Doom.

Atlantské křídlo bylo už v době, kdy se Chicagská operační skupina dostala k *Phracku*, vykázáno do patřičných mezí. Ale Legion of Doom byl jako hydra. Koncem roku 1989 zahájil provoz zbrusu nový board Legie, „Projekt Fénix“ v Austinu v Texasu. Sysopem Projektu Fénix nebyl nikdo menší než sám Mentor, jemuž byl schopným pomocníkem student Texaské univerzity a ostřílený člen LoDu „Erik Bloodaxe“ („Krvavá sekyra“). Jak jsme viděli z jeho manifestu ve *Phracku*, byl Mentor hackerský fanatik, považující pronikání do počítačů za cosi jako morální povinnost. A projekt Fénix byla ambiciózní operace; jejím cílem bylo oživit digitální underground do toho, co Mentor považoval za jeho slavné doby počátku 80. let. Fénix měl také poskytnout elitním hackerům fórum pro otevřené diskuse se spojařskou „opozicí“. Na Fénixu měli nejchytřejší hackeři Ameriky rozdrtit předpotopní názory spojařských tradicionalistů a třeba je i přesvědčit, že elita z LoDu jsou ve skutečnosti sympatičtí kluci. *Phrack* udělal premiéře Projektu Fénix důkladnou reklamu a Projekt Fénix měl všechna čísla *Phracku*, včetně Dokumentu 911 ve verzi, kterou *Phrack* publikoval.

Projekt Fénix byl pouze jedním z mnoha - možná stovek - nodů a boardů po celé Americe, které ilegálně přechovávaly Dokument 911. Ale Fénix byl každým coulem boardem Legion of Doom. Pod Mentorovým vedením systematicky provokoval bezpečnostní odborníky telekomunikací. A co horšího, aktivně se pokoušel *získat je na svoji stranu*, udělat z nich sympatizanty elity digitálního undergroundu. Na Fénixu nebyla žádná čísla kreditních karet ani přístupové kódy. Hackerská elita jeho uživatelů ho považovala za přinejmenším technicky legální. Ale Fénix měl špatný vliv; jeho hackerská anarchie rozežírala slabá místa obchodního vlastnictví jako kyselina. Chicagská operační skupina proti počítačové zpronevěře a zneužití počítače byla nyní připravena zahájit operaci v texaském Austinu.

Kupodivu nikoli jedna, ale *dvě* stopy vedly vyšetřování Chicagské operační skupiny směrem k Austinu. Město Austin, podobně jako Atlanta, se stalo významným centrem na informatické mapě amerického jihozápadu, se silným univerzitním výzkumem a sídlem mnoha technologicky vyspělých elektronických firem, například Motoroly, Dellu, CompuAddu, IBM, Sematechu a MCC.

Kde se rozvinul počítačový průmysl, objevili se zpravidla brzy i hackeři. Austin se mohl pochlubit nejen Projektem Fénix, v této době nejvlivnějším undergroundovým boardem LoDu, ale i množstvím unixovských nodů.

Jedním z těchto nodů byl „Elephant“ („Slon“), vedený unixovským konzultantem Robertem Izenbergem. Izenberg, oceňující neuspěchaný jižanský životní styl a nižší běžné náklady, se nedávno přestěhoval do Austinu z New Jersey. V New Jersey pracoval Izenberg pro malou dodavatelskou společnost, vyvíjející unixovské programy přímo pro AT&T. Terminus byl častým hostem na Izenbergově soukromém nodu Elephant.

Po výslechu Terminuse a prozkoumání záznamů NetSysu byli členové Chicagské operační skupiny přesvědčeni, že odhalili gang unixovských softwarových pirátů, zjevně vinných transportem ilegálně zkopírovaného zdrojového kódu AT&T přes hranice států USA. V síti zatažené kolem „dokonalého unixovského hackera“ uvízl i Izenberg.

V Austinu se Izenberg pustil do práce pod Unixem pro texaskou pobočku IBM. Nepracoval už na zakázkách pro AT&T, ale stále udržoval kontakty se svými přáteli v New Jersey a přihlašoval se k tamním unixovským počítačům AT&T v podstatě kdy se mu zachtělo. Izenbergova činnost připadala Chicagské operační skupině vysoce podezřelá. Izenberg mohl docela dobře pronikat do počítačů AT&T, krást jejich software, které od něj prostřednictvím sítě unixovských nodů přebíral Terminus a možná i další společníci. A tato data nestála jen 79 449 dolarů, ale statisíce!

21. února 1990 se Robert Izenberg vrátil domů z práce v IBM a zjistil, že všechny počítače v jeho bytě v Austinu záhadně zmizely. Přirozeně předpokládal, že byl okraden. Jeho node Elephant i ostatní stroje, poznámkové bloky, diskety, pásky, všechno pryč! Ale přitom se zdálo, že nic jiného nechybí - a v bytě nebyl nepořádek. Asi po pěti minutách se záhada dále zkomplikovala. U dveří Izenbergova bytu se objevil agent Tajné služby USA Al Soliz z úřadovny v Austinu, doprovázený bezpečnostním specialistou Texaské univerzity Larrym Coutoriem a všudypřítomným Timem Foleym. Byli v civilu: džíny, tričko. Požádali o rozhovor, a Tim Foley obvinil Izenberga, že je členem Legion of Doom.

Izenberg odpověděl, že o žádné „Legii soudného dne“ v životě neslyšel. A co takhle o jistém ukradeném Dokumentu 911, představujícím přímé ohrožení policejních linek nouzového volání? Izenberg prohlásil, že ani o tom nic neví.

Vyslýchající tomu nemohli uvěřit. Co mu říká jméno Terminus?

Kdo?

Řekli mu jeho pravé jméno. Ale ano, odpověděl Izenberg. *Tohohle* chlápka zná docela dobře - vede na Internetu diskuse o počítačích AT&T, zejména o AT&T 3B2.

AT&T si dala záležet na uvedení tohoto počítače na trh, ale jako mnoho jiných velkorysých pokusů této společnosti o proniknutí mezi výrobce počítačů, neměl ani 3B2 zrovna skvělý úspěch. Izenberg sám kdysi pracoval na zakázce pro odbor AT&T zajišťující technickou podporu 3B2. Celý tento odbor byl zrušen. Tou nejlacinější a nejrychlejší cestou, jak získat pomoc při zvládání tohoto zlomyslného kusu železa, nyní bylo připojit si jednu z diskusních skupin, které vedl Terminus na Internetu, a získat expertní pomoc zdarma od přívětivých hackerů.

Přirozeně, konverzaci v těchto skupinách by si AT&T nedala za rámeček... *tohle* byl problém?

Foley řekl Izenbergovi, že Terminus získává kradený software přes jeho, Izenbergův počítač.

Izenberg pokrčil rameny. Přes jeho node UUCP proudilo dobrých osm megabytů dat denně. Nody UUCP je chrlily jako požární hadice vodu. Elephant byl přímo připojen k NetSysu - přirozeně, vždyť Terminus byl expert na 3B2 a Izenberg pro tento počítač programoval. Izenberg byl připojen i k „attctc“ a k Texaské univerzitě. Terminus byl známý unixovský expert a mohl si na Elephantu dělat prakticky co chtěl. Izenberg s tím nemohl nic dělat. Technicky to bylo nemožné - jehla v kupce sena.

V průběhu čtyřhodinového výslechu vyzval Foley Izenberga, aby se přiznal, že Terminus a on se zúčastnili spiknutí a že je členem Legion of Doom. Izenberg to odmítl. Nebyl žádný bláznivý nezletilý hacker - bylo mu dvaatřicet a neměl ani vlastní „handle“. Izenberg byl bývalý televizní opravář a specialista na elektroniku, který se začal živit Unixem až jako dospělý. Izenberg a Terminus se nikdy fyzicky nesetkali. Pravda, jednou od něj lacino koupil vysokorychlostní modem.

Foley mu řekl, že tento modem (Telenet T2500, s přenosovou rychlostí 19.2 kilobaudů, který právě opustil Izenbergův byt do úschovy Tajné služby USA) byl pravděpodobně kradený. Izenberga to zarazilo; ale na druhé straně, většina jeho vybavení, jako vybavení skoro každého jiného nezávislého počítačového profesionála, byla zakoupena se slevou, prodávaná z ruky do ruky v sérii výměnných obchodů, z nichž ne všechny by snesly oficiální pozornost. Neexistoval žádný důkaz, že modem je kradený, a i kdyby byl, Izenberg stejně nemohl pochopit, proč by mu kvůli tomu měli sebrat veškerou elektroniku v domě.

Nicméně, pokud Tajná služba USA usoudila, že potřebuje jeho počítač pro zajištění národní bezpečnosti - nebo tak něco - byl Izenberg

ochoten se přizpůsobit. Odhodlal se obětovat své profesionální vybavení za dvacet tisíc dolarů, v duchu účinné spolupráce s ochránci zákona a morálních závazků řádného občana.

Robert Izenberg nebyl zatčen. Nebyl obžalován ze žádného zločinu. Jeho node UUCP - s přibližně 140 megabyty souborů, pošty a dat, patřících jemu a asi tuctu jeho naprosto nevinných uživatelů - byl zabaven jako „důkaz". I s disky a páskami přišel Izenberg asi o 800 megabytů dat.

Uplynulo šest měsíců, než se Izenberg rozhodl zatelefonovat do úřadovny Tajné služby a zeptat se, jak se jeho případ vyvíjí. Tehdy poprvé uslyšel jméno William Cook. Ještě v lednu 1992, dva roky po domovní prohlídce, bloudil Robert Izenberg, stále neobžalovaný ze žádného zločinu, labyrintem soudů ve snaze zachránit své profesionální vybavení za tisíce dolarů.

Izenbergův případ si nezískal naprosto žádnou pozornost tisku. Tajná služba USA přišla do domu v Austinu a odnesla si unixovský board. Operace se nesetkala s žádným odporem.

Ale zpráva o ní se rozšířila mezi členy Legion of Doom. Mentor dobrovolně zastavil svůj Projekt Fénix. Byla to škoda, zvláště proto, že na Fénixu se skutečně objevili bezpečnostní experti telekomunikací, jak Mentor doufal - spolu s obvyklým nesourodým davem špiček, známých a obdivovatelů LoDu, telefandů a hackerů. Mezi uživateli byl „Sandy" Sandquist z bezpečnostního odboru US SPRINT a nějaký Henry Kluepfel přímo z Bellcore! Kluepfel přívětivě konverzoval s hackery na Fénixu od 30. ledna (čtrnáct dní po kolapsu telefonní sítě AT&T). Přítomnost takové spojařské hvězdy byla pro Projekt Fénix velkým povzbuzením.

Nicméně Mentor cítil potíže. Atlanta v troskách, *Phrack* v nebezpečí, podivné události kolem unixovských nodů - to vše nabádalo k opatrnosti. Projekt Fénix byl zastaven.

Kluepfel samozřejmě monitoroval board LoDu pro své vlastní cíle - a pro cíle Chicagské operační skupiny. Už v červnu 1987 se Kluepfel napojil na texaský undergroundový board „Phreak Klass 2600". Na něm našel chicagského mladíka jménem „Shadowhawk" („Stínový jestřáb"), který se vychloubal svými výpravami za soubory AT&T a plány proniknout do počítačů Bellcore užívaných AT&T pomocí trojských koňů. Kluepfel o tom informoval Cooka v Chicagu, Shadowhawkův počítač byl zabaven Tajnou službou USA a Shadowhawk sám skončil ve vězení.

Nyní byl na řadě Projekt Fénix. Projekt Fénix se zaštiťoval řečmi o „legalitě" a „pouze akademickém zájmu", ale byl cítit undergroundem. Byl na něm *Phrack*. Byl na něm Dokument 911. Byla na něm spousta podezřelých řečí o pronikání do systémů, včetně dalekosáhlých a nebezpečných plánů na jakousi „dešifrovací službu", kterou chtěl Mentor se svými přáteli založit pro podporu získávání zašifrovaných hesel z „nabouraných" počítačů.

Mentor byl dospělý. Tam, kde pracoval, byla BBS. Kluepfel se připojil i k tomuto boardu a zjistil, že se jmenuje „Illuminati". Vlastnila ho jakási firma jménem „Steve Jackson Games". 1. března 1990 se mašinérie austinského zátahu rozjela.

Ráno 1. března - ve čtvrtek - byl jednadvacetiletý student Texaské univerzity „Erik Bloodaxe", co-sysop Projektu Fénix a aktivní člen Legion of Doom, probuzen hlavní policejní pistole na svém spánku.

Nervózní Bloodaxe sledoval, jak agenti Tajné služby USA zabavují jeho 300-baudový terminál a v jeho souborech nalézají drahocenný zdrojový kód nechvalně známého „Internet Worma" Roberta Morrise. Ale Bloodaxe, zkušený veterán, měl podezření, že k něčemu takovému může dojít. Všechno jeho nejcennější vybavení bylo ukryto někde jinde. Návštěvníci nicméně sebrali veškerou elektroniku včetně telefonu. Odolala jim jen jeho robustní videohra Pac-Man, příliš těžká, než aby se s ní dalo hýbat; nechali ji tedy na místě.

Bloodaxe nebyl zatčen. Nebyl obžalován ze žádného zločinu. Nicméně po více než dvou letech policie stále nevrátila nic z toho, co mu bylo zabaveno.

Mentor nebyl tak opatrný. Ranní razie vyhnala jeho i jeho manželku z postele ve spodním prádle a šest agentů Tajné služby USA, doprovázených austinským policistou a samotným Henrym Kluepfelem, mělo bohatý lov. V bílé dodávce Chevrolet patřící Tajné službě USA zmizely: klon IBM PC-AT se čtyřmi mega paměti a stodvaceti megabytovým pevným diskem, laserová tiskárna Hewlett-Packard LaserJet II, naprosto legální a velice drahý operační systém SCO-Xenix 286, diskety s programem PageMaker a dokumentace k němu a textový editor Microsoft Word. Mentorova manželka měla na pevném disku nedokončenou diplomovou práci; i o tu přišla, stejně jako o telefon. Ještě o dva roky později zůstávaly všechny tyto věci v úschově policie.

Mentor zůstal pod dozorem ve svém bytě, zatímco se agenti připravovali k razii ve Steve Jackson Games. Nijak jim nebránila skutečnost, že šlo o ředitelství podniku a nikoli o soukromý dům. Stále ještě bylo brzy ráno; v práci dosud nikdo nebyl. Agenti se chystali rozbít dveře, ale Mentor, odposlouchávající vysílačky Tajné služby, je poprosil, aby to nedělali, a nabídl svůj klíč k budově.

Detaily dalšího průběhu operace jsou nejasné. Agenti nenechali nikoho jiného vstoupit dovnitř. Povolení k prohlídce, které posléze předložili, nebylo podepsáno. Zjevně snídali v místním stánku s občerstvením, protože uvnitř byly později nalezeny papírové obaly hamburgerů. Důkladně také okusili gumové medvídky ze sáčku jednoho ze zaměstnanců SJG. Nálepka „Dukakis for President" byla stržena ze zdi.

Zaměstnanci SJG, přicházející do zaměstnání a očekávající normální pracovní den, byli zastavováni u dveří a krátce vyslýcháni agenty Tajné služby USA. V úžasu sledovali, jak agenti, vyzbrojení páčidly a šroubováky, vycházejí se zajatými počítači. Dveře venkovních skladů otevřeli řezačkou. Agenti byli oblečeni v modrých větrovkách s nápisem „TAJNÁ SLUŽBA" na zádech, teniskách a džínách.

Jacksonova společnost přišla o tři počítače, několik pevných disků, stovku disket, dva monitory, tři modemy, laserovou tiskárnu, různé elektrické šňůry, kabely a adaptéry (a kupodivu i o malý pytlík šroubků, matiček a podobných drobností). Zabavení BBS Illuminati připravilo SJG o všechny programy, textové soubory a soukromou elektronickou poštu na boardu. Ztráta dalších dvou strojů byla pro firmu stejně závažná, protože na nich byly elektronicky zaznamenané smlouvy, finanční rozbory, seznamy a adresáře odběratelů, údaje o zaměstnancích, obchodní korespondence a neméně důležité koncepty nových her a herních knih.

Nikdo ze Steve Jackson Games nebyl zatčen. Nikdo nebyl obžalován ze žádného zločinu. Nebylo vzneseno vůbec žádné obvinění. Všechny odnesené věci byly oficiálně zadrženy jako „důkaz" zločinů, které nebyly nikdy specifikovány.

Po precedenčním procesu s *Phrackem* byl skandál kolem Steve Jackson Games tím nejbizarnějším a nevíce znepokojujícím incidentem Zátahu na hackery v roce 1990. Razie Chicagské operační skupiny ve vydavatelství vědecko-fantastických her vyprovokovala bzučící roj sporů kolem občanských práv a stala se zárodkem zásadního střetu, jehož rostoucí důsledky se neustále komplikovaly ještě o dva roky později.

Pronásledování Dokumentu 911 skončilo s razií ve Steve Jackson Games. Jak jsme viděli, byly v Americe stovky, možná tisíce uživatelů počítačů, vlastnících Dokument 911. Teoreticky byla Chicagská skupina ze zákona naprosto oprávněna provést domovní prohlídku u kteréhokoli z těchto lidí a legálně zabavit počítač každého odběratele *Phracku*. Ale na Jacksonově boardu Illuminati nebyla žádná kopie Dokumentu 911. A tam chicagští vyšetřovatelé skončili; od té doby žádnou razii neuskutečnili.

Dalo by se předpokládat, že Rich Andrews a Charlie Boykin, kteří upozornili bezpečnostní odborníky telekomunikací na Dokument 911, nebudou oficiálními orgány nijak podezříváni. Ale jak už jsme viděli, ochota „plně spolupracovat" nabízí malou, pokud vůbec nějakou záruku před stíháním federálními lovci hackerů.

Richard Andrews měl kvůli Dokumentu 911 velké potíže. Andrews žil v Illinois, na domácím hřišti Chicagské operační skupiny. 3. a 6. února byl jeho dům i jeho pracoviště prohledáváno Tajnou službou USA. I on přišel o své počítače a byl důkladně vyslýchán (zatčen nicméně

nebyl). Andrews měl prokazatelně ve svém vlastnictví údajně ilegální kopie následujícího softwaru (mimo jiné): UNIX SVR 3.2; UNIX SVR 3.1; UUCP; PMON; WWB; IWB; DWB; NROFF; KORN shell '88; C++; QUEST. Andrews získal tento copyrightovaný kód - AT&T si ho cenila na více než 250 000 dolarů - prostřednictvím unixovské sítě, většinou jako osobní dárek od Terminuse. Co bylo možná ještě horší, Andrews připustil, že tuto laskavost oplatil a předal mu kopii zdrojového kódu programu STARLAN, copyrightovaného AT&T.

Dokonce i Charles Boykin, zaměstnanec AT&T, měl problémy. V roce 1990 už téměř zapomněl na Dokument 911, o kterém podal zprávu v září 1988; ostatně od té doby předal Jerrymu Daltonovi dvě další varování, týkající se věcí, které Boykin považoval za mnohem větší bezpečnostní hrozbu než Dokument 911.

Ale v roce 1990, v době Zátahu na hackery, ztratil bezpečnostní odbor AT&T s Boykinovým „Killerem" trpělivost. Tento stroj nepřinášel AT&T žádný přímý zisk a navíc poskytoval útočiště a pomoc mraku podezřelých texaských buranů, kteří neměli s AT&T nic společného a někteří z nich dokonce aktivně ohrožovali její vlastnictví a obchodní zájmy. Ať už Killer získal pro AT&T jakoukoli publicitu a popularitu mezi svými patnácti sty oddaných uživatelů, nebylo to nadále považováno za dostatečnou protiváhu bezpečnostních rizik jeho provozu. 20. února 1990 přijel Jerry Dalton do Dallasu; jednoduše vytáhl telefonní linky ze zástrček a postavil tak překvapené uživatele před hotovou věc. Provoz Killera definitivně skončil a ohromné knihovny programů a velké množství elektronické pošty bylo ztraceno. Killer nebyl nikdy obnoven. AT&T neprojevila žádné zvláštní ohledy na „vlastnictví" jeho 1500 uživatelů. Ať už skladovali na počítači AT&T jakékoli „vlastnictví", prostě o něj přišli.

Boykin, který sám na Dokument 911 upozornil, se ocitl v mračnu podezření. V groteskní repríze razií Tajné služby USA, uskutečněné soukromou bezpečnostní službou, byl jeho dům navštíven bezpečnostními specialisty AT&T a jeho vlastní počítače odneseny.

Ale Boykinův případ měl výrazné specifické rysy. Boykinovy diskety a jeho osobní počítače byly jeho zaměstnavatelem urychleně prozkoumány a po několika dnech zdvořile vráceny (na rozdíl od věci zabavených Tajnou službou USA, které běžně zůstávají v úschově měsíce či léta). Boykin nebyl obviněn z žádného zločinu ani neetického chování a zůstal zaměstnán u AT&T (byť už v září 1991, v 52 letech, odešel do důchodu).

Je zajímavé všimnout si, že Tajná služba USA neodnesla Boykinova Killera a nezabavila počítač patřící AT&T. Neprohledali ani Boykinův dům. Zjevně jim naprosto stačilo slovo bezpečnostního odboru AT&T, že zaměstnanec AT&T a node AT&T neobsahují žádný hackerský kontraband a jsou v úplném pořádku.

Dnes už to jsou digitální loňské sněhy, protože Killerových 3200 megabytů texaské elektronické komunity bylo v roce 1990 smazáno a Killer sám byl odvezen ze státu Texas.

Ale zkušenosti Andrewse a Boykina, stejně jako uživatelů jejich systémů, zůstaly vedlejšími. Nezačaly nabývat společenské, politické a právní důležitosti těch sporů, které se rozvinuly, pomalu, ale nezadržitelně, kolem razie ve Steve Jackson Games. Musíme nyní obrátit svoji pozornost na samotné vydavatelství Steve Jackson Games a vysvětlit, jaký to byl podnik, co ve skutečnosti dělal a jak se mu podařilo přilákat své nekonvenční a nebezpečné potíže. Čtenář si možná vzpomene, že toto není poprvé, ale podruhé, co se společnost SJG objevila v tomto příběhu; hra od Steve Jackson Games zvaná GURPS byla oblíbeným koníčkem Urvila, hackera z Atlanty, a Urvilovy vědecko-fantastické poznámky byly volně smíchány s poznámkami o jeho skutečných průnicích do počítačů. [...]

Profesionální autoři her se chopili nové příležitosti. Jedním z nich byl i Mentor, který byl velkým příznivcem cyberpunku, podobně jako většina jeho přátel z Legion of Doom. Mentor byl přesvědčen, že nastal čas napsat *opravdovou* cyberpunkovou hrací knihu - takovou, kterou budou moci hrát titáni počítačového zločinu z Legion of Doom, aniž by se jí museli smát. Tato kniha, *GURPS Cyberpunk*, bude mít autentickou on-line kulturu.

Mentor byl pro tento úkol výjimečně dobře kvalifikován. Věděl přirozeně o pronikání do počítačů a soubojích po síti mnohem víc než kterýkoli cyberpunkový autor před ním. Ale nejen to, byl i dobrý spisovatel. Bohatá představivost, zkombinovaná s instinktivním citem pro to, jak pracují systémy a zvláště kde jsou jejich slabá místa, to jsou pro profesionálního autora her velmi užitečné kvality.

1.března byl *GURPS Cyberpunk* už téměř hotov, připravený k tisku a k expedici. Steve Jackson očekával, že se bude velmi dobře prodávat, a doufal, že jeho společnost finančně zabezpečí na několik měsíců. *GURPS Cyberpunk*, stejně jako ostatní „moduly" GURPS, nebyla „hra" jako třeba „Dostihy a sázky", ale *kniha*: paperback silný jako tlustý časopis, s výraznou barevnou obálkou a plný textu, ilustrací, tabulek a poznámek. Byl propagován jako hra a měl sloužit jako pomůcka při hraní her, ale byla to kniha, s číslem ISBN, publikovaná ve státě Texas, copyrightovaná a prodávaná v knihkupectvích. A nyní byla tato kniha, uložená v počítači, zabavena do úschovy Tajnou službou USA.

Den po razii navštívil Steve Jackson místní úřadovnu Tajné služby USA v doprovodu právníka. Vyžádal si rozhovor s Timem Foleym (který byl ještě stále v Austinu) a chtěl svoji knihu zpět. Ale to nebylo tak jednoduché. *GURPS Cyberpunk*, jak řekl agent Tajné služby užaslému podnikateli, byla „příručka pro počítačové zločince".

„Je to sci-fi," tvrdil Jackson.

„Ne, je to pravé." Toto tvrzení bylo různými agenty mnohokrát opakováno. Jacksonova zlověstně přesná hra se přesunula ze světa čisté, tajemné, privátní fantazie do světa velké, mlhavé a vysoce medializované fantazie Zátahu na hackery. O pravém důvodu domovní prohlídky nepadla ani zmínka. Podle povolení k ní vyšetřovatelé očekávali, že najdou na Jacksonově boardu Dokument 911. Ale toto povolení bylo zapečetěno, což je procedura, ke které se policisté zpravidla uchylují jen tehdy, hrozí-li zjevně ohrožení života. Skutečný důvod k prohlídce nebyl zjištěn, dokud se Jacksonovým právníkům nepodařilo povolení odpečetit o mnoho měsíců později. Agenti Tajné služby USA ani členové Chicagské operační skupiny proti počítačové zpronevěře a zneužití počítače neřekli Stevu Jacksonovi naprosto nic o nějakém ohrožení policejních linek systému 911. Nezmínili se o Atlantské trojce, *Phracku*, Knight Lightningovi ani o Terminusovi.

Jackson byl ponechán v představě, že jeho počítače byly zabaveny, protože měl v úmyslu publikovat vědecko-fantastickou knihu, kterou policie považovala za příliš nebezpečnou, než aby mohla být vydána.

Zákon a pořádek

Zločinné boardy / Největší světová razie na hackery / Dejte jim lekci / Tajná služba Spojených států amerických / Tajná služba proti penězokazům / Procházka městem / FCIC: oblak s ostřím / Šerifové elektronického pohraničí / Škola stopařů

Ze všech různých policejních akcí roku 1990 byla „Operace Sundevil“ tou zdaleka nejznámější. Razie celostátního rozsahu z 8. května 1990 měla bezprecedentní rozsah a dostalo se jí velké, byť dosti selektivní, publicity.

Na rozdíl od aktivit Chicagské operační skupiny neměla Operace Sundevil za cíl zadržet hackery pronikající do cizích počítačů a zkušeně reprogramující telefonní ústředny. Neměla také nic co dělat s hackery kopírujícími software AT&T ani s důvěrnými dokumenty BellSouth.

Operace Sundevil byla razií na tradiční nectnosti digitálního undergroundu: krádeže kreditních karet a zneužívání telefonních kódů. Ambiciózní aktivity Chicaga ani méně známé, nicméně energické akce newyorské policie proti hackerům nikdy nebyly vlastní součástí Operace Sundevil, jež byla řízena z Arizony.

Nicméně po spektakulární razii z 8. května spojila veřejnost, zmatená policejní neochotou podávat informace, panikou hackerů a bezradnými americkými novináři, všechny složky celostátního zátahu na hackery pod společný název Operace Sundevil. „Sundevil“ je stále tím nejznámějším synonymem pro zátah roku 1990. Ale arizonští organizátoři „Sundevilu“ si tuto reputaci ve skutečnosti nezaslouží - stejně jako si mnozí hackeři nezaslouží „hackerskou“ reputaci.

Tento nepřesný přístup se, pravda, dal ospravedlnit. Zmatek byl například podněcován washingtonskou úřadovnou Tajné služby USA, jež odpovídala na dotazy o Operaci Sundevil, vznesené podle Zákona o svobodě informací, odkazy žadatelů na veřejně známé případy Knight Lightninga a Atlantské trojky. A „Sundevil“ byl určitě tou největší složkou zátahu, byl nejlépe naplánovaný a nejefektivněji provedený. Byl to zátah na elektronické podvodníky a jako takovému mu chybělo frenetické tempo války s Legion of Doom; naopak, terče Operace Sundevil byly vybírány s chladnou pečlivostí v průběhu systematického vyšetřování trvajícího plné dva roky.

Těmito terči byly opět BBS.

Boardy mohou být důležitou pomůckou organizovaných krádeží. Na undergroundových boardech probíhají živé, rozsáhlé, detailní a často velice nestydaté „diskuse“ o metodách a aktivitách porušujících zákon. Abstraktně „diskutovat“ o zločinu či o detailech kriminálních případů není protizákonné - ale existují přísné federální i státní zákony proti spikleneckým skupinám, chladnokrevně plánujícím své zločiny.

Policie nepovažuje skupiny lidí, kteří aktivně konspirují o nezákonných cílech, za „kluby“, „debatní salóny“, „skupiny uživatelů“ či „příznivce svobody slova“. Takoví lidé spíše zjišťují, že byli formálně obviněni jako členové „gangů“, „vyděračských skupin“, „spikleneckých organizací“ a „zločinných spolčení“.

Navíc ilegální data přechovávaná na nezákonných boardech sahají mnohem dál než k pouhým verbálním projevům či možnému zločinnému spiknutí. Jak jsme viděli, je v digitálním undergroundu běžnou praxí zveřejňovat na boardech ukradené telefonní kódy, aby je mohl zneužít jakýkoli telefanda či hacker, který o to stojí. Má snad být takovéto zveřejňování digitální kořisti chráněno Prvním dodatkem ústavy? Stěží - ačkoli ani tento spor, jako ostatně většina sporů v cyberspace, není rozhodnut s konečnou platností. Někteří teoretikové tvrdí, že pouhé *oznámení* čísla veřejnosti není ilegální - pouze jeho *užití* je ilegální. Ale policisté pronásledující hackery zdůrazňují, že noviny a časopisy (tedy tradičnější instituce profitující ze svobody slova) ukradené telefonní kódy nikdy nepublikují (i když by to docela dobře mohlo zvýšit jejich náklad).

Ukradená čísla kreditních karet, jež jsou cennější a riskantnější, nebyla na boardech zveřejňována tak často - ale není sporu o tom, že některé undergroundové boardy zprostředkovávaly zprávy o „kreditním nákupu“, zpravidla v soukromé poště.

Undergroundové boardy obsahovaly i praktické programy pro systematické zkoušení telefonních kódů a nájezdy na společnosti poskytující kreditní karty, stejně jako obvyklé provokativní hromady pirátského softwaru, ilegálně získaných hesel, schémat „modrých skříněk“, návodů na pronikání do počítačů, anarchistických a pornografických souborů atd.

Kromě své nepříjemné schopnosti šířit zakázané vědění mají boardy pro profesionálního vyšetřovatele ještě jeden svrchovaně důležitý aspekt. Jsou přímo nacpány *důkazy*. Celý ten neustávající proud elektronické pošty, všechno hackerské vychloubání, chvástání a naparování, dokonce i ukradené kódy a čísla karet, to vše jsou úhledné, kompletní, elektronické záznamy kriminálních aktivit. Jako vyšetřovatel, který zabavil pirátský board, máte k dispozici stejně přesvědčivé důkazy jako z odposlouchávání telefonů a kontrolování pošty. Ale přitom nemusíte odposlouchávat žádné telefony a kontrolovat žádnou poštu. Procedury pro získávání důkazů telefonními odposlechy a kontrolou pošty prošly dlouhým vývojem, jsou přísné a policie, prokurátoři i advokáti obhajoby jim velice dobře rozumějí. Procedury pro získávání důkazů z boardů jsou nové, plné děr a nerozumí jim vůbec nikdo.

Operace Sundevil byla tou největší razií na boardy v historii. 7., 8. a 9. května 1990 bylo zabaveno asi čtyřicet dva počítačových systémů. Boardy běžely přibližně na pětadvaceti z těchto dvaačtyřiceti počítačů. (Neurčitost těchto tvrzení plyne z neurčitosti za a) pojmu „počítačový systém“ a za b) činnosti „běžícího boardu“ - na jednom, dvou nebo třech počítačích.)

V květnu 1990 zmizelo do úschovy policie přibližně pětadvacet boardů. Jak jsme viděli, počet boardů v Americe se dnes odhaduje na 30 000. Předpokládáme-li, že na jednom boardu ze sta probíhají nekalé operace s přístupovými kódy a čísly karet (což je velmi lichotivé ocenění počestnosti jejich uživatelů), plyne z toho, že Operace Sundevil vynechala 2 975 nezákonných boardů. V jejím průběhu byla zabavena asi desetina procenta amerických boardů. Objektivně řečeno, systematický útok na všech frontách vypadá jinak. V roce 1990 měli organizátoři Sundevilu - tým úřadovny Tajné služby USA ve Phoenixu a Úřad generálního prokurátora státu Arizona - seznam přinejmenším *tří set* boardů, které si podle nich zasloužily vydání povolení k domovní prohlídce a zabavení důkazů. Pětadvacet skutečně zabavených boardů byly z těchto kandidátů pouze nejznámější a nejkřiklavější. Všechny tyto boardy byly předem prozkoumány - buď informátory, kteří předali výsledky svého průzkumu Tajné službě, nebo samotnými jejími agenty, kteří nejen že mají modemy, ale také s nimi umějí zacházet. [...]

Žádný zatýkaný hacker dodnes nevytáhl zbraň, ačkoli na boardech se občas chlubí, že přesně tohle udělají. Tyto hrozby jsou brány vážně. Razie na hackery uskutečněné Tajnou službou USA jsou rychlé, důkladné a účastní se jich dostatek (někdy až příliš) mužů; agenti zpravidla rozrazí všechny dveře v domě naráz, někdy s tasenými zbraněmi. Jakýkoli potenciální odpor je rychle uklidněn. Razie na hackery probíhají zpravidla v soukromých domech. A razie v americkém domě může být velmi nebezpečná - lidé snadno zpanikaří, když do jejich soukromí vtrhnou cizinci. Statisticky tou nejnebezpečnější věcí, kterou policista může udělat, je vstoupit do cizího domu. (Druhou nejnebezpečnější je zastavit cizí auto.) Lidé mají doma zbraně. V soukromých domech je zraněno mnohem více policistů než v motorkářských hospodách či masážních salónech.

Během Operace Sundevil, a ostatně nikdy v průběhu Zátahu na hackery, nebyl ovšem zraněn nikdo.

Nevyskytly se ani žádné stížnosti na špatné zacházení s podezřelými. Podezřelí byli zadržováni s tasenými zbraněmi a jejich výslechy byly ostré a dlouhé, ale žádný z nich si v roce 1990 nestěžoval, že by se k němu nějaký policista choval brutálně.

Kromě asi čtyřiceti počítačů bylo během Operace Sundevil zabaveno obzvláště velké množství disket - přibližně 23 000 - a na nich přirozeně všechny možné druhy ilegálních dat: pirátské kopie her, kradené telefonní kódy a čísla kreditních karet, kompletní pošta a software celých pirátských boardů. Tyto diskety, dodnes opatrované policií, představují pro policejní vyšetřování gigantický, téměř nezvládnutelně bohatý zdroj. Těchto 23 000 disket také obsahuje dosud neznámé množství legálně koupených počítačových her, legálního softwaru, teoreticky „soukromé“ elektronické pošty, obchodních záznamů a osobní korespondence všeho druhu.

Standardní formulace povolení k prohlídce při vyšetřování počítačových zločinů dávají velký důraz na zabavení písemných dokumentů stejně jako počítačů - explicitně zmiňují fotokopie, počítačové výpisy, telefonní účty, adresáře, deníky, záznamy, poznámky a korespondenci. V praxi to znamená, že diáře, hráčské časopisy, softwarová dokumentace, literatura faktu o hackerech a počítačové bezpečnosti a někdy i sci-fi knihy mizí do policejní úschovy. Mizí i široké spektrum elektrických spotřebičů, včetně telefonů, televizí, záznamníků, walkmanů, tiskáren, CD disků a magnetofonových pásek.

Ne méně než 150 agentů Tajné služby USA bylo v průběhu Operace Sundevil vysláno do akce. Zpravidla byli doprovázeni příslušníky místní a/nebo státní policie. Většina z těchto policistů - zejména místních - se nikdy předtím žádné razie na hackery nezúčastnila. (To byl ostatně jeden z dobrých důvodů, proč na ni byli pozváni.) Kromě toho přítomnost uniformovaného policisty ubezpečuje lidi na místě razie, že do jejich domu vtrhla opravdu policie. Agenti Tajné služby USA chodí v civilu. A v civilu chodí i bezpečnostní odborníci telekomunikací, kteří je při raziích často doprovázejí (a kteří se nijak zvlášť nesnaží identifikovat jako pouzí zaměstnanci soukromé společnosti).

Typická razie na hackery probíhá asi takto. Za prvé, policie bleskurychle vtrhne dovnitř, všemi vchody najednou a plnou silou, podle předpokladu, že tato taktika sníží ztráty na minimum. Za druhé, potenciální podezřelí jsou okamžitě odděleni ode všech dostupných počítačových systémů, aby neměli šanci odstranit nebo zničit počítačové důkazy. Jsou odvedeni do místnosti bez počítačů, třeba do obývacího pokoje, a hlídáni; ne *ozbrojenou* stráží - revolvery jsou rychle schovány zpět do pouzder - ale přece jenom stráží. Je jim předloženo povolení k domovní prohlídce a jsou varováni, že všechno, co řeknou, může být použito proti nim. Většinou mají hodně co říct, zejména nic netušící rodiče.

Někde v domě je „centrála“ - počítač připojený k telefonní lince (někdy i několik počítačů na několika telefonních linkách). Obvykle je to hackerova ložnice, ale může to být kdekoli v domě; a hledaných míst může být i víc. „Centrála“ je svěřena dvoučlennému týmu agentů, „pátrači“ a „zapisovateli“. „Pátrač“ má počítačovou kvalifikaci, často je to agent, který má případ na starosti a který osobně získal od soudce povolení k domovní prohlídce. Ví, co má hledat, a vlastnoručně uskutečňuje sběr důkazů: rozpojuje kabely, otvírá skříně a zásuvky, prohlíží papírové pořadače a boxy s disketami atd. „Zapisovatel“ fotografuje veškeré vybavení, jak stojí a leží - zvlášť změť kabelů za počítačem, jejíž obnovení může být bez návodu prací přímo sisyfovskou. „Zapisovatel“ také zpravidla vyfotografuje všechny pokoje v domě, aby žádný rafinovaný zločinec nemohl tvrdit, že mu policie během prohlídky něco ukradla. Někteří „zapisovatelé“ používají videokamery nebo diktafony, ale prostý písemný zápis je obvyklejší. Objekty zabavované pátračem jsou očíslovány a popsány, většinou na standardních policejních inventárních lístcích.

Agenti Tajné služby USA nebyli - a nejsou - počítačovými experty. Nedělali - a nedělají - závěry na místě o tom, představuje-li určitý kus počítačového vybavení důkaz či hrozbu. Mohou být přístupní argumentům; mohou například nechat tatínkovi jeho počítač, ale *nemusejí*. Povolení k domovní prohlídce, vydávaná při vyšetřování počítačových zločinů, která byla standardizována počátkem 80. let, používají velmi obecné výrazy, vztahující se na počítače, téměř všechno, co je připojeno k počítači, téměř všechno, čím se počítač ovládá, téměř všechno, co počítač vzdáleně připomíná, plus úplně všechny písemnosti nacházející se v okolí počítače. Vyšetřovatelé počítačových zločinů agenty důrazně upozorňují, aby sebrali všechno.

V tomto smyslu slavila Operace Sundevil úspěch. Zastavila provoz boardů z celé Ameriky, které byly hromadně dopraveny do kriminalistické počítačové laboratoře Tajné služby USA ve Washingtonu, stejně jako 23 000 disket a neznámé množství tištěných materiálů.

Ale zabavení pětadvaceti boardů a gigabytových hor potenciálních důkazů nacházejících se v těchto boardech (a v dalších počítačích jejich majitelů, jež byly rovněž převzaty do policejní úschovy) nebylo ani zdaleka jediným motivem Operace Sundevil. Motivy tak bezprecedentní, velké a ambiciózní akce musejí být chápány jako *politické*. Operace Sundevil byla propagační akcí a jejím cílem bylo vyslat jisté signály a objasnit jisté okolnosti, a to jak veřejnosti, tak různým společenským skupinám lidí okolo elektroniky.

Za prvé - a tato motivace byla podstatná - vyslala policie „zprávu“ digitálnímu undergroundu. Tato zpráva byla velmi jasně formulována Garrym M. Jenkinsem, zástupcem ředitele Tajné služby USA, na tiskové konferenci o Operaci Sundevil ve Phoenixu, 9. května 1990, tedy bezprostředně po razii. Stručně řečeno, hackeři se hrubě zmýlili, když si mysleli, že se mohou schovávat „za své relativně anonymní počítačové terminály“. Naopak, mohou si být jisti, že místní i federální policisté patrolují v cyberspace stejně jako všude jinde a že vědí i o odporných, špinavých doupatech elektronické neřesti, tedy o undergroundových boardech.

Není nijak neobvyklé, že se policie obrací k porušovatelům zákona s takovouto zprávou. Je to standardní zpráva, nový je pouze kontext. V tomto smyslu byly razie „Sundevilu“ digitálním ekvivalentem běžných prohlídek v erotických salónech, sexshopech, barech narkomanů a ilegálních sázkových kancelářích. Při takové razii je zatčeno jen málo lidí, pokud vůbec někdo; žádné výslechy, žádná obvinění, žádné soudy. V těchto případech policie prostě zabavuje: erotické časopisy, pornografické videokazety, sexuální pomůcky, vybavení heren, pytle marihuany...

Samozřejmě, když policisté objeví při razii něco opravdu hrozného, následuje zatýkání a trestní stíhání. Ovšem daleko častěji je jejím důsledkem prostě krátkodobé, ale výrazné narušení uzavřeného světa přestupníků. Cílem je „válka nervů“. „Červená.“ „Studená sprcha“ pro porušovatele zákona. A, samozřejmě, okamžitá ztráta zabavených předmětů. Je velice nepravděpodobné, že cokoli z odneseného materiálu bude kdy vráceno. Ať už jsou podezřelí obviněni, případně odsouzeni, či nikoli, téměř jistě nebudou mít nervy žádat o vrácení svého majetku.

Zatýkání, soudy a vůbec dostávání lidí za mříže musí počítat s všemožnými právními kličkami; ale zajišťování práce pro soudní systém není ani zdaleka jediným úkolem policie. Cílem policie není jednoduše zatýkat lidi a dostávat je do vězení. Policisté chápou svou práci jinak. Policie „chrání a slouží“. Policie „udržuje klid a pořádek“. Stejně jako ostatní formy policejní práce, ani udržování pořádku není exaktní věda. Udržování pořádku je něco jako umělecká disciplína.

Když se skupina hrozivě vyhlížejících mladistvých chuligánů poflakuje na rohu ulice, nikoho nepřekvapí, že k nim přijde uniformovaný

strážník a rázně je vyzve, aby „to rozpustili“. Naopak velmi překvapivé by bylo, kdyby některý z těchto flákačů zamířil k nejbližší telefonní budce, zavolal právníkovi a požádal soud o ochranu svých ústavních práv na svobodu slova a svobodu shromažďování. Ovšem cosi zcela analogického bylo jen jedním z mnoha anomálních důsledků Zátahu na hackery.

Operace Sundevil vyslala i jiné užitečné zprávy dalším společenským skupinám lidí okolo počítačů. Tyto zprávy nemusely být nutně čteny z pódia ve Phoenixu shromážděným novinářům, ale to neznamená, že byly nezřetelné. Uklidňující zpráva byla určena hlavním obětem krádeží kódů a „kreditního nákupu“: telekomunikačním společnostem a bankám poskytujícím kreditní karty. Bezpečnostní specialisté společností používajících elektroniku „Sundevil“ radostně uvítali. Po letech zneužívání techniky a násobících se ztrát příjmů byly jejich stížnosti na bezostyšné porušování zákona vzaty policií vážně. Už žádné vytáčky a krčení ramen; žádné hloupé výmluvy na „nedostatek kvalifikovaných policistů“ a nízkou prioritu vyšetřování počítačových „zločinů bílých límečků“, jež nemají „přímé oběti“.

Odborníci na počítačový zločin již dlouho soudí, že mnoho případů zneužití počítače není oznámeno policii. Považují to za velký skandál svého oboru. Některé oběti si nestěžují, protože si myslí, že policisté jsou počítačově negramotní a nedokážou ani nechtějí vyšetřovat počítačové zločiny. Jiné jsou zahanbeny svou zranitelností a přijímají účinná opatření, aby se vyhnuly publicitě. To platí zvlášť o bankách, jež se obávají ztráty důvěry investorů v důsledku veřejného vyšetřování zpronevěry či telekomunikačního podvodu. A některé oběti jsou tak zmatené svou vlastní moderní technologií, že si ani nevšimnou, že došlo k zločinu - ani tehdy, jsou-li obrány až na kost.

Důsledky této situace jsou neradostné. Zločinci unikají dopadení a trestu. Existující jednotky pro potírání počítačového zločinu nemají práci. Skutečný stav počítačového zločinu - jeho rozsah, povaha, hrozba, kterou představuje, i legální opatření, jež by mu měla bránit - to vše zůstává neznámé. O dalším problému mluví policisté jen zřídkakdy, jakkoli jim působí vážné starosti. Když policie nechrání občany proti zločinu, mohou vzít právo do svých rukou. Telekomunikační společnosti, banky poskytující kreditní karty, velké koncerny udržující rozsáhlé počítačové sítě, které mohou být cílem hackerů - to jsou mocné, bohaté a politicky vlivné organizace. Nejsou ochotné nechat si diktovat pravidla hry od zlodějů (a v podstatě ani od nikoho jiného). Často si platí dobře organizované soukromé bezpečnostní agentury, běžně vedené zkušenými veterány z armády či policie, kteří odešli ze služby veřejnosti na zelenější pastviny soukromého sektoru. Pro policii může být bezpečnostní odborník soukromé společnosti mocným spojencem; ale nenajde-li tento muž spojence v řadách policie, a je-li vystaven tlaku své správní rady, může se potichu pustit do samostatné akce.

A nájemní pomocníci bezpečnostního odboru se vždycky najdou. Soukromé bezpečnostní agentury - a vůbec „obchod s bezpečností“ - v 80. letech bouřlivě rostl. Dnes existují celé špionážní armády „bezpečnostních konzultantů“, „osobních strážců“, „soukromých detektivů“ a „externích expertů“ - všechny druhy podezřelých podnikavců prodávajících „výsledky“ a diskrétnost. Samozřejmě, mnoho z těchto pánů a dam může být příkladem profesionálních i občanských ctností. Ale jak ví každý čtenář detektivních příběhů „drsné školy“, policie zpravidla není nadšena takovou soukromou konkurencí.

Je známo, že některé společnosti si ve snaze o své počítačové zabezpečení najaly hackery. Policii taková vyhlídka přímo děsí.

Policie chrání své dobré vztahy se světem obchodu jako oko v hlavě. Zřídkakdy je některý policista tak indiskrétní, aby veřejně prohlásil, že nějaký významný zaměstnavatel v jeho státě či městě podlehl paranoidním představám a utrhl se ze řetězu. Nicméně policie - a zvláště počítačová policie - je si této možnosti vědoma. Policisté specializovaní na vyšetřování počítačových zločinů běžně tráví polovinu své pracovní doby pěstováním vztahů s veřejností na seminářích a předváděním „živých policajtů“ pro skupiny rodičů či uživatele počítačů, ale zpravidla pro své stálé publikum: potenciální oběti počítačového zločinu. To jsou samozřejmě telekomunikace, banky nabízející kreditní karty a velké koncerny s rozsáhlými počítačovými sítěmi. Policie je důrazně vyzývá, aby jako řádní občané hlásili trestné činy, o kterých se dozvědí, a vznášeli obvinění. Upozorňují, že v příslušných institucích pracují chápaví a schopní lidé, kteří umějí přijmout účinná opatření, dojde-li k počítačovému zločinu. Ale verbální ujišťování je laciné. Operace Sundevil byla opravdová.

A poslední zpráva „Sundevilu“ byla určena pro vnitřní potřebu policejních sborů. Operace Sundevil byla důkazem, že americká počítačová policie dospěla. Byla důkazem, že nyní je možno zorganizovat velkorysé operace. Byla důkazem, že Tajná služba USA a její spojenci z místních policejních jednotek dokáží pracovat jako dobře namazaný stroj (přes komplikace s používáním těch otravných telefonů kódujících hlas). Byla důkazem, že její iniciátoři z arizonské „Organized Crime and Racketeering Unit“ („Jednotka proti organizovanému zločinu a vyděračství“) patří do světové extraligy, co se týče ambicí, organizace a opravdu koncepční velkorysosti.

A posledním tahem štětce byla zpráva, kterou Tajná služba USA poslala svým dávným rivalům z FBI. Podle dekretu Kongresu sdílejí Tajná služba USA a FBI zodpovědnost za federální vyšetřování počítačových zločinů. Žádnou z těchto organizací tento mlhavý kompromis nikdy ani zdaleka neuspokojil. Vypadá to, jako by se Kongres nemohl rozhodnout, která z nich je kvalifikovanější. A stěží existuje nějaký G-man či zvláštní agent, který by v této otázce neměl zcela jasno. [...]

Nikdo, kdo se zajímá o Operaci Sundevil - a vůbec o americký počítačový zločin - nemůže neznat jméno Gail Thackerayové, pomocné státní zástupkyně státu Arizona. Příručky pro vyšetřovatele počítačových zločinů často uvádějí její skupinu jako příklad a citují její práce; měla nejvyšší funkci ve státní administrativě ze všech úředníků specializujících se na odhalování počítačové trestné činnosti. Její jméno bylo uvedeno v tiskové zprávě o Operaci Sundevil (byť skromně notný kus za místním federálním prokurátorem a šéfem úřadovny Tajné služby USA ve Phoenixu). Jak se komentáře k Zátahu na hackery - a jeho kritika - začaly množit, stávala se arizonská státní úřednice čím dál tím známější. Ačkoli neřekla téměř nic specifického o samotné Operaci Sundevil, byla Gail Thackerayová autorkou těch nejlakoničtějších výroků začínající propagandistické války, třeba „Agenti pracují v dobré víře, a nemyslím, že totéž můžete říci o hackerské komunitě“. Dalším bylo slavné „Nejsem žádný prokurátorský fanatik“ (v *Houston Chronicle* 2. září 1990). Ve stejné době zachovávala Tajná služba USA svou obvyklou diskrétnost a Chicagská operační skupina, poučená následky skandálu kolem Steve Jackson Games, úplně zalezla.

Při uspořádávání své rostoucí kolekce novinových výstřižků jsem si potvrdil, že Gail Thackerayová je ve srovnání s ostatními veřejnými zdroji o policejních operacích úplnou fontánou vědomostí.

Rozhodl jsem se, že bych se s ní měl seznámit osobně. Napsal jsem jí do arizonského úřadu státního zástupce.

Nejen že mi zdvořile odpověděla, ale k mému úžasu velice dobře věděla, co je to „cyberpunková“ science-fiction.

Krátce poté přišla Gail Thackerayová o zaměstnání. A já jsem dočasně pověsil na hřebík svou kariéru sci-fi spisovatele a stal se novinářem specializujícím se na počítačový zločin. Začátkem března 1991 jsem přiletěl do Phoenixu v Arizoně udělat interview s Gail Thackerayovou pro svou knihu o zátahu na hackery.

„Kreditní karty bývaly zadarmo,“ říká Gail Thackerayová. „Dneska stojí čtyřicet dolarů - jen na pokrytí ztrát způsobených ‚šidiči‘.“

Elektroničtí zlodějíčci jsou paraziti. Jako jednotlivci nejsou moc nebezpeční, nic zvláštního. Ale nikdy nepřicházejí jako jednotlivci. Přicházejí v tlupách, bandách, houfech, někdy v celých subkulturách. A koušou. Každému, kdo si dnes pořídí kreditní kartu, odsaje tento zvláštní druh komárů nějaké peníze. Které formy elektronického zločinu jsou podle jejího odborného názoru nejhorší, ptám se a nahlížím do svých poznámek. Krádeže kreditních karet? Vloupání do bankomatů? Telefandovství? Průniky do počítačů? Šíření virů? Krádeže přístupových kódů? Manipulace databází? Softwarové pirátství? Pornografické BBS? Černé přijímače satelitní televize? Krádeže kabelového spojení? Je to dlouhý seznam. Jeho odříkávání mě přivádí do pesimistické nálady. „Ale ne,“ odpovídá Gail Thackerayová a energicky se naklání nad stůl, nefalšovaně rozčilená. „Nejhorší je telefonní zpronevěra. Falešné loterie, falešné dobročinné sbírky. Podvodné charitativní nadace. S tím,

co tihle lidi ukradnou, by se dal zaplatit státní dluh... Zaměřují se na důchodce, používají kreditní přehledy a demografické statistiky, okrádají staré a slabé.“ Mluví rychle a vztekle.

Založit falešnou nadaci je jednoduché. Podvodníci začali mámit z lidí peníze telefonem už před desetiletími. Anglické slovo „phoney“ (falešný) je odvozeno ze slova „phone“ (telefon)!

Ale dnes je to o tolik *snazší*, strašlivě zjednodušené technologickým pokrokem a komplikovanou strukturou moderní telefonní sítě. Ti samí profesionální podvodníci to dělají znovu a znovu, říká mi Thackerayová, schovávají se za vrstvami nastrčených firem... za devíti nebo desetičlánkovým řetězem falešných holdingových společností po celém kontinentu. Nechají si zavést telefon na falešné jméno do prázdného bezpečného domu. A propojí všechny hovory z tohoto telefonu do jiného telefonu, který klidně může být v jiném *státě*. Neplatí ani telefonní účty; za měsíc se prostě vypaří. A pak se ta samá banda zkušených zlodějů usadí někde jinde, v nějaké jiné Zlámané Lhotě. Koupí nebo ukradnou obchodní přehledy o používání kreditních karet, nacpou je do počítače a nechají si vybrat lidi nad pětašedesát let, kteří dávají hodně na dobročinnost. Živí se tím celá subkultura nelítostných podvodníků.

„‚Žárovky pro slepé‘,“ říká Thackerayová s hlubokým odporem. „Není jim konce.“

I *delikventi* žádají Gail Thackerayovou o radu. Telefandové jí volají do kanceláře. Velice dobře vědí, co je zač. Dolují z ní informace o tom, co mají policisté za lubem a kolik toho vědí. Někdy jí volají celé *skupiny* telefandů, spojené do ilegální telefonické konference. Vysmívají se jí. A, jako obvykle, vychloubají se. Telefandové, opravdoví, nenapravitelní telefandové, prostě *nedokážou zmlknout*. Vydrží se vybavovat celé hodiny.

Jsou-li ponecháni sami sobě, mluví většinou o detailech kolem šizení telefonů; je to asi tak zajímavé jako poslouchat, jak se automechanici baví o pérování a předstihu zapalování. Také pomlouvají jeden druhého. A když mluví s Gail Thackerayovou, obviňují sami sebe. „Mám pásky,“ konstatuje Thackerayová suše.

Telefandové mluví prostě jako blázni. Například „Dial-Tone“ („Volací tón“) z Alabamy strávil svého času půl hodiny prostě čtením ukradených přístupových kódů do záznamníků hlasové pošty. Stovky, tisíce čísel, monotónně recitovaných bez jediné pauzy - abnormální případ. Když je telefanda zatčen, jen zcela výjimečně neprozradí všechny podrobnosti o každém, koho zná.

Hackeři nejsou o nic lepší. Který jiný druh zločinců, pokládá Thackerayová řečnickou otázku, vydává časopisy a pořádá srazy? Zdá se, že nebetyčná drzost takového jednání ji doopravdy dráždí, ačkoli nezaujatého pozorovatele může taková aktivita přimět k pochybám o tom, zdali by hackeři vůbec měli být považováni za „zločince“. Skateboardisté mají časopisy, a dopouštějí se řady deliktů. Amatérští automobiloví konstruktéři mají časopisy, a překračují rychlostní omezení a občas zabíjejí lidi...

Ptám se jí, bylo-li by pro společnost ztrátou, kdyby všichni telefandové a hackeři svůj koníček prostě opustili a nechali ležet ladem, takže už by to nikdo nikdy nedělal. Vypadá překvapeně. „Ne,“ říká bez váhání. „Možná trochu... za starých časů... na MITu... Ale dneska můžete s počítači dělat spoustu úžasných legálních věcí, nepotřebujete se vloupávat do cizích, jen abyste se s nimi naučili zacházet. Tahle výmluva už neexistuje. Můžete se učit, jak je vám libo.“ „Pronikala jste někdy do počítačů?,“ ptám se.

Účastníci kursů v Glyncu to dělají. Aby viděli, kde jsou systémy zranitelné. Tahle představa ji nechává chladnou. Nevzrušuje ji to. „Jaký počítač máte?“

„Compaq 286LE,“ říká tiše.

„A jaký byste *chtěla* mít?“

Po této otázce se v očích Gail Thackerayové rozhoří pravý hackerský oheň. Napřímí se a mluví rychle a vzrušeně: „Amigu 2000, s IBM kartou a Macovskou emulací! Nejvíc hackerů má Amigy a Commodory. A Apply.“ Kdyby měla Amigu, vysvětluje entuziasticky, mohla by zkoumat celé světy disket zabavených jako důkaz pohodlně a prakticky na jediném univerzálním stroji. A laciném. Ne jako ve staré laboratoři na generální prokuratuře, kde měli pravěký CP/M, nějaké Amigy a Apply, pár IBM, všechny možné pomocné programy... ale žádné Commodory. Pracovní stanice na generální prokuratuře jsou Wangy, jednoúčelové počítače pro psaní textů. Krotké stroje uvázané ke kancelářské síti - i když pravda, mají přístup on-line do právnických databází Lexis a Westlaw...

Neříkám nic, ale bezpečně rozpoznávám příznaky. Tato počítačová horečka se šíří vrstvami americké společnosti už léta. Lidé *touží* po megahertzech a megabytech. A je to epidemická choroba; kosí společenské večírky, jejichž účastníci se vrhají do nejhlubších a nejtemnějších propastí konverzace o verzích softwaru a drahých periferiích... Odznak hackerské šelmy. Já ho mám taky. Celá „elektronická komunita“ - ať už to sakra znamená co chce - ho má. Gail Thackerayová ho má. Gail Thackerayová je hackerský policajt. Mojí bezprostřední reakcí je záchvat uražené lítosti: *proč té dámě nikdo nekoupí Amigu?!* Nechce přece žádný superpočítač, žádný Cray X-MP; Amiga je pěkná malá hračka. Podvodníci nás stojí nespočetné milióny; soud s jediným hackerem může snadno přijít na sto tisíc dolarů. Jak to, že nikdo nedá dohromady mizerné čtyři tisíce, aby mohla Gail Thackerayová dělat svoji práci? Za sto tisíc bychom mohli koupit Amigu každému počítačovému policajtovi v Americe. Není jich zas tolik.

A zločinci se učí rychle. Není-li „křivka učení“ příliš příkrá, nevyžaduje-li nová technologie odrazující množství znalostí a zkušeností, jsou zločinci často mezi jejími prvními průkopníky. Zvláště když jim pomáhá skrýt se. Zločinci se topí v penězích. Nové komunikační technologie - pagery, mobilní telefony, faxy, Federální expresní poštu - používali jako první bohatí manažeři, a zločinci. V počátcích používání pagerů a pípátek si obchodníci s drogami tuto technologii zamilovali natolik, že vlastnictví pípátka bylo prakticky důkazem obchodu s kokainem. Amatérská rádia se bouřlivě rozšířila, když byla rychlost na silnicích omezena na 55 mil a její překračování se stalo národním sportem. Obchodníci s drogami posílají hotovost Federální expresní poštou přesto, a nebo možná *právě proto*, že v každém jejím úřadě visí varování, abyste to nikdy nezkoušeli. Federální expresní pošta kontroluje zásilky rentgenem a psy, aby zamezila přepravě drog. Nestačí to.

Mobilní telefony obchodníky s drogami nadchly. Je snadné změnit identifikační číslo mobilního telefonu a zajistit si tak telefonní spojení z pohyblivého místa, bezplatné a prakticky nevystopovatelné. Společnosti poskytující mobilní telefony, které jsou jejich obětí, nyní běžně předkládají ohromné seznamy nezaplacených hovorů do Kolumbie a Pákistánu.

Rozhodnutí soudce Greena o rozdělení AT&T se pro kriminalisty stalo noční můrou. *Čtyři tisíce* telekomunikačních společností. Exponenciální nárůst zpronevěry. Všechno, co se dá za peníze koupit, dostupné pomocí telefonu a čísla kreditní karty. Zločiny beze stop. Celý svět nových elegantních podrazů.

Kdyby si Thackerayová mohla vybrat jedno splněné přání, byla by to přímá legální cesta tímto fragmentovaným labyrintem.

Nějaká nová forma povolení k elektronické domovní prohlídce, elektronická „carte blanche“ vydaná soudcem. Používala by se stejně výjimečně jako odposlech a umožňovala by „elektronický pohotovostní zásah“ - bleskurychlý postup přes státní hranice a zajištění spolupráce všech zainteresovaných provozovatelů klasických i mobilních telefonů, optických, podnikových a počítačových sítí, AT&T a jejích dceřinných společností, nezávislých podniků poskytujících dálkové hovory i majitelů rádií. Nějaké oprávnění, nějaký mocný soudní příkaz, který by dokázal proniknout čtyřmi tisíci různých byrokratických lejster ke zdroji telefonického hovoru, ke zdroji virů, ke zdroji hrozeb šířených elektronickou poštou, výhružek bombami a únosy. „V dnešní době,“ říká, „Lindbergovo unesené dítě vždycky zemře.“

Něco, co by zastavilo Síť, třeba jen na okamžik. Něco, co by jí dalo křídla. Sedmimílové boty. To by potřebovala. „Těm chlapům stačí nanosekundy a já používám Pony Expres.“ A pak je tu přicházející internacionalizace. Elektronický zločin nikdy nebylo snadné lokalizovat a určit

místní orgány, do jejichž pravomoci spadá jeho stíhání. Telefandové a hackeři nesnášejí hranice a překračují je, kdykoli mají příležitost. Angličani. Holanďani. A Němci, zvlášť všudypřítomný Chaos Computer Club. Australani. Ti všichni se v Americe naučili zneužívat telefony. A podsvětí roste. Mezinárodní sítě jsou globální, ale vlády a policie prostě ne. Ani zákony. Ani zákonné principy ochrany občanů.

Ale existuje jeden globální jazyk - angličtina. Telefandové mluví anglicky; je to jejich přirozený jazyk, i když jsou Němci. Angličtina mohla kdysi být jazykem Angličanů, ale nyní je jazykem Sítě; zrovna tak dobře by se jí mohlo říkat „CNNština".

Asiaty telefandovství nijak zvlášť neláká. Zato jsou v první lize organizovaného softwarového pirátství. Nevěnují se mu ani Francouzi. Francouzi se s pomocí počítačů věnují průmyslové špionáži.

Za starých časů pravých hackerů z MITu shazování systémů nikoho nebolelo. Aspoň ne moc. Ne trvale. Teď je situace jiná. Následky jsou horší. Hackeři brzo začnou zabíjet lidi. Už dnes existují metody zahlcení linek systému 911, rozčilující policii a možná vedoucí k smrti nějaké nevinné oběti marně volající o pomoc. Hackeři v počítačích řídících provoz vlaků a letišť jednou někoho zabijí. Možná mnoho lidí. Gail Thackerayová je o tom přesvědčena. [...]

Federální výbor pro počítačové vyšetřování (Federal Computer Investigations Committee čili FCIC) je nejdůležitější a nejvlivnější americkou organizací potírající počítačový zločin. A protože policie jiných zemí přebírá většinu svých metod boje proti počítačovému zločinu z Ameriky, může být FCIC klidně nazván nejdůležitější takovou skupinou na světě.

Je to také organizace, ve srovnání s jinými americkými federálními institucemi, velmi neortodoxní. Jsou v ní místní a státní vyšetřovatelé spolu s federálními agenty. Právníci, účetní auditoři a programátoři specializovaní na počítačovou bezpečnost si vyměňují zkušenosti s uniformovanými strážníky. Zabezpečovací firmy a bezpečnostní experti telekomunikací přicházejí, aby vysvětlili, co umějí jejich nástroje, a žádají o ochranu a spravedlnost. Soukromí vyšetřovatelé, akademičtí experti a komerční poradci přispívají svou troškou do mlýna. FCIC je antitezí formální byrokratické struktury. A jeho členové jsou na to hrdí; chápou, že jejich skupina je abnormální, ale jsou zcela přesvědčeni, že takové, pro státní zaměstnance naprosto *groteskní* chování je *zcela nezbytné*, pokud chtějí dobře dělat svou práci.

Aktivní členové FCIC - z Tajné služby USA, FBI, finanční prokuratury, Ministerstva práce, úřadů federálních prokurátorů, státní policie, vojenského letectva a kontrašpionáže - často navštěvují konference, pořádané na různých místech Spojených států, na své vlastní útraty. FCIC nedostává granty. Členství v něm je bezplatné. Nemá šéfa. Nemá ani kancelář - jen poštovní schránku ve Washingtonu, na Odboru zpronevěry Tajné služby USA. Nemá rozpočet. Nemá plán činnosti. Členové se setkávají třikrát do roka - víceméně. FCIC čas od času vydává brožury, ale nemá stálého vydavatele, pokladníka, dokonce ani sekretářku. Konference FCIC nemají psaný program. Lidé, kteří nepracují pro federální instituce, jsou považováni za „nehlasující členy", ovšem k hlasování prakticky nedochází. Visačky, odznaky ani členské průkazy FCIC neexistují. Všichni členové si navzájem tykají. Je jich asi čtyřicet. Kolik přesně, nikdo neví. Lidé přicházejí a odcházejí, někdy formálně odejdou, ale stále se podílejí na činnosti skupiny. Nikdo se nikdy nepokoušel specifikovat, co přesně znamená „členství" v tomto „výboru".

Jakkoli taková „organizace" může někomu připadat podivná, každý, kdo zná sociální struktury lidí kolem počítačů, ji snadno rozezná.

Ekonomové a teoretici řízení už léta spekulují, že vlna informační revoluce zničí nepružné, hierarchické byrokracie, kde je všechno řízeno centrálně shora dolů. Vysoce kvalifikovaní „zaměstnanci" převezmou mnohem větší zodpovědnost, budou iniciativně zahajovat práci na nových úkolech a řešit je bez dozoru nadřízených, budou se rychle a pružně přesouvat z místa na místo a od jedné úlohy k druhé. Zavládne „ad-hokracie", skupiny lidí spontánně vznikající napříč tradiční organizační strukturou pro řešení konkrétního problému, s významnou pomocí počítačem podporovaných expertiz, a opět zanikající po jeho vyřešení.

V podstatě toto se opravdu stalo ve světě počítačového zločinu. S výraznou výjimkou telefonních společností, které jsou koneckonců přes sto let staré, funguje prakticky *každá* organizace, o které je v této knize řeč, stejně jako FCIC. Chicagská operační skupina, arizonská Jednotka proti organizovanému zločinu a vyděračství, Legion of Doom, přispěvatelé *Phracku*, Nadace elektronického pohraničí - ti *všichni* vypadají a jednají jako „komanda" a „uživatelské skupiny". To všechno jsou elektronické ad-hokracie, spontánně vznikající a měnící svou strukturu podle potřeby. Někteří z nich jsou policisté. Někteří jsou, přísně vzato, zločinci. Někteří jsou političtí lobbyisté. Ale každá z těchto skupin se chová stejně spontánně - „Hej, vy! Strejda má hospodu - pojďte si tam zahrát!"

Každá z těchto skupin se za svůj „amatérismus" stydí a pěstuje si image pro nepočítačový svět - snaží se vypadat co možná nejpůsobivěji, nejseriózněji a nejformálněji. Obyvatelé elektronického pohraničí se tak podobají pionýrům devatenáctého století toužícím po vlastní státnosti. Ale v historické zkušenosti „pionýrů" devatenáctého a jednadvacátého století existují dva zásadní rozdíly.

Za prvé, mocné informační technologie *prospívají* malým, pružným, volně organizovaným skupinám. Vždycky existovali „pionýři", „hobbyisté", „fanoušci", „amatéři", „dobrovolníci", „hnutí", „uživatelské skupiny" a „nezávislí experti". Ale taková skupina, má-li technické možnosti šířit ohromné množství specializovaných informací rychlostí světla svým členům, vládě a tisku, to je prostě úplně jiné zvíře. Je to jako rozdíl mezi úhořem a elektrickým úhořem.

Druhým zásadním rozdílem je, že americká společnost je nyní ve stavu blížícím se permanentní technologické revoluci. Zejména ve světě počítačů je prakticky nemožné *přestat* být pionýrem, pokud neumřete nebo se dobrovolně na všechno nevykašlete. Vývoj se nikdy nezpomalil natolik, aby se scéna mohla nějak institucializovat. „Počítačová revoluce" pokračuje po dvaceti, třiceti, čtyřiceti letech, stále se rozšiřuje do nových oblastí společnosti. Všechno, co doopravdy funguje, je už zastaralé.

Když jste „pionýr" po celou dobu své dospělosti, ztratí pro vás slovo „pionýr" svůj význam. Čím dál tím méně budete chápat svůj způsob života jako přípravu na něco jiného, něco usedlejšího a organizovanějšího, a stále více jako *normální stav*. V pojmu „permanentní revoluce" je ve skutečnosti neodstranitelný rozpor. Když „chaos" trvá dost dlouho, stane se z něj prostě *nový společenský řád* - a historie se opakuje, s novými hráči a novými pravidly. Aplikujte toto tvrzení na svět mužů zákona na konci dvacátého století, a dostanete skutečně originální a pozoruhodné výsledky. Jakákoli byrokratická příručka o vyšetřování počítačových zločinů bude zastarávající, než ji dopíšete, a téměř starožitnost, než bude vytištěna. Pružnost a rychlé reakce FCIC mu dávají v tomto směru velkou výhodu a vysvětlují jeho úspěch. Ani při nejlepší vůli (kterou ostatně nemá) se organizace velikosti FBI nemůže přizpůsobit rychlosti změn teorie a praxe počítačového zločinu. Kdyby se pokusili cvičit všechny své agenty tak, aby byli na špici vývoje, bylo by to *sebevražedné*, protože *nic jiného už by nikdy nestihli*.

FBI učí své agenty základům teorie elektronického zločinu na své základně v Quanticu ve Virginii. A Tajná služba USA pořádá spolu s dalšími federálními organizacemi úspěšné a hojně navštěvované kursy o telefonní zpronevěře, počítačovém zločinu a pronikání do počítačů ve Federálním policejním tréninkovém centru (Federal Law Enforcement Training Center čili FLETC, čteno „fletsy") v Glyncu v Georgii. Ale ani maximální snaha těchto tradičních organizací neodstraňuje absolutní nezbytnost „oblaku s ostřím", jakým je FCIC.

Členové FCIC jsou totiž *učiteli* ostatních policejních institucí. Prakticky a doslovně vzato je Fakulta počítačového zločinu v Glyncu jen jiné jméno pro FCIC. Kdyby autobus s jeho členy havaroval, byli by američtí policisté ve světě počítačového zločinu slepí, hluší a němí, a brzy by pocítili zoufalou nutnost vymyslet FCIC znovu. A teď vůbec není vhodná doba začínat zase od začátku.

11. června 1991 jsem opět přijel do Phoenixu v Arizoně, abych se zúčastnil zatím poslední konference Federálního výboru pro počítačové vyšetřování. Bylo to přibližně dvacáté setkání této slavné skupiny. Údaj je neurčitý, protože nikdo neví, zdali počítat setkání „Kolokvia", jak byl FCIC nazýván v polovině 80. let, předtím, než mu byla dopřána důstojnost vlastní zkratky. [...]

Popovídali jsme si o „Isis", nebo přesněji IACIS čili International Association of Computer Investigation Specialists („Mezinárodní asoci-

ace specialistů na počítačové vyšetřování“). Zabývají se „počítačovými důkazy“ - metodami rozebírání počítačů, jež nezničí důležité údaje. IACIS, která má nyní centrálu v Oregonu, se skládá z vyšetřovatelů ze Spojených států, Kanady, Taiwanu a Irska. „Taiwanu a Irska?“, opakoval jsem. To jsou *Taiwan* a *Irsko* v tomto oboru na špici? No to zrovna ne, připustil můj partner. Jsou to prostě ti, kteří o téhle organizaci uslyšeli první. A mezinárodní rozměr je důležitý, protože problém sám je zjevně mezinárodní. Telefonní linky vedou všude.

Konference se zúčastnil i zástupce Kanadské jízdní, a vypadal velice spokojeně. Nikdo tohoto Kanaďana nevyhodil, protože by mohl představovat ohrožení státní bezpečnosti. Tihle policajti hlídají cyberspace. Pořád mají spoustu starostí s „územní příslušností“ trestných činů, ale pouhá geografie je netrápí. Neukázal se nikdo z Národního úřadu pro letectví a kosmonautiku. NASA má velké problémy s průniky do počítačů, organizovaných zejména australskými nájezdníky a nechvalně známými členy skupiny Chaos Computer Club, a v roce 1990 vzbudilo krátkou, ale intenzívní pozornost tisku odhalení, že jedna z neveřejných ústředen NASA v Houstonu byla systematicky zneužívána gangem telefandů. Ale fondy NASA byly seškrtány. Museli omezit všechno.

OSI čili Office of Special Investigations („Úřad zvláštního vyšetřování“) vojenského letectva USA je *jedinou* federální organizací zabývající se výhradně počítačovou bezpečností. Čekalo se, že se ukáží v plné síle, ale někteří odřekli - Pentagon omezuje rozpočet.

Jak se prázdné láhve hromadily, atmosféra se uvolňovala a přítomní začali vyprávět veselé příhody. „Jsou to policajti,“ usmála se Thackerayová. „Když nemluví o práci, mluví o ženských a pití.“

Vyslechl jsem příhodu o člověku, který byl požádán o „zkopírování“ diskety a *zkopíroval nálepku na ní*. Strčil disketu do kopírky a výboj statické elektřiny zcela zničil informace, které na ní byly.

Nějaký jiný nešťastník hodil celý balík zkonfiskovaných disket do kufru policejního vozu, hned vedle rádia. Rádiový signál je vymazal. Poslechli jsme si o Dave Genesonovi, prvním prokurátorovi, který vznášel obžaloby v případech počítačových zločinů. Dave Geneson měl sprinterský start, což je při přechodu do světa počítačového zločinu první ctností. Většina diskutujících souhlasila s tím, že je snazší porozumět nejprve počítačům a potom policejní a prokurátorské práci. Můžete vzít některé lidi od počítačů a udělat z nich dobré policajty - ale samozřejmě musejí mít *policajtskou mentalitu*. Musejí mít pouliční instinkty. Trpělivost. Vytrvalost. A diskrétnost. Musíte si být jistí, že to nejsou žádní divočáci, vejtahové, kovbojové.

Většina z lidí u baru pracovala původně jako vojenští bezpečnostní experti nebo policisté vyšetřující obchod s drogami či vraždy. Byl vyjádřen nezdvořilý názor, že vojenský expert je nesmyslný pojem a také že i odpudivý svět vražd je čistší než operace proti obchodníkům s drogami. Jeden z přítomných pracoval pod cizím jménem na drogovém případu v Evropě nepřetržitě čtyři roky. „Už jsem se skoro vzpamatoval,“ prohlásil s kamennou tváří, s černým, sžíravým, vpravdě policajtským humorem. „Teď už dokážu říct ‚mrd‘ a nestrkat před něj ‚matku‘.“

„V policajtském světě,“ prohlásil jiný, „je všechno dobré a špatné, černé a bílé. U počítačů je všechno šedivé.“

Jeden ze zakládajících členů FCIC, který byl členem této skupiny už v době, kdy byla ještě Kolokviem, vyprávěl o tom, jak se k tomu dostal. Dělal ve Washingtonu v oddělení vražd a byl vyslán vyšetřovat „hackerský“ případ. Podle slova „hack“ („sekat“) přirozeně předpokládal, že má najít psychopata s nožem, a přišel do počítačového střediska očekávaje krev a mrtvolu. Když mu konečně došlo, o co jde (po hlasitých a marných výzvách, aby programátoři „mluvili anglicky“), zavolal na velitelství a řekl jim, že o počítačích nic neví. Odpověděli mu, že všichni ostatní vědí zrovna tolik a ať se sakra kouká dát do práce.

Takže použil srovnání. Analogii. Metaforu. „Někdo se vloupal do vašeho počítače, jo?“ Násilné vniknutí - to znám. „Jak se dostal dovnitř?“ „Telefonem.“ Výhružné telefonáty, to je jasné! Potřebujeme záznamník a zjistit volajícího!

Fungovalo to. Lépe než nic. A fungovalo to mnohem líp, když se seznámil s dalším policajtem, který řešil něco podobného. A ti dva našli dalšího, a dalšího, a Kolokvium bylo brzy na světě. Velkou výhodou bylo, že snad všichni znali Carltona Fitzpatricka, počítačového lektora z Glynka.

Ledy se prolomily ve velkém stylu v Memphisu v roce 1986. Kolokvium přitáhlo spoustu nových lidí - z Tajné služby, z FBI, od vojáků, z jiných federálních agentur - profesionály. Nikdo nechtěl nikomu říct ani slovo. Obávali se, že kdyby se to dostalo k jejich šéfům, přišli by o místo. Strávili nepříjemně opatrné odpoledne.

S formalitami se nedostali nikam. Ale když oficiální program skončil, přinesli organizátoři basu piv. A jakmile účastníci opustili byrokratické formace a kompetenční spory, všechno se změnilo. „Otevřel jsem své srdce,“ vzpomínal hrdě jeden z veteránů. Než nastala noc, stavěli z prázdných pivních plechovek pyramidy a málem skládali vlastní bojovou píseň.

FCIC není jedinou americkou organizací počítačových policistů. Existovala třeba District Attorneys’ Technology Theft Association („Asociace prokurátorů pro případy krádeží technologií“) čili DATTA, i když ta se specializovala spíše na krádeže čipů, duševní vlastnictví a počítačový černý trh. Nebo High Tech Computer Investigators Association („Asociace počítačových vyšetřovatelů“) čili HTCIA, založená v Silicon Valley v Kalifornii o rok dříve než FCIC, jejímiž členy byly osobnosti jako Donald Ingraham. Nebo Law Enforcement Electronic Technology Assistance Committee („Výbor pro pomoc policii v elektronických technologiích“) čili LEETAC na Floridě a útvary počítačových kriminalistů v Illinois, Marylandu, Texasu, Ohiu, Coloradu a Pennsylvanii. Ale to všechno byly místní skupiny. FCIC byl první organizací v opravdu celostátním měřítku a na federální úrovni.

Členové FCIC žijí na telefonních linkách. Ne na boardech - velice dobře se vyznají v tom, jak boardy fungují, a vědí, že nejsou bezpečné. Každý člen FCIC má telefonní účet, jakému byste neuvěřili. Lidé z FCIC mají už dlouho těsné kontakty s lidmi od telefonů. Cyberspace je jejich přirozeným prostředím.

FCIC má tři základní podskupiny: lektory, bezpečnostní odborníky a vyšetřovatele. Proto se také jmenuje „Výbor pro vyšetřování“ a v jeho názvu se neobjevuje nepopulární termín „počítačový zločin“. Oficiálně je FCIC „střechovou organizací agentur, nikoli jednotlivců“; neoficiálně je pole jeho působnosti tak specializované, že význam jednotlivců je zásadní. Všichni přítomní musejí být osobně pozváni, a prakticky každý člen FCIC se považuje za živý důkaz tvrzení, že doma není nikdo prorokem.

Slyším to znovu a znovu, různými slovy, ale stejným tónem. „Připadal jsem si jako poustevník, který si povídá pro sebe.“ „Byl jsem úplně izolován.“ „Byl jsem zoufalý.“ „FCIC je pro vyšetřování počítačových zločinů v Americe to nejlepší, co může být.“ „FCIC skutečně funguje.“ „Tady najdete lidi, co vám opravdu řeknou, co se ve skutečnosti děje, a ne jen právníky hledající mouchy.“ „Naučili jsme jeden druhého všechno, co víme.“

Upřímnost těchto tvrzení mě přesvědčuje, že jsou pravdivá. FCIC je funkční a nenahraditelný. Je také v zásadním rozporu z tradicí a mocenskou strukturou amerických policejních institucí. Skupina tak neformální a podnikavá jako FCIC pravděpodobně neexistovala od dob počátků Tajné služby USA v 60. letech 19. století. Lidé z FCIC žijí jako lidé jednadvacátého století v prostředí dvacátého století, a jakkoli se dá shromáždit mnoho argumentů pro toto uspořádání, dá se shromáždit i mnoho protiargumentů, a rozpočty kontrolují zpravidla ti, kteří shromažďují protiargumenty. Poslouchal jsem, jak si dva členové FCIC z New Jersey vyměňují životní zkušenosti. Jeden z nich byl v 60. letech motorkářem z poměrně drsného gangu. „Jo, a znal si toho a toho?“, zeptal se jeho kolega z New Jersey. „Kus chlapa, ramenatej.“

„Jo, znal.“

„No tak ten byl od nás. Náš agent v gangu.“

„Vážně? Sakra! Pamatuju si ho. Fajn chlap.“

Thackerayová vzpomínala, jak byla oslepená slzným plynem při protestech proti válce ve Vietnamu ve Washingtonu v listopadu 1969, ze kterých dělala reportáž pro studentský časopis své školy. „Taky jsem tam byl," ušklíbl se jiný policista. „Rád slyším, že ten slzák někoho trefil." On sám byl tak slepý, přiznal se, že později toho dne zatkl malý stromek.

FCIC je podivná skupina, shromážděná náhodou a nezbytností, líheň policistů nového typu. Na světě je spousta specializovaných policajtů - odborníci na skořápkáře, na drogy, na daně, ale pravděpodobně jedinou skupinou, která je stejně izolovaná jako FCIC, jsou asi policisté pátrající po dětské pornografii. Obě tyto skupiny se totiž zabývají spiklenci, kterým velice záleží na výměně ilegálních dat a na zachování své anonymity; a žádný jiný policista o nich nechce ani slyšet.

Členové FCIC poměrně často mění zaměstnání. Zřídkakdy mají veškeré vybavení a trénink, které chtějí a potřebují. A jsou poměrně často žalováni.

Jak se připozdívalo - v baru začali hrát - nálada se stávala pochmurnější. Vláda nikdy nic neudělá, tvrdil kdosi, dokud nedojde k nějakému kolapsu. O počítačové kolapsy není co stát, ale nedá se popřít, že velice prospívají důvěryhodnosti FCIC. Vezměte si třeba „Internet Worm". „Léta jsme varovali před něčím takovým - ale proti tomu, co nás čeká, je to maličkost." Tito lidé očekávají katastrofu. Vědí, že dokud nedojde ke katastrofě, nic podstatného se nezmění.

Další den jsme vyslechli rozsáhlou přednášku muže, který býval počítačovým policistou, dostal se do sporu s jistou arizonskou radnicí a nyní se živil instalováním počítačových sítí (za podstatně vyšší plat). Mluvil o rozebírání sítí z optických kabelů.

I jediný počítač, má-li hodně periférií, je v podstatě „síť" - skupina strojů propojených dráty nesrovnatelně složitějším způsobem než třeba stereo věž. Členově FCIC vyvíjejí a publikují návody, jak zabavovat počítače a jak z nich získávat důkazy. Někdy jsou to jednoduchá pravidla, nicméně pro obyčejného policajta, který dnes může zakopnout o běžící počítač při protidrogové razii či vyšetřování zpronevěry, mohou mít zásadní důležitost. Například: Vyfotografuj systém, než na něj sáhneš. Označ konce všech kabelů, než je odpojíš. „Zaparkuj" hlavičky pevných disků, než s nimi pohneš [u dnešních počítačů je toto zpravidla zajišťováno automaticky - pozn. překl.]. Seber diskety. Nedávej je do magnetického pole. Nepiš na ně kuličkovým perem. Seber manuály. Seber výpisy. Seber poznámky ležící u počítače. Zkopíruj data, než se na ně podíváš, a zkoumej kopii, ne originál.

Náš přednášející rozdal namnožené diagramy typické sítě LAN („Local Area Network" čili „místní síť") odkudsi z Connecticutu. *Sto padesát devět* osobních počítačů, každý se svými vlastními periferiemi. Tři „souborové servery". Pět „hvězdicovitých bran", každá s dvaatřiceti porty. Jedna šestnáctiportová brána na detašovaném pracovišti. A všechny tyto stroje komunikují jeden s druhým, distribuují elektronickou poštu, software a třeba i důkazy o trestné činnosti. Všechny jsou propojeny optickými kabely s vysokou přenosovou kapacitou. Pachatel - policajti často mluví o „pachatelích" - může sedět u PC číslo 47 nebo 123 a mít všechna svá ilegální data na „soukromém" počítači nějakého trouby v jiné kanceláři - nebo v jiném patře - nebo klidně dvě tři míle daleko! Data mohou být i „roztrhána" do nečitelných kousků, ukrytých na různých místech, na celé řadě různých disků.

Přednášející nás vyzval, abychom navrhli postup vyšetřování. Byl jsem naprosto bezmocný. Kdyby záleželo na mně, bylo vše ztraceno. V této jediné budově bylo pravděpodobně více disků, než bylo zabaveno v průběhu celé „Operace Sundevil". „Informátor," řekl někdo. Správně. Lidský faktor vždycky hraje roli, a při přemýšlení o tajemných zákoutích moderní technologie se na něj snadno zapomíná. Policajti umějí přimět lidi, aby se rozpovídali, a lidé od počítačů, je-li jim věnována židle a soustředěná pozornost, budou o svých počítačích mluvit, dokud jim vydrží hlasivky. Byl zaznamenán případ, kdy jediná otázka - „Jak jste to udělal?" - vyprovokovala souvislou pětačtyřicetiminutovou odpověď, zaznamenanou na video, v jejímž průběhu se počítačový zločinec nejen ke všemu přiznal, ale kreslil vysvětlující náčrtky.

***

Lidé od počítačů jsou upovídaní. Hackeři se *vytahují*. Telefandové jsou *patologicky* upovídaní - copak kradou přístupové kódy pro něco jiného, než aby se mohli vybavovat deset hodin v tahu se svými přáteli z druhého konce kontinentu? Lidé, kteří umějí zacházet s počítači, mají opravdu k dispozici arzenál rafinovaných pomůcek a technik, který jim umožňuje zakrýt všechny možné exotické triky, a kdyby o nich dokázali prostě *nekecat*, nejspíš by jim spousta fantastických elektronických zločinů prošla. Ale takhle to nefunguje - nebo přinejmenším, takhle to *dosud nefungovalo*.

Prakticky každý telefanda, který byl kdy chycen, bez váhání obvinil své učitele, své žáky i své přátele. Prakticky každý počítačový zločinec „s bílým límečkem", suverénně přesvědčený o neprůstřelnosti svého elegantního plánu, je nepříjemně překvapen, když se k němu, poprvé v jeho životě, nakloní opravdový, přímočaře agresivní policajt, chytne ho za košili, podívá se mu do očí a řekne: „Tak fajn, hajzlíku - půjdem se projít!" Ani všechen hardware na světě neochrání vaše nervy před reálnými, neoddiskutovatelnými pocity strachu a viny.

Policajti se umějí dostat od bodu A k bodu Z, aniž by kvůli tomu museli číst každé písmeno v abecedě nějakého vyčůraného zloděje. Policajti vědí, jak říznout do masa. Policajti vědí spoustu věcí, které ostatní lidé nevědí.

I hackeři vědí spoustu věcí, které ostatní lidé nevědí. Vědí třeba, jak se telefonní linkou dostat do tvého počítače. Ale policajti mohou přijít *přímo do tvého domu* a zamknout *tebe* a tvůj počítač do různých pevných schránek. Policajt zajímající se o hackery si je může chytit a prostudovat. Hacker zajímající se o policajty se musí spokojit se zprávami z druhé ruky, undergroundovými legendami a tím, co jsou policajti ochotní říct veřejnosti. A Tajná služba USA se nejmenuje tajná, protože má ve zvyku hodně o sobě prozrazovat.

Někteří lidé, informoval nás náš přednášející, se mylně domnívají, že odposlouchávat provoz na optickém kabelu je „nemožné". On se svým synem, pokračoval, si ve své domácí dílně nedávno vyrobili odposlouchávací zařízení pro optické linky. Nechal ho kolovat, spolu s počítačovou kartou LAN, na které byly pomocné obvody, abychom ho poznali, kdybychom se s ním setkali při nějakém vyšetřování. Každý si ho mohl prohlédnout.

Odposlouchávací zařízení vypadalo jako klasický prototyp - kovový váleček dlouhý jako palec se dvěma plastikovými svorkami. Z jedné visely tři tenké černé drátky, každý zakončený malou černou plastikovou krytkou. Když jste ji sundali, mohli jste si prohlédnout optické vlákno - ne silnější než vlas.

Přednášející vysvětlil, že kovový váleček je „vlnový rozbočovač". Zjevně se používal tak, že člověk rozřízl optický kabel, napojil na odříznuté konce dva drátky a opět tak navázal přerušené spojení a pak četl všechna data procházející kabelem na nějakém speciálním monitoru připojeném ke třetímu vývodu. Znělo to docela jednoduše. Rád bych věděl, proč to nikoho nenapadlo dřív. A taky bych rád věděl, kolik má syn přednášejícího, hrající si v domácí dílně, nezletilých přátel.

Dali jsme si pauzu. Muž sedící vedle mně měl na hlavě reklamní baseballovou čepici se sloganem doporučujícím samopaly Uzi. Vyměnili jsme si o nich pár společenských poznámek. Dlouho to byly oblíbené zbraně Tajné služby USA, ale zdá se, že vyšly z módy počátkem války v Perském zálivu, když se našich arabských přátel dotklo, že Američané dávají přednost izraelským zbraním. Kromě toho, jak mě informoval jiný expert, samopaly Uzi se zasekávají. Upřednostňovanou zbraní této třídy je nyní německý Heckler&Koch.

Muž s baseballovou čepicí byl soudní fotograf. Často také pořizoval fotografie v průběhu vyšetřování počítačových zločinů. Pořizoval - než došlo k politickému zemětřesení ve Phoenixu. Nyní byl soukromým detektivem a spolu se svou ženou vedl fotografický salón specializující se na svatby a portrétní fotografie. Jeho příjmy - nutno opakovat - se podstatně zvýšily. Byl stále členem FCIC. Jestli jste náhodou členy FCIC a potřebujete si promluvit s expertem na soudní fotografii, tak tady ho máte, schopného a ochotného. Kdyby se neukázal, ostatní by ho po-

strádali.

Přednášející zdůraznil důležitost předběžného vyšetřování, které musí předcházet zabavení důkazů. Je nezbytně nutné vědět, o kolik počítačů se jedná, jaký je na nich operační systém, kolik lidí je používá, kde jsou ve skutečnosti uložena data. Jednoduše vtrhnout do kanceláře a žádat „všechny počítače“ znamená koledovat si o velký malér.

Diskrétní úvodní vyšetřování je nezbytné. Ve skutečnosti je nezbytná normální tajná operace. *Špiclování*, abychom to řekli jasně.

Při konverzaci po přednášce jsem se zeptal jednoho z účastníků, jestli by nepomohl „trashing“.

Dostalo se mi improvizované přednášky o teorii a praxi „kontroly odpadu“. Policejní „kontrola odpadu“, stejně jako kontrola pošty nebo odposlouchávání telefonů, vyžaduje soudní povolení. Po jeho získání je činnost policistů zcela analogická „odpadování“ hackerů - ovšem důkladnější a mnohem lépe organizovaná. Je tak užitečná, dozvěděl jsem se, že mafiáni ve Phoenixu často používají zamčené popelnice, vybírané specializovanou metařskou společností zachovávající přísná bezpečnostní opatření.

Při vyšetřování jednoho případu „odpadovalo“ komando arizonských policistů jeden dům po čtyři měsíce. Každý týden přijeli kuka-vozem, přestrojení za metaře, odvezli obsah popelnic na skryté místo a pečlivě ho prozkoumali - špinavá práce, zvlášť vzhledem k tomu, že jeden z obyvatel domu se podroboval dialýze ledvin. Všechny zajímavé dokumenty byly očištěny, vysušeny a prozkoumány. Zvláště vydatným zdrojem dat byla odhozená páska do psacího stroje, na níž byl písmeno po písmenu obsah všech dopisů odeslaných z domu. Dopisy byly přepsány policejní sekretářkou, vybavenou velkou stolní lupou. [...]

Atmosféra setkání se nyní změnila s příchodem hostů z Nadace elektronického pohraničí (Electronic Frontier Foundation čili EFF). EFF, jejímž zakladatelům a historii se budeme podrobně věnovat v příští kapitole, je občanská organizace, jež vznikla jako přímá odpověď na zátah na hackery v roce 1990.

Mitchell Kapor, prezident Nadace, a Michael Godwin, její hlavní právník, se vůbec poprvé přišli postavit federálním policistům *muž proti muži*. Kapor s Godwinem, kteří si byli jako obvykle vědomi nekonečných možností publicity, s sebou přivedli vlastního novináře: Roberta Drapera z Austinu, jehož nedávno publikovaná a dobře přijatá kniha o časopise *Rolling Stone* byla stále ještě k dostání. Draper pracoval na reportáži pro *Texaský měsíčník*.

Proces Steve Jackson (a EFF) versus Chicagská operační skupina proti počítačové zpronevěře a zneužití počítače vzbudil v Texasu značnou pozornost. Teď se sešli dva novináři z Austinu, kteří se o něj zajímali. I s Goodwinem (rodákem z Austinu a bývalým novinářem) jsme byli tři. Na obědě jsem si připadal jako na setkání spolužáků po dvaceti letech. [...]

V konferenčním sále Thackerayová srdečně, byť dosti stručně, představila Kapora s Godwinem svým kolegům. Byly rozdány připravené materiály a Kapor se ujal slova. Úspěšný bostonský podnikatel s moderními technologiemi, za normálních okolností rázný šéf svého vlastního impéria a velice dobrý veřejný řečník, byl viditelně nervózní a upřímně se k tomu přiznal. Začal konstatováním, že považuje pronikání do počítačů za neetické a nemorální a že EFF není „fond na podporu hackerů,“ jak se objevilo v tisku. Chvilku se věnoval základní motivaci své skupiny a zdůraznil její dobrou vůli, ochotu naslouchat a snahu o soulad s muži zákona - kdykoli je to, ehm, možné.

Pak, po Godwinově výzvě, náhle poznamenal, že i internetovský node EFF byl nedávno napaden hackery a že EFF na tom nevidí nic směšného.

Po tomto překvapujícím přiznání se atmosféra začala rychle uvolňovat. Brzy Kapor zodpovídal otázky, odrážel námitky, zpochybňoval definice a žongloval s paradigmaty se svým obvyklým gustem.

Kapor měl zjevně značný úspěch se svou inteligentní a skeptickou analýzou podstaty „osobních čísel“ nabízených telekomunikačními společnostmi. (Na tomto poli nebyli FCIC a EFF nikdy ve sporu a nemají žádné valy, jež by chtěli bránit.) Osobní čísla jsou zpravidla propagována jako nástroj pro zvýšení soukromí zákazníků, což Kapor nazval „kouřovou clonou“ a zdůraznil, že skutečným cílem osobních čísel je *umožnit velkým společnostem vybudování rozsáhlých komerčních databází lidí, kteří jim telefonují a faxují*. Zřejmě jen málo lidí v sále tato možnost napadla, možná s výjimkou dvou pozdních příchozích z bezpečnostního odboru telefonní společnosti US WEST, kteří nervózně pokašlávali.

Mike Godwin poté podrobně prezentoval „Občanskoprávní aspekty prohledávání a zabavování počítačů“. Tím jsme se konečně dostali k jádru kontroverze, ke skutečnému politickému sporu. Obecenstvo pozorně poslouchalo a občas se ozývaly hněvivé výkřiky: „Neučte nás naši práci!“ „Těmhle otázkám se věnujeme už léta! Nezapomínáme na ně ani na den!“ „Když nezabavím všechno, zažalují mě poškození!“ „Porušuju zákon, když někomu nechám deset tisíc disků plných *pirátského softwaru* a *kradených kódů*!“ „Naše práce je zabránit lidem porušovat ústavu - my jsme *ochránci* ústavy!“ „Zabavujeme, když víme, že ty věci stejně propadnou na náhradu škody!“

„Jestli mají propadnout, nežádejte o povolení k prohlídce, ale o zabavení propadlé věci,“ navrhl suše Godwin. Zdůraznil, že většina podezřelých z počítačových zločinů *nechce*, aby byly jejich počítače odneseny, na blíže neurčenou dobu, bůhví kam. Prohlídka jim nemusí vadit, ani důkladná prohlídka, ale chtějí, aby byly jejich stroje prohlíženy na místě. „To je máme nechat určit, co nám chtějí dát?“ zeptal se někdo kousavě. „A co kdybyste si vzali kopie dat?“ opáčil Godwin.

„To před soudem nikdy neobstojí.“ „Dobře, tak udělejte kopie, dejte *jim* kopie a vezměte si originály.“

„Hmm.“

Godwin vykreslil systémy BBS jako schránky projevů chráněných Prvním dodatkem americké ústavy, zaručujícím svobodu slova. Postěžoval si, že příručky o vyšetřování počítačových zločinů, vydávané federálními agenturami, dělají boardům špatnou publicitu; tvrdí, že to jsou zločinecká hnízda, plná pedofilů a zlodějů, zatímco ve skutečnosti je naprostá většina z tisíců amerických boardů zcela neškodná a vůbec ne tak romanticky podezřelá.

Lidé, kteří mají boardy, prostě nesnášejí, když jsou jejich systémy zabaveny, a desítky (nebo stovky) jejich uživatelů přihlížejí v bezmocné hrůze. Jejich právo na svobodu projevu je omezeno. Jejich právo na svobodu shromažďování a spolčování s jinými lidmi je ohroženo. A jejich soukromí je narušeno, když se jejich soukromá elektronická pošta stane majetkem policie.

Nikdo se neozval, aby bránil praxi zabavování boardů. Výklad proběhl v pokorném tichu. Ať už právní principy říkají cokoli - (a právní principy nemohou být všeobecně uznány, dokud nejsou přijaty zákony či ustanoveny precedenty) - zabavování boardů se pro vztahy americké počítačové policie s veřejností stalo smrtelným jedem.

A ostatně to ani není nezbytné. Když jste policajt, můžete se o pirátském boardu dozvědět prakticky všechno od svých informátorů. Davy samozvaných strážců veřejného blaha - no dobře, tak *znepokojených občanů* - se obracejí na policii, kdykoli ve svém okolí zpozorují pirátský board (a řeknou o něm policii tolik a s tolika technickými detaily, že si až budete přát, aby už konečně zmlkli). Ochotně předají policii rozsáhlé soubory stažené z BBS a počítačové výpisy o jejím provozu. Je *nemožné* udržet rtuťovitou elektronickou informaci z dosahu policie. Některé lidi kolem počítačů dráždí představa policie „monitorující“ boardy. Zejména agenti Tajné služby USA zkoumají boardy poměrně pravidelně a tyto aktivity mají své diskutabilní aspekty. Ale předpokládat, že elektronická policie bude vzhledem k právě tomuto médiu slepá, hluchá a němá, prostě odporuje zdravému rozumu. Policisté se dívají na televizi, poslouchají rádio, čtou noviny a časopisy; proč by se měli vyhýbat boardům? Policajti mají stejný přístup k elektronickým informacím jako kdokoli jiný. Jak jsme viděli, pěkných pár počítačových policistů má *své vlastní* boardy, včetně boardů nastražených na hackery, jež se celkem velice osvědčily.

A nakonec, jejich přátelé z Kanadské jízdní (a kolegové v Irsku a na Taiwanu), nemají První dodatek ani další americké právní restrikce, ale mají telefonní linky a mohou volat jakýkoli board v Americe, kdykoli se jim zlíbí. Tytéž technologické faktory, které využívají hackeři, telefandové a softwaroví piráti, může využívat i policie. „Technologické faktory“ *nemají* lidské oblíbence. Nejsou černé ani bílé, nekopou za establishment ani za underground, nebojují pro něco ani proti něčemu.

Godwin podrobně kritizoval předpoklad, jež nazval „scénářem o chytrém amatérovi“ - hypotézu, že „hacker“, jehož se chystáte navštívit, je určitě technický génius, a že tedy prohlídka jeho bytu musí být extrémně důkladná. Tedy z pohledu mužů zákona: proč riskovat, že něco vynecháte? Zabavte všechno. Zabavte jeho počítač. Zabavte jeho knihy. Zabavte jeho poznámkové sešity. Zabavte elektronické koncepty jeho milostných dopisů. Zabavte jeho walkmana. Zabavte počítač jeho manželky. Zabavte počítač jeho otce. Zabavte počítač jeho malé sestřičky. Zabavte počítač jeho zaměstnavatele. Zabavte mu CD disky - *mohou* to být disky CD-ROM, rafinovaně zamaskované jako populární hudba. Zabavte mu laserovou tiskárnu - mohl schovat něco důležitého v jejích pěti megabytech paměti. Zabavte mu manuály k programům a dokumentaci k počítači. Zabavte mu vědecko-fantastické a hrací knihy. Zabavte mu konzoli Nintenda a Pac-Mana. Zabavte mu telefonní záznamník a vytrhněte telefon ze zdi. Zabavte všechno, co je jen trochu podezřelé.

Godwin zdůraznil, že většina „hackerů“ nejsou žádní techničtí géniové. Je mezi nimi mnoho podvodníků a zlodějů, kteří se v technice nijak zvlášť nevyznají - znají jen pár jednoduchých technik šizení. A totéž platí pro většinu patnáctiletých kluků, kteří získali z pirátského boardu program testující přístupové kódy. Není třeba zabavit všechno, co mají na dosah. Úspěšná obžaloba nepotřebuje celý počítačový systém a deset tisíc disket.

„A je-li počítač nástrojem trestné činnosti?“ otázal se kdosi.

Godwin klidně připustil, že princip zabavování nástrojů trestné činnosti je v americkém právním systému pevně zakotven. Setkání skončilo. Godwin a Kapor museli odejít. Příští ráno měl Kapor vystoupit v Odboru veřejných služeb státu Massachusetts a promluvit o standardech ISDN pro rozlehlé sítě.

Jakmile byli pryč, Thackerayová se rozzářila. Podnikla riskantní akci a uspěla s ní. Její kolegové neutrhli Kaporovi s Godwinem hlavy. Byla na ně velmi hrdá a také jim to řekla.

„Slyšeli jste, co říkal Godwin o *nástrojích trestné činnosti*?“ jásala. „Pánové, to přece znamená, že *Mitch mě nebude žalovat*!“

Americká počítačová policie je zajímavá společenská skupina. Jako sociologický fenomén jsou mnohem zajímavější, a mnohem důležitější, než nezletilí telefandové a hackeři. Především jsou starší a moudřejší; ne přelétaví amatéři s pochybnou morálkou, ale ostřílení dospělí profesionálové a zodpovědní státní zaměstnanci. A, na rozdíl od hackerů, nemají jen izolovanou *technickou* moc, ale solidní právní a společenskou autoritu.

A, což je zvlášť zajímavé, jsou v cyberspace právě tak doma jako kdokoli jiný. Nemají z toho radost. Policie je od přirozenosti autoritářská a dává přednost chování podle pravidel a precedentů. (I ti policisté, kteří potají v nebezpečné oblasti s chutí říznou zatáčku, důstojně odmítnou jakékoli „kovbojské“ akce.) Ale v cyberspace *neexistují* žádná pravidla a precedenty. Počítačoví policisté jsou pionýři dobývající nový svět, šerifové elektronického pohraničí, ať se jim to líbí nebo ne.

Podle mého názoru by každý mladík (či dívka) milující počítače, fascinovaný komplikovanými detaily počítačové bezpečnosti a přitahovaný vábením specializovaných vědomostí a moci udělal dobře, kdyby zapomněl na hackerské snahy a pokusil se stát federálním agentem. Federální agenti triumfnou hackery v prakticky čemkoli, co hackeři umějí, včetně shromažďování špionážních informací, používání falešných totožností, „odpadování“, odposlouchávání telefonů, tvorby kartoték, spolupráce přes počítačové sítě a pronikání do počítačových systémů - *zločineckých* počítačových systémů. Agenti Tajné služby USA vědí o telefonech, přístupových kódech a kreditních kartách víc, než se většina telefandů naučí za celá léta, a co se týče virů, vloupání, softwarových bomb a trojských koňů, agenti mají přímý přístup k aktuálním a úplným důvěrným informacím, o nichž se v undergroundu vyprávějí jen neurčité legendy.

A jestli ti jde o uznání veřejnosti, jen málo lidí na světě se může měřit s chladně nebezpečnou elegancí dobře trénovaného a dobře vyzbrojeného agenta Tajné služby Spojených států amerických. Přirozeně, ke získání této moci a znalostí je třeba několika osobních obětí. Především je třeba dodržovat protivnou disciplínu nezbytnou pro velké organizace; ale svět počítačového zločinu je stále tak malý a mění se tak rychle, že v nejbližších letech se ani zdaleka neusadí. Další obětí je, že nebudeš moci šidit lidi. To není velká ztráta. Zákaz užívání ilegálních drog, jež je také vyžadován, prospěje tvému zdraví.

Počítačová bezpečnost dává v dnešní době mladým mužům a ženám možnost zajímavé kariéry. Tento obor se v příštích letech bude téměř jistě dramaticky rozvíjet. Je-li ti dnes méně než osmnáct let, budou v době, kdy se staneš profesionálem, z pionýrů, o kterých jsi četl v této knize, velké postavy tvého oboru, obklopené nespočetnými učedníky a následníky. Přirozeně, někteří z nich, jako William P. Wood, který v roce 1865 zakládal Tajnou službu USA, mohou uvíznout v ozubených kolech soudní mašinérie; ale než vstoupíš na scénu počítačového zločinu, patrně se poněkud stabilizuje, aniž by přestala být vzrušující výzvou.

Ale policejní odznak si nemůžeš prostě vzít. Musíš si ho zasloužit. A trénink federálních agentů je tvrdý - je to výzva. Nic pro měkoty a zbabělce.

Každý agent Tajné služby USA musí úspěšně absolvovat náročné kursy ve Federálním policejním tréninkovém centru. (Navíc se jich agenti zúčastňují periodicky v průběhu celé své kariéry.) Abych si uměl představit, jak takový trénink vypadá, rozhodl jsem se navštívit FLETC osobně.

Nadace

NíPrometheus + FBI = Grateful Dead / Planeta Země + počítačová revoluce = WELL / Slavný desperát a board ve střehu / Proces Knight Lightninga / Pád Jestřába / Kyrie ve zpovědnici / 79 499 dolarů / Akademická vyšetřovatelka / Počítače, svoboda a soukromí

Příběh Zátahu na hackery, jak jsme ho sledovali až dosud, byl technologický, subkulturní, kriminální a právní. Příběh ochránců občanských práv, jakkoli také obsahuje tyto aspekty, je výrazně a hluboce *politický*.

V roce 1990 se tichý, již dlouho doutnající boj o povahu a vlastnictví cyberspace stal zjevně a nezvratitelně věcí veřejnou. Lidé z těch nejpodivnějších konců americké společnosti náhle zjistili, že se z nich staly veřejně známé osobnosti. Někteří zjistili, že taková situace je mnohem víc, než kdy chtěli mít. Šlápli na brzdu a pokusili se vrátit do obskurních stínů svých útulných subkultur. Tato taktika se zpravidla ukázala chybnou.

Ale ochránci občanských práv se v roce 1990 chopili příležitosti. Jali se organizovat, propagovat, přesvědčovat, vyjednávat, mlátit do řečnických pultů, pořádat propagační cesty, pózovat pro fotografy, dávat interview a šilhat ve světle reflektorů ve zprvu nesmělém a pokusném, ale stále propracovanějším a sebevědomějším tanci na politickém jevišti.

Je snadné vidět, jaké výhody měli ochránci občanských práv před ostatními skupinami angažovanými v Zátahu na hackery.

Hackeři z digitálního undergroundu jsou esoteričtí elitáři. Je pro ně těžké předestřít široké veřejnosti aspoň trochu přesvědčivou obhajobu svých akcí. Ve skutečnosti hackeři zpravidla „ignorantskou“ veřejností pohrdají a nedůvěřují úsudku „systému“. Hackeři si dělají reklamu, ale pouze mezi sebou, zpravidla formou nerealistických výzev k třídnímu boji, generační vzpouře či naivním technologickým utopiím, plných pravopisných chyb. Hackeři se musí chvástat a naparovat, aby si v undergroundu získali a uchovali reputaci. Ale když mluví příliš veřejně a nahlas, naruší křehkou rovnováhu undergroundové subkultury a jsou obtěžováni kolegy či zatčeni policií. Z hlediska dlouhodobé perspektivy většina hackerů prohrává, jsou chyceni, zrazeni nebo se prostě na všechno vykašlou. Jako politická síla je digitální underground bezmocný.

Telekomunikační společnosti jsou slonovinové věže v trvalém obležení. Mají spoustu peněz, se kterými mohou šířit svůj propracovaný image, ale velkou část své energie a důvěryhodnosti vyplýtvávají ve vzájemných útocích urážlivými a nactiutrhačnými inzertními kampaněmi. Telekomunikační společnosti přišly o mnoho v důsledku zásahů politiků. Podobně jako hackeři nedůvěřují úsudku veřejnosti. A jejich nedůvěra může být oprávněná. Kdyby široká veřejnost technologické společnosti 90. let pochopila, jaké telekomunikace jsou v jejím zájmu, mohlo by to představovat vážnou hrozbu pro specializovanou technickou moc a autoritu, které spojaři požívají již více než sto let. Telekomunikační společnosti mají důležité výhody: loajální zaměstnance, specializované znalosti, vliv ve vládnoucích kruzích, taktické spojence u policie a fantastické finanční zdroje. Ale z politického hlediska jim chybí opravdová podpora veřejnosti; nemají prostě příliš mnoho přátel.

Policajti vědí spoustu věcí, které ostatní lidé nevědí. Ale policajti dobrovolně odhalí pouze ty části svých vědomostí, které podle jejich názoru prospějí cílům jejich organizace a veřejnému pořádku. Policajti mají respekt, pravomoci, moc na ulicích a dokonce i v domech, ale světlo reflektorů jim nesvědčí. Jsou-li k tomu dotlačeni, vystoupí na veřejnost a pohrozí přestupníkům, upokojí prominentní občany či důrazně poučí naivní a svedené. Ale pak se vrátí do svého přirozeného prostředí, do pevnosti policejní stanice, do soudní síně a ke svým směrnicím.

Ale ochránci občanských práv prokázali, že se v politice cítí jako ryba ve vodě. Velmi brzy pochopili postmoderní axiom, že komunikace je moc. Publicita je moc. Stopáž v televizi je moc. Schopnost dostat svůj spor před zraky veřejnosti - a *udržet ho tam* - je moc. Sláva je moc. Obyčejný osobní šarm a výmluvnost mohou být moc, když dokážete vzbudit pozornost a zájem veřejnosti.

Ochránci občanských práv neměli žádný monopol na „technickou moc“ - ačkoli všichni vlastnili počítače, nebyli většinou zvlášť pokročilými počítačovými experty. Měli slušné majetky, ale ani zdaleka ne takové hory peněz a galaxie zdrojů jako telekomunikační společnosti či federální agentury. Nemohli zavírat lidi. Nepoužívali žádné telefandovské a hackerské špinavé triky.

Ale doopravdy uměli komunikovat.

Na rozdíl od ostatních skupin v této knize operovali ochránci občanských práv v zásadě otevřeně, přímo na veřejném kolbišti. Pořádali přednášky pro každého, kdo měl zájem, mluvili s nesčetnými žurnalisty a přitom cizelovali své bonmoty. Udržovali nehasnoucí světlo reflektorů, nenechali zastavit faxy ani fotokopírky, vyměňovali si elektronickou poštu, lízali obálky a utráceli malá jmění za letenky a dálkové hovory. V informační společnosti se tato otevřená, veřejná, neskrývaná aktivita projevila jako velmi efektivní.

V roce 1990 se ochránci občanských práv v cyberspace vynořili odnikud a zorganizovali se nadsvětelnou rychlostí. Tato „skupina“ (ve skutečnosti spíše volný shluk zainteresovaných osob, který si stěží zaslouží i tak obecný název) nemá téměř nic z toho, co tvoří formální organizaci. Ty formální organizace ochránců občanských práv, jež se zajímaly o problémy v cyberspace, zejména Computer Professionals for Social Responsibility („Počítačoví profesionálové za sociální zodpovědnost“) a American Civil Liberties Union („Americký svaz občanských svobod“), nestačily v roce 1990 tempu událostí a sloužily většinou jako základny, pomocníci a ručitelé.

Ochránci občanských práv byli ze všech skupin Zátahu na hackery tou nejúspěšnější. V čase vzniku této knihy vypadá jejich budoucnost růžově a politická iniciativa je pevně v jejich rukou. Až budeme studovat jejich vysoce nepravděpodobné životy a životní styly, měli bychom si uvědomovat, co všechno dokázali.

V červnu 1989 měla společnost Apple Computer, sídlící v Cupertinu v Kalifornii, problém. Někdo ilegálně zkopíroval malý kousek copyrightovaného softwaru Apple, softwaru, který kontroloval čip řídící výstup na obrazovku počítače Macintosh. Zdrojový kód Color QuickDraw byl přísně střeženou částí intelektuálního vlastnictví firmy Apple. Měli k němu mít přístup pouze její důvěryhodní zaměstnanci.

Ale „NuPrometheus League“ („Liga NíPrometheus“) se to rozhodla změnit. Tato osoba (či osoby) pořídila několik ilegálních kopií tohoto zdrojového kódu, možná až dva tucty. Pak dala diskety s nimi do obálek a rozeslala je lidem po celé Americe: lidem pracujícím v počítačovém průmyslu, kteří měli vazby ke společnosti Apple Computer, ale nebyli u ní přímo zaměstnáni.

Akce NíPromethea byla promyšleným, vysoce ideologickým a velmi hackerským trestným činem. Prometheus, jak známo, ukradl oheň bohům a dal tento mocný dar k všeobecnému použití utlačovanému lidstvu. Analogické chování „bohů u koryta“ bylo přisouzeno vrcholovým manažerům Apple Computer, zatímco ní-, tedy mikro-Prometheus si zvolil roli vzpurného poloboha. Pirátsky získaná data byla rozdávána zadarmo.

Nový Prometheus, ať už to byl kdokoli, unikl osudu Promethea řeckých legend, jež byl pomstychtivými bohy na několik set let přikován ke skále, kde mu orel rval a jedl játra. Na druhé straně byl NíPrometheus poněkud bledým odrazem svého vzoru. Malý kousek kódu Color QuickDraw, který vynesl a namnožil, byl pro konkurenci Applu (a ostatně i pro kohokoli jiného) prakticky bezcenný. Spíše než k darování ohně lidstvu by se akce NíPromethea dala přirovnat ke zkopírování části reflektoru jízdního kola. Nešlo o skutečnou průmyslovou špionáž. Nejpřesněji mohla být interpretována jako symbolická, uvážená facka špičce hierarchie Applu.

Vnitřní boje v Apple Computer byly v průmyslových kruzích veřejně známy. Zakladatelé Applu, Jobs a Wozniak, už dávno odešli. Nevázané jádro jejich dlouholetých zaměstnanců byli Kaliforňané šedesátých let se sklonem k exhibicím a mnozí z nich nebyli nijak spokojeni s novým, seriózním režimem multimiliónových obchodů, který ve společnosti zavládl. Mnozí z programátorů a vývojářů, kteří počátkem 80. let vymysleli počítač Macintosh, také dali výpověď. Oni, ne současní vládci Applu, vymysleli Color QuickDraw. Akce NíPromethea byla dobře promyšlenou ranou vztahům mezi zaměstnanci.

Společnost Apple zavolala FBI. FBI vyšetřuje významné případy průmyslové špionáže, krádeží intelektuálního vlastnictví a obchodních tajemství. Nejspíš to byli ti praví lidé, které bylo třeba zavolat, a pověst tvrdí, že zodpovědné osoby byly ve skutečnosti FBI odhaleny a management Applu je tiše zamáčkl. NíPrometheus nebyl nikdy veřejně obviněn, stíhán ani zatčen. Ale nedošlo už k žádným dalším případům ilegálního zveřejňování vnitřního softwaru počítače Macintosh. Nakonec zájem o nepříjemný skandál kolem NíPromethea opadl.

Ale ne dříve, než mnoho nezúčastněných, překvapených lidí přijalo překvapivou návštěvu z FBI.

Jedním z těchto lidí byl John Perry Barlow. Barlow je velmi neobyčejný muž, jehož je těžké popsat konvenčními pojmy. Patrně nejznámější je jako textař rockové skupiny Grateful Dead; napsal texty písní „Hell in a Bucket“, „Picasso Moon“, „Mexicali Blues“, „I Need a Miracle“ a mnoha dalších. Pro Grateful Dead píše od roku 1970.

Než se začneme zabývat dráždivou otázkou, proč FBI vyslýchá rockového textaře v případě počítačového zločinu, bude vhodné říci několik slov o Grateful Dead. Skupina Grateful Dead je možná tím nejúspěšnějším a nejtrvanlivějším z četných kulturních výbojů vycházejících ze sanfranciské čtvrti Haight-Ashbury za slavných dnů politických hnutí a kyselinové transcedence. Grateful Dead jsou centrem, pravým okem uragánu nášivek, psychedélických karavanů, batikovaných triček, sepraných džín, divokého tance a otevřeného a neskrývaného užívání drog. Symboly, a realita, kalifornských „dětí květin“ obklopují Grateful Dead jako macramé.

Grateful Dead a tisíce „Deadheads“, jejich fanoušků, jsou radikální bohémové. To je všeobecně známo. Co to přesně znamená v devadesátých letech dvacátého století je poněkud problematičtější.

Grateful Dead patří mezi nejpopulárnější a nejbohatší hvězdy zábavního průmyslu na světě: podle časopisu *Forbes* jsou na 20. místě, mezi M.C. Hammerem a Seanem Connerym. V roce 1990 vydělala tato skupina v džínách, pěstující si image vyvrhelů společnosti, sedmnáct miliónů dolarů. A podobné sumy vydělávají už delší čas.

A jakkoli Grateful Dead nejsou investiční bankéři ani profesionální daňoví experti - nakonec, jsou to hippie muzikanti - tyto peníze nebyly vyházeny na nesmyslné bohémské výstřelky. Grateful Dead již po léta tiše sponzorují nejrůznější chvályhodné aktivity ve své rozlehlé a živé kulturní komunitě.

Grateful Dead nejsou konvenčními hráči v amerických mocenských kruzích. Jsou ale silou, se kterou je nutno počítat. Mají spoustu peněz a spoustu přátel na mnoha místech, očekávaných i neočekávaných.

Grateful Dead mohou být známi svou rétorikou o „návratu k přírodě“, ale to z nich stěží dělá nepřátele technologie. Naopak, jako většina rockových hudebníků, strávili i Grateful Dead celý svůj život ve společnosti složitého elektronického vybavení. Mají na to, aby si pořídili každý sofistikovaný nástroj či hračku, která je zaujme. A zajímá je toho dost.

Komunita „Deadheads“ se může pochlubit nespočetně odborníky na záznam zvuku, osvětlení, rockové video a elektroniku ve všech podobách. A spojení je obousměrné. Steve Wozniak, spoluzakladatel Applu, kdysi pořádal rockové festivaly. Silicon Valley duní rockem.

Dnes jsou devadesátá léta, ne šedesátá. Dnes, pro překvapující množství lidí po celé Americe, údajná dělicí čára mezi bohémem a technikem prostě neexistuje. Lidé tohoto druhu mohou nosit copánky a mít psa s šátkem kolem krku, ale nejspíš mají i nový model Macintoshe s hudebním MIDI softwarem a halucinogenními simulacemi fraktálů. Dnes i samotný Timothy Leary, prorok LSD, používá na svých přednáškách programy demonstrující počítačovou grafiku.

John Perry Barlow není členem Grateful Dead. Je ale významným „Deadheadem“.

Barlow o sobě mluví jako o „techno-cvokovi“. Obecný termín, například „sociální aktivista“, by také nebyl nepřesný. Ale lépe je ho možno popsat jako *básníka* - pokud si člověk pamatuje archaickou definici Percy Shelleyho, podle níž jsou básníci „neuznanými zákonodárci světa“.

Barlow se jednou pokusil získat status uznaného zákonodárce. V roce 1987 těsně prohrál kandidaturu za republikány na uvolněné křeslo v senátu státu Wyoming. Narodil se ve Wyomingu, ve třetí generaci vážené rančerské rodiny. Je mu něco málo přes čtyřicet, je ženatý a má tři dcery.

Barlow se nenechává příliš omezovat tím, co si jiní lidé myslí o konzistentnosti. Koncem 80. let prodal tento republikánský rockový textař a chovatel dobytka svůj ranč a začal se věnovat počítačové komunikaci.

Barlow změnil svůj životní styl úspěšně a s lehkým srdcem. Počítače ho opravdu nadchly. Se zapísknutím svého modemu se přesunul z malého Pinedale ve Wyomingu do elektronického světa velkého a živého davu chytrých, sympatických a vynalézavých technologických nadšenců z celého světa. Barlowovi se zalíbila společnost kolem počítačů: její rychlý vývoj, svobodomyslná rétorika, otevřené možnosti. Začal psát články o počítačích. Měly úspěch, protože Barlow se učil rychle a byl inteligentní a výmluvný. Často jezdil do San Franciska, kde se setkával se svými přáteli mezi „Deadheads“. Získal tam také rozsáhlé kontakty v kalifornské počítačové komunitě, včetně přátelství s několika nekonformními zaměstnanci Applu.

V květnu 1990 ho ve Wyomingu navštívil místní agent FBI a Barlow se seznámil s případem NíPrometheus.

Znepokojilo ho, že je vyšetřován kvůli svým zájmům v oblasti, která byla kdysi dokonale prosta aktivit federální policie. Musel se velmi snažit, aby vysvětlil samu podstatu počítačového zločinu rozpačitému agentovi FBI, který se specializoval na krádeže dobytka. Společensky rozprávějícího Barlowa, demonstrujícího zázračné možnosti svého modemu zaraženému agentovi, alarmovalo, když zjistil, že všichni „hackeři“ jsou FBI považováni za nepřátelské elementy v počítačové komunitě. FBI, pronásledující hackera jménem NíPrometheus, pátrala po členech podezřelé skupiny jménem Hackerská konference.

Hackerská konference, která se poprvé konala v roce 1984, bylo každoroční setkání kalifornských počítačových průkopníků a entuziastů. Hackeři z Hackerské konference měli jen málo, pokud vůbec něco, společného s hackery z digitálního undergroundu. Naopak, hackeři z této konference byli většinou vážení kalifornští ředitelé počítačových firem, konzultanti, novináři a podnikatelé. (Přesně ten druh „hacke-

rů“, od kterých se dala očekávat bouřlivá reakce na jakoukoli kriminální degradaci pojmu „hacker“.)

Barlow, ačkoli nebyl zatčen ani z ničeho obviněn a jeho počítač naprosto nebyl zabaven, byl touto anomálií velmi znepokojen. Informoval o ní WELL.

Stejně jako Hackerská konference, byl i WELL („Studna“), projektem Point Foundation. Point Foundation, inspirovaná Stewartem Brandem, bohatým kalifornským radikálem 60. let, se později stala významnou základnou snah ochránců občanských práv.

Kulturní aktivity Point Foundation, stejně jako aktivity Grateful Dead (které se též soustřeďovaly do okolí San Franciska), byly mnohostranné a mnohočetné. *Whole Earth Catalog* („Katalog planety Země“), vydávaný Point Foundation, se nikdy nevyznačoval svazující ideologickou konzistentností. Na vrcholu slávy byla tato publikace koncem 60. a počátkem 70. let, kdy nabízela stovky praktických (i méně praktických) typů na život v komunách, ochranu životního prostředí a návrat k přírodě. Tehdy se Katalogu planety Země a jeho pokračování prodalo dva a půl milionu výtisků a byl vyhlášen Knihou roku.

S pomalým rozpadem amerického radikálního disentu se Katalog planety Země posunul dále od centra kulturní sféry; ale ve formě časopisu *CoEvolution Quarterly* („Koevoluční čtvrtletník“) pokračovala Point Foundation v nabídce kaleidoskopického mišmaše „nástrojů a idejí pro každého“.

Čtvrtletník, který začal vycházet v roce 1974, nikdy nebyl široce populárním časopisem. Přes periodické záchvaty chiliastické horečky se *CoEvolution Quarterly* nepodařilo revolucionalizovat západní civilizaci a nahradit váhu historie novými elegantními kalifornskými paradigmaty. Místo toho se tento propagační nástroj Point Foundation pohyboval na úzké hranici mezi zářivou, působivou suverenitou a úlety New Age. *CoEvolution Quarterly* neobsahoval žádné inzeráty, byl drahý a tištěný na laciném papíře se skromnými černobílými obrázky. Byl špatně distribuován a prodáván zpravidla na předplatné lidem, kteří se o něm dozvěděli od svých známých.

Nevypadalo to, že by se kdy dokázal dostat přes třicet tisíc předplatitelů. Ale na druhé straně nebyl nikdy ohrožen jejich úbytkem. Rok, dva, deset, dvacet, stále se udržovala jakási neurčitá společenská menšina věrná tomuto časopisu. Nezdálo se, že by pravidelní čtenáři měli nějaké společné politické postoje či ideály. Někdy bylo těžké pochopit, co je vlastně drží pospolu (pokud se ostré polemiky na stránkách věnovaných dopisům čtenářů dají vůbec označit za „pospolitost“).

Jestliže časopis nevzkvétal, byl přinejmenším vytrvalý - nepotápěl se. V roce 1984, kdy vznikl počítač Macintosh, narazil *CoEvolution Quarterly* na zlatou žílu. Point Foundation objevila počítačovou revoluci. Byl vydán *Whole Earth Software Catalog* („Katalog softwaru planety Země“) a posléze *Whole Earth Review*, tedy současné vtělení časopisu, nyní vedeného guruem virtuální reality Howardem Rheingoldem.

A v roce 1985 se zrodil WELL čili „Whole Earth ‚Lectronic Link“ („Elektronické spojení planety Země“). WELL byl boardem Point Foundation.

Mezi boardy byl WELL od počátku anomálií a zůstal jí až dodnes. Byl určen pro obyvatele San Franciska a jeho okolí. Byl obrovský - měl množství telefonních linek a enormně rozsáhlé návody k použití. Jeho komplexní unixovský software naprosto nemohl být nazván uživatelsky přívětivým. Běžel na sálovém počítači umístěném v kancelářích neziskové kulturní nadace, adaptovaných v obytném domě v Sausalitu, na předměstí San Franciska. A byl nacpán fanoušky Grateful Dead.

I když se na WELLu bavili hippie přívrženci sanfranciské alternativní kultury, nebyl v žádném případě boardem digitálního undergroundu. Bylo na něm jen velmi málo nezletilých; většina uživatelů WELLu, nazývajících se „Wellbeings“ (tj. „zdar“, ale také „bytost WELLu“), byli lidé středního věku, narození v padesátých a šedesátých letech. Často pracovali s informačními technologiemi: hardwarem, softwarem, telekomunikacemi, masmédii, zábavou. Zvlášť mnoho bylo na WELLu knihovníků, vysokoškolských profesorů a novinářů, přitahovaných „nástroji a idejemi pro každého“, štědře nabízenými Point Foundation.

Na WELLu nebyly žádné anarchistické soubory a stěží zmínka o přístupových kódech a krádežích kreditních karet. Nikdo nepoužíval přezdívky. „Flames“, tedy nadávky v elektronické poště, byly celkem udržovány na úrovni společensky přijatelného bručení. Debaty byly někdy ostré, ale žádný „Wellbeing“ nikdy netvrdil, že mu oponent odpojil telefon, prohledal dům či zveřejnil čísla jeho kreditních karet.

V průběhu 80. let WELL pomalu rostl. Za přístup a ukládání dat žádal jen mírné poplatky a léta byl prodělečný - ne ovšem natolik, aby to poškodilo Point Foundation, což byla ostatně stejně nezisková organizace. V roce 1990 měl WELL kolem pěti tisíc uživatelů, kteří se procházeli cyberspace a vybírali si z obrovitého švédského stolu „konferencí“. Každá z nich se skládala z masy „témat“ a každé téma obsahovalo desítky, někdy i stovky „zpráv“ tvořících neuspořádaný, mnohostranný rozhovor, který mohl probíhat měsíce nebo i léta.

```
                    KONFERENCE WELLU
                 Diskmag WELLu - výběr
              The best of WELL - klasika
        Seznam nových témat ve všech konferencích

                  Obchod - Vzdělávání

  Apple Library Users Group          Agriculture („Zemědělství“)
  Brainstorming                      Classifieds („Inzeráty“)
  Computer Journalism                Consultants
  Consumers („Spotřebitelé“)         Design
  Desktop Publishing                 Disability („Invalidita“)
  Education („Vzdělávání“)           Energy
  Entrepreneurs („Podnikatelé“)
  Homeowners („Rodinné domky“)       Indexing
  Investments („Investice“)          Kids91 („Děti“)
  Legal („Právní“)
  One Person Business („Živnostníci“)
  Periodical/newsletter („Periodika“)
  Telecomm Law („Telefonní zákony“)  The Future („Budoucnost“)
  Translators („Překladatelé“)       Travel („Cestování“)
  Work („Práce“)

  Electronic Frontier Foundation („Nadace elektronického
  pohraničí“)
  Computers, Freedom & Privacy („Počítače, svoboda a soukromí“)
```

Computer Professionals for Social Responsibility („Počítačoví profesionálové za společenskou zodpovědnost“)

Společenské - Politické - Humanitní

Aging („Stáří“)
AIDS
Amnesty International
Archives
Berkeley
Buddhist
Christian („Křesťanství“)
Couples („Páry“)
Current Events („Současný svět“)
Dreams („Sny“)
Drugs („Drogy“)
East Coast („Východní pobřeží“)
Emotional Health**** („Duševní zdraví“)
Erotica
Environment („Životní prostředí“)
Firearms („Střelné zbraně“)
First Amendment („První dodatek americké ústavy“)
Fringes of Reason („Meze rozumu“)
Gay
Gay („Private“)# („Gay - soukromá“)
Geography („Zeměpis“)
German („Německá“)
Gulf War („Válka v Perském zálivu“)
Hawaii („Havaj“)
Health („Zdraví“)
History („Historie“)
Holistic („Alternativní medicína“)
Interview
Italian („Italská“)
Jewish („Židovská“)
Liberty („Svoboda“)
Mind („Mysl“)
Miscellaneous („Různé“)
Men on the WELL** („Muži na WELLu“)
Network Integration („Integrace sítí“)
Nonprofits („Neziskové“)
North Bay („Severní zátoka“)
Northwest („Severozápad“)
Pacific Rim („Dálný východ“)
Parenting („Rodičovství“)
Peace („Mír“)
Peninsula („Ibérie“)
Poetry („Poezie“)
Philosophy
Politics
Psychology
Psychotherapy („Psychoterapie“)
Recovery## („Odvykání“)
San Francisco
Scams („Podfuky“)
Sexuality
Singles („Svobodní“)
Southern („Jižní“)
Spanish („Španělská“)
Spirituality
Tibet
Transportation („Transport“)
True Confessions („Vyznání“)
Unclear („Nejasné“)
WELL Writer’s Workshop*** („Spisovatelská dílna WELLu“)
Whole Earth („Planeta Země“)
Women on the WELL* („Ženy na WELLu“)
Words („Slova“)
Writers („Spisovatelé“)

**** soukromá konference - nové uživatele přihlašuje wooly
*** soukromá konference - nové uživatele přihlašuje sonia
** soukromá konference - nové uživatele přihlašuje flash
* soukromá konference - nové uživatele přihlašuje reva
# soukromá konference - nové uživatele přihlašuje hudu
soukromá konference - nové uživatele přihlašuje dhawk

Umění - Rekreace - Zábava

ArtCom Electronic Net
Audio-Videophilia („Audio a video šílenci“)
Bicycles („Jízdní kola“)
Bay Area Tonight** („San Francisco a okolí dnes v noci“)
Boating („Čluny“)
Books („Knihy“)
CD’s
Comics
Cooking („Vaření“)
Flying („Létání“)
Fun („Legrace“)
Games („Hry“)
Gardening („Zahrádka“)
Kids („Děti“)
Nightowls* („Noční ptáci“)
Jokes („Vtipy“)
MIDI
Movies („Kina“)
Motorcycling („Motorky“)
Motoring
Music („Hudba“)
On Stage („Na pódiu“)
Pets („Domácí mazlíčci“)
Radio
Restaurant
Science Fiction

```
Sports                              Star Trek
Television                          Theater („Divadlo“)
Weird („Groteskní“)
Zines/Factsheet Five („Fanziny“)

  *  Otevřeno od půlnoci do šesti ráno
  ** Denně aktualizováno

                      Grateful Dead

Grateful Dead                       Deadplan* („Plány“)
Deadlit („Knihy“)                   Feedback („Zpětná vazba“)
GD Hour                             Tapes („Pásky“)
Tickets („Lístky“)                  Tours („Turné“)

  * soukromá konference - nové uživatele přihlašuje tnf

                        Počítače

AI/Forth/Realtime                   Amiga
Apple                               Computer Books („Knihy“)
Art & Graphics („Umění a grafika“)  Hacking
HyperCard                           IBM PC
LANs („Místní sítě“)                Laptop
Macintosh                           Mactech
Microtimes                          Muchomedia
NeXt                                OS/2
Printers („Tiskárny“)
Programmer's Net („Programátorská síť“)
Siggraph                            Software Design
Software/Programming
Software Support („Softwarová podpora“)
Unix                                Windows
Word Processing („Zpracování textů“)

                  Technika - Komunikace

Bioinfo                             Info
Media                               NAPLPS
Netweaver („Snovač sítí“)           Networld („Svět sítí“)
Packet Radio („Radiové sítě“)       Photography („Fotografie“)
Radio                               Science („Věda“)
Technical Writers („Techničti spisovatelé“)
Telecommunications („Telekomunikace“)
Usenet („Elektronická pošta v Internetu“)
Video
Virtual Reality („Virtuální realita“)

                      Vlastní WELL

Deeper („Do hloubky“)               Entry („Vstupní bod“)
General („Obecně“)                  Help
Hosts („Hostitelé“)                 Policy („Pravidla“)
System News                         Test
```

Už sám seznam je ohromující; neškolené oko vnímá jen závratný vír světa, v němž si havajští holističtí fotografové na vysokohorské výpravě vyměňují vyznání s bisexuálními Tibeťany, zpracovávajícími texty na počítačích.

Ale tento zmatek je spíše zdánlivý než skutečný. Každá z konferencí byla malým, izolovaným světem v cyberspace, skládajícím se z desítek, možná stovek podtémat. Každá konference byla pravidelně navštěvována relativně malou komunitou s velmi příbuznými názory, možná několika tucty lidí. Žádný smrtelník by nedokázal obsáhnout celý WELL (zvlášť když doba přístupu k sálovému počítači WELLu byla účtována). Většina dlouhodobých uživatelů se spokojila s několika oblíbenými tématy a občasným výpadem do exotických končin. Ale zvláště důležité zprávy a diskuse o aktuálních tématech si mohly získat pozornost celé komunity WELLu.

Jako každá komunita, měl i WELL své celebrity, a John Perry Barlow, básník Grateful Dead se stříbrným jazykem a stříbrným modemem, byl jednou z nich. A právě na WELLu zveřejnil svůj příběh ze života o střetnutí s FBI vyšetřující počítačový zločin.

Příběh, jak se dalo čekat, vyvolal velký rozruch. WELL byl už připraven na spor o hackerech. V prosinci 1989 zorganizoval časopis *Harper's* na WELLu debatu o etice pronikání do počítačů. Zúčastnilo se jí více než čtyřicet počítačových guruů a Barlow byl její hvězdou. Dalšími hvězdami byli Acid Phreak („Narkoman“) a Phiber Optik („Optický Kabel“), dva mladí newyorští hackeři a telefandové, jejichž schopnostem pronikání do telefonních ústředen se vyrovnala jen jejich nenasytná touha po slávě. Příchod těchto vyzývavých desperátů na půdu WELLu vyvolal asi takový rozruch jako příchod Černých Pantherů na večírek salónních radikálů.

Zvlášť Phiber Optik se v roce 1990 dostal do světel reflektorů. Oddaný člen kroužku kolem *2600* a pilíř newyorské hackerské skupiny „Masters of Deception“ („Mistři klamu“) byl krásným exemplářem přesvědčeného hackera-disidenta. Osmnáctiletý Phiber Optik, který před-

časně ukončil studium na střední škole a pracoval na částečný úvazek jako opravář počítačů, byl digitální frajer, mladý, chytrý a bezohledný, měl rád vyzývavé oblečení a vyzývavé řeči a demonstrativně, kavalírsky pohrdal všemi pravidly kromě svých vlastních. Než skončil rok 1991, objevil se Phiber Optik v časopisech *Harper's* a *Esquire*, v deníku *The New York Times*, na nesčetných veřejných debatách a shromážděních a dokonce i v televizní show Geralda Rivery.

Phiber Optik se rychle stal hvězdou WELLu; Barlow a další celebrity s ním jednali s s opatrným respektem. Kupodivu, navzdory svému kousavému tónu a posedlosti svým koníčkem vzbuzoval Phiber Optik ve většině lidí, kteří se s ním seznámili, téměř mateřské ochranné instinkty. Byl výborným materiálem pro žurnalisty, vždy připravený k vytahování a, což bylo ještě lepší, skutečným *demonstracím* nějakého neuvěřitelného digitálního triku. Byl rozeným miláčkem médií.

Zdálo se, že i policisté uznávali, že na tomto potížistovi je cosi nezemského a nezločineckého. Byl tak horkokrevný, tak tvrdohlavý, tak mladý a tak zjevně odsouzený k brzkému konci, že i lidé, kteří zásadně nesouhlasili s jeho akcemi, se strachovali o jeho osud a chovali se k němu jako k ohroženému tulenímu mláděti.

24. ledna 1990 (devět dní po kolapsu na výročí Martina Luthera Kinga) uskutečnila Tajná služba USA razii u Phiber Optika, Acid Phreaka a třetího newyorského delikventa jménem Scorpion. Jejich počítače byly zabaveny, a s nimi jako obvykle hromady papírů, poznámkových bloků, CD desek, telefonních záznamníků, walkmanů atd. Acid Phreak i Phiber Optik byli obviněni, že způsobili kolaps z 15. ledna.

Mlýny spravedlnosti melou pomalu. Případ nakonec připadl policii státu New York. Phiber Optik přišel při razii o svůj počítač, ale více než rok proti němu nebyla vznesena obžaloba.

Jeho nesnáze byly na WELLu široce komentovány a policejní taktika vzbudila velký odpor. Jedna věc je slyšet o tom, že u nějakého hackera byla provedena domovní prohlídka, a druhá vidět, jak policie útočí na někoho, koho osobně znáte a kdo vám podrobně vysvětlil své motivy. Při debatě na WELLu organizované časopisem *Harper's* se jeho uživatelé ujistili, že Phiber Optik ve skutečnosti nechce nic rozbíjet. Za svých vlastních mladých let mnoho z nich ochutnalo slzný plyn ve tvrdých pouličních potyčkách s policií. Měli porozumění pro akty občanské neposlušnosti.

„Wellbeings" byli také zneklidněni drakonickou důkladností typické razie proti hackerům. Nebylo pro ně těžké představit si sebe samé jako oběti takové akce.

Už v lednu 1990 se nálada na WELLu zhoršovala a lidé si začali stěžovat, že nespravedlivý establishment se chová k „hackerům" jako slon v porcelánu. Ve shrnutí debaty v časopise *Harper's* se objevila pochybnost, je-li pronikání do počítačů vůbec zločinem. Jak to později vyjádřil Barlow: „Položil jsem si otázku, zdali bychom nepovažovali i speleology za nebezpečné desperáty, kdyby všechny jeskyně patřily AT&T".

V únoru 1991, více než rok po razii v jeho domě, byl Phiber Optik konečně zatčen a obviněn ze „zvláště nebezpečného ovlivňování činnosti počítače a jeho zneužívání", což jsou trestné činy podle kodexu státu New York. Byl také obviněn z přestupku krádeže služeb, týkajícího se složitého triku s číslem s předvolbou 900, umožňujícím bezplatné volání. Phiber Optik se přiznal k přestupku a byl odsouzen na třicet pět hodin veřejných prací.

Tato drobná nesnáz s nevyzpytatelným světem zákonů Phiber Optika nijak zvlášť netrápila. Když při lednové razii přišel o svůj počítač, jednoduše si koupil přenosný, aby policistům znemožnil monitorování telefonu v bytě, kde žil se svou matkou, a nerušeně pokračoval ve svých výbojích, někdy v živém rádiovém vysílání či před televizními kamerami.

Jakkoli byla newyorská razie neúčinná, co se týkalo odrazení Phiber Optika, její vliv na uživatele WELLu byl hluboce negativní. A v průběhu roku 1990 chřestění zbraní pokračovalo: razie u Knight Lightninga, u Steva Jacksona, celostátní Operace Sundevil. Výroky policie jasně ukazovaly, že skutečně probíhá soustředěný zátah na hackery.

Hackeři z Hackerské konference, „Wellbeings" a jim podobní v zásadě neměli námitky proti proti občasnému nepochopení pojmu „hacker" ze strany veřejnosti; koneckonců, membrána oddělující mainstreamovou společnost od počítačové komunity jim umožňovala cítit se jinými, chytřejšími, lepšími. Nikdy předtím se ale neocitli pod palbou soustředěné defamační kampaně.

Barlowova ústřední role v protiofenzívě byla jednou z hlavních anomálií Zátahu na hackery v roce 1990. Novináři sledující tuto kontroverzi často o Barlowa zakopli, ale zpravidla se zase oprášili a běželi dál, jako by se nic nestalo. Vypadalo to, jako kdyby *odmítali uvěřit*, že radikál ze 60. let od Grateful Dead se postavil proti celostátní policejní operaci *a zřejmě vyhrává*!

Barlow neměl žádnou zjevnou základnu pro politický boj tohoto druhu. Neměl žádná formální právní ani technická privilegia. Ale Barlow byl síťovým organizátorem vpravdě hvězdných kvalit. Měl básnický dar přiléhavého, barvitého vyjadřování. Měl i novinářskou chytrost, nekonvenční, ironický vtip a vrchovatou míru starého dobrého osobního kouzla.

Autorita, kterou Barlow měl, je poměrně běžná v literárních, hudebních a vůbec uměleckých kruzích. Nadaný kritik může získat velký vliv tím, že definuje „ducha času", vymyslí nová motta a termíny debaty, jež se v dané době ujmou. (A Barlow skutečně *byl* mimo jiné i uměleckým kritikem; jeho oblíbeným umělcem byl malíř amerického Západu Frederic Remington.)

Barlow byl prvním novinářem, který začal používat působivý vědecko-fantastický pojem Williama Gibsona „cyberspace" jako synonymum pro současné prolnutí počítačových a telekomunikačních sítí. Barlow zdůrazňoval, že cyberspace by měl být chápán jako kvalitativně nový svět, nově osidlované „pohraničí". Podle Barlowa nemůže být svět elektronických komunikací, nyní zviditelněný na obrazovkách počítačů, nadále chápán jen jako klubko složitě propojených drátů. Stalo se z něj *místo*, cyberspace, vyžadující nové metafory, nová pravidla a nový přístup. Tento termín, ve smyslu použitém Barlowem, vzbudil široký ohlas - koncept cyberspace převzaly časopisy *Time* a *Scientific American*, počítačová policie, hackeři a dokonce i odborníci na ústavní právo. Zdá se, že slovo cyberspace se stane trvalou součástí jazyka.

Barlow je na první pohled výraznou osobností: vysoký, vousatý Západaň s ostrými rysy a hlubokým hlasem v perfektním kovbojském oblečení, v džínách, vestě, jezdeckých botách, s šátkem kolem krku a neodmyslitelným odznáčkem Grateful Dead v klopě.

Ale opravdu kompletní je Barlow až se svým modemem. Formální hierarchie nejsou jeho živlem; zřídkakdy si dá ujít příležitost navézt se do „trubců z velkých organizací" a jejich konvenčního, nepružného způsobu myšlení. Barlow dává přednost neformálnímu přesvědčování; velcí bílí náčelníci a jejich suity na něj nedělají dojem. Ale co se týče využívání digitálních tamtamů, je Barlow organizátorem světové třídy.

Neexistovala armáda Barlowů. Byl jen jeden Barlow, a to byla velmi neobvyklá osobnost. Ale zdálo se, že situace vyžaduje *právě jediného* Barlowa. Ve skutečnosti nejspíš mnoho lidí po roce 1990 usoudilo, že jediný Barlow je mnohem víc, než kdy toužili mít.

Barlowův jízlivý esej o jeho setkání s FBI vzbudil na WELLu velký ohlas. Mnoho jiných volnomyšlenkářů pohybujících se kolem společnosti Apple se octlo v podezření a nelíbilo se jim to ani o chlup více než jemu.

Jedním z nich byl Mitchell Kapor, spoluautor tabulkového procesoru „Lotus 1-2-3" a zakladatel Lotus Development Corporation. Kapor se smířil s nedůstojnou epizodou braní otisků prstů v kanceláři FBI v Bostonu, ale Barlowova zpráva mu ozřejmila celostátní rozsah operace FBI. Kapor začal věnovat této kontroverzi intenzívní pozornost. Když v roce 1990 Tajná služba USA rozvinula celostátní operaci proti hackerům, sledoval Kapor každý tah s hlubokým skepticismem a rostoucím znepokojením.

Kapor se už s Barlowem osobně setkal - poskytl mu rozhovor pro jeden kalifornský počítačový časopis. A Barlow mu velice zaimponoval,

stejně jako většině lidí, kteří ho poznali. Kapor se rozhodl, že zaskočí za Barlowem a prodiskutuje s ním situaci od srdce k srdci.

Kapor byl pravidelným hostem na WELLu. Byl příznivcem *Whole Earth katalogu* a hrdým majitelem všech jeho čísel. A měl nejen modem, ale také soukromé letadlo. Při dozoru na rozptýlené investice do moderních technologií Kapor Enterprises Inc., své soukromé holdingové společnosti v ceně mnoha miliónů dolarů, Kapor běžně překračoval hranice států a věnoval tomu asi takovou pozornost, s jakou může člověk odfaxovat dopis.

Porada Kapora s Barlowem, jež se uskutečnila v červnu 1990 ve wyomingském Pinedale, byla počátkem Nadace elektronického pohraničí. Barlow ruče napsal manifest „Crime and Puzzlement" („Zločin a tajemství"), oznamující jeho - a Kaporův - úmysl zformovat politickou organizaci s cílem „získávat a vynakládat prostředky na vzdělávání, lobbování a soudní spory v oblastech souvisejících s digitálním projevem a rozšířením ústavy do cyberspace".

Dále manifest tvrdil, že Nadace bude „financovat, uskutečňovat a podporovat snahy, které by právní cestou demonstrovaly, že Tajná služba USA uskutečňovala preventivní cenzuru publikací, omezovala svobodu slova, neoprávněně zabavovala vybavení a data, užívala nepřiměřenou sílu a všeobecně postupovala arogantně, despoticky a protiústavně". „Crime and Puzzlement" byl široce distribuován počítačovými kanály a také vytištěn v *Whole Earth Review*. Náhlá publikace koherentního, politického protiúderu z řad hackerů jejich komunitu elektrizovala. Steve Wozniak (možná trochu dotčený skandálem kolem NíPromethea), obratem nabídl stejnou částku, jakou Nadaci věnuje Kapor.

John Gilmore, jeden ze zakladatelů společnosti Sun Microsystems, nabídl rozsáhlou finanční i osobní podporu. Přesvědčený radikální individualista Gilmore prokázal, že je schopným obhájcem elektronického soukromí, zejména svobody před vládním a podnikovým sledováním aktivit soukromých osob s pomocí počítačů.

Na druhém setkání v San Francisku se přidali další spojenci: Stewart Brand z Point Foundation, průkopníci virtuální reality Jaron Lanier a Chuck Blanchard, podnikatel s počítačovými sítěmi a specialista na zakládání nových podniků Nat Goldhaber. Na pracovní večeři se aktivisté shodli na oficiálním názvu: Electronic Frontier Foundation, Incorporated. Kapor se stal jejím prezidentem. Na WELLu, patřícím Point Foundation, byla otevřena nová konference EFF a WELL byl prohlášen za „domov Nadace elektronického pohraničí".

Zájem novinářů byl okamžitý a intenzívní. Stejně jako jejich duchovní předchůdci z devatenáctého století, Alexander Graham Bell a Thomas Watson, byli i počítačoví podnikatelé 70. a 80. let století dvacátého - lidé jako Wozniak, Jobs, Kapor, Gates a H. Ross Perot - kteří se vlastním přičiněním dostali na vrchol nového, úžasného průmyslového odvětví, velmi kvalitním novinářským materiálem.

Ale zatímco uživatelé WELLu se radovali, tisk obecně byl samozvanými „pionýry cyberspace" zjevně zmaten. Tvrzení EFF, že válka proti „hackerům" vedla k vážným ústavním problémům s občanskými právy, se zdálo poněkud přepjaté, zvláště když žádný z organizátorů EFF nebyl právník ani uznávaný politik. Zejména pro listy specializované na obchodní zpravodajství bylo snazší soustředit se na nejsnáze viditelnou část příběhu - že počítačový podnikatel Mitchell Kapor založil „fond na obhajobu hackerů". Byla EFF skutečně důležitým politickým faktorem, nebo jen klakou bohatých excentriků, míchajících se do věcí, jež by měly být spíše přenechány příslušným státním orgánům? Verdikt dosud nebyl vynesen.

Ale scéna již byla připravena pro otevřenou konfrontaci. První a nejkritičtější bitvou byl precedenční soudní proces Knight Lightninga.

V této knize jsem se držel pojmenovávání hackerů pouze jejich přezdívkami. Uvedení jejich pravých jmen má málo výhod; mnozí z nich jsou nezletilí, mnozí nebyli nikdy usvědčeni ze žádného zločinu a mnozí mají nevinné rodiče, kteří už si užili dost.

Ale proces Knight Lightninga, probíhající 24. až 27. července 1990, udělal z tohoto „hackera" celostátně známou osobnost. Ani jemu, ani jeho rodině nemůže způsobit žádnou zvláštní škodu, když zopakuji dobře známý fakt, že se jmenuje Craig Neidorf (vysl. Nýdorf).

Neidorfův porotní soud se odehrával před Státním soudem Východní zóny Severního distriktu státu Illinois, jemuž předsedal ctihodný Nicholas J. Bua. Poškozeným byly Spojené státy americké, obžalovaným pan Neidorf. Jeho obhájcem byl Sheldon T. Zenner z chicagské firmy Katten, Muchin a Zavis.

Obžalobu vedli prominentní členové Chicagské operační skupiny proti počítačové zpronevěře a zneužití počítače: William J. Cook, Colleen D. Coughlinová a David A. Glockner, všichni pomocní federální státní zástupci. Agentem Tajné služby USA pověřeným případem byl Timothy M. Foley.

Připomeňme si, že Neidorf byl jedním ze dvou redaktorů undergroundového hackerského „časopisu" jménem *Phrack*. *Phrack* byl zcela elektronickou publikací, distribuovanou prostřednictvím bulletin boardů a elektronickými sítěmi. Bylo to amatérské periodikum šířené zdarma. Neidorf za svoji práci na *Phracku* nikdy nezískal žádné peníze. Stejně tak druhý, neobžalovaný editor „Taran King" ani žádný z početných přispěvatelů *Phracku*.

Nicméně Chicagská operační skupina proti počítačové zpronevěře a zneužití počítače se rozhodla obvinit Neidorfa z finančního podvodu. Formálně připustit, že *Phrack* je „časopis" a Neidorf „vydavatel" by pro obžalobu znamenalo otevřít Pandořinu skříňku problémů kolem Prvního dodatku americké ústavy. Udělat něco takového by znamenalo nahrát na smeč Zennerovi a jeho poradcům z EFF, mezi nimiž byl i úderný oddíl prominentních newyorských advokátů specializujících se na občanská práva a profesionální právnické zázemí firmy Katten, Muchin a Zavis. Místo toho se obžaloba soustředila na otázku podvodu s použitím přístupového zařízení, na paragraf 1029 článku 18, na tu část zákona, z níž Tajná služba USA čerpala své nejpřímější pověření k pronásledování počítačového zločinu.

Zločiny, ze kterých byl Neidorf obžalován, se soustřeďovaly kolem Dokumentu 911. Byl obviněn, že se podílel na podvodném spiknutí s Prophetem, což, připomeňme si, byl atlantský člen LoDu, který ilegálně okopíroval Dokument 911 v systému AIMSX společnosti BellSouth.

Prophet sám byl v Neidorfově procesu také obžalován, jako společník údajného „podvodného spiknutí" s cílem „ukrást" společnosti BellSouth Dokument 911 (a přepravit ho přes hranici státu USA, což pomohlo prosadit obžalobu Neidorfa jako federální případ). Prophet, v duchu plné spolupráce s policií, souhlasil, že bude svědčit proti Neidorfovi.

Ve skutečnosti byli všichni tři atlantští hackeři připraveni svědčit proti Neidorfovi. Jejich vlastní federální žalobci v Atlantě obvinili Atlantskou trojku z: a) spiknutí, b) počítačového podvodu, c) telefonního podvodu, d) podvodu s použitím přístupového zařízení a e) mezistátní přepravy kradeného majetku (článek 18, paragrafy 371, 1030, 1343, 1029 a 2314).

Tváří v tvář takovému uragánu potíží se Prophet a Leftist vyhnuli veřejnému líčení a přiznali se k menším obviněním - každý k jednomu spiknutí. Urvile se přiznal k oné podivné části paragrafu 1029, jež zakazuje vlastnit „patnáct či více" ilegálních přístupových zařízení (v jeho případě počítačových hesel). A jejich rozsudky měly být vyneseny 14. září - bezpečně po skončení Neidorfova procesu. Dalo se spolehnout, že jako svědkové se budou chovat slušně.

Neidorf ale trval na tom, že je nevinný. Kromě něj prakticky každý, kdo byl při zátahu chycen, „plně spolupracoval" a přiznal se v naději, že jeho trest bude snížen. (Další důležitou výjimkou byl samozřejmě Steve Jackson, který od samého začátku důrazně tvrdil, že je nevinen. Ale Steve Jackson se nemohl dostat k soudu - Steve Jackson jednoduše nikdy nebyl obviněn ze žádného zločinu.)

Neidorf byl vyzýván, aby se přiznal. Ale Neidorf studoval společenské vědy a nechtělo se mu jít do vězení za „podvod", když nezískal žádné peníze, nepronikl do žádného počítače a publikoval časopis, který byl podle jeho názoru pod ochranou Prvního dodatku ústavy.

Neidorfův proces byl *jedinou* legální akcí z celého Zátahu na hackery, jež skutečně předestřela sporné otázky k veřejnému rozhodnutí porotou amerických občanů.

I Neidorf spolupracoval s policií. Dobrovolně vydal mnoho důkazů, jež vedly k jeho vlastnímu obvinění. Písemně připustil, že věděl, že Dokument 911 byl ukraden, ještě předtím, než ho „publikoval“ ve *Phracku* - nebo, z pohledu obžaloby, než ilegálně po telefonní lince přepravil kradený majetek jako součást něčeho, co se vydávalo za „publikaci“.

Ale i kdyby „publikace“ Dokumentu 911 nebyla uznána za zločin, neměl by Neidorf po starostech. Neidorf obdržel Dokument 911, když mu ho Prophet poslal z Jolnetu Riche Andrewse. A při té příležitosti určitě nebyl „publikován“ - byla to prostě a jednoduše hackerská trofej, přepravovaná přes hranici státu USA.

Chicagská operační skupina přesvědčila chicagskou velkou porotu, aby obvinila Neidorfa z řady zločinů, jež ho mohly dostat za mříže na třicet let. Když byla některá z těchto obvinění úspěšně zpochybněna ještě před tím, než se Neidorf dostal před soud, reorganizovala je Chicagská operační skupina tak, že mu hrozilo uvěznění na více než šedesát let! Neidorf nebyl dosud trestán, takže bylo velice nepravděpodobné, že jeho rozsudek bude tak drastický; ale Chicagská operační skupina zjevně usilovala o to, aby se dostal do vězení a jeho spiklenecký „časopis“ byl trvale zastaven. Šlo o federální případ a Neidorf byl obviněn z krádeže majetku za téměř osmdesát tisíc dolarů.

William Cook byl přesvědčen o užitečnosti žalob, které měly širokou publicitu a symbolické významy. Často publikoval články o své práci v listech pro bezpečnostní experty soukromého sektoru a tvrdil, že „bylo nutné vyslat jasný signál veřejnosti jako celku a počítačové komunitě zvláště, že pirátské útoky na počítače a krádeže počítačových informací soudy nebudou tolerovat“.

Předmět sporu byl komplikovaný, taktika obžaloby poněkud neortodoxní, ale Chicagská operační skupina měla až dosud úspěch. V roce 1989 přistřihla křídla Shadowhawkovi, jež byl odsouzen na devět měsíců do vězení. „Stínový jestřáb“ byl obviněn podle paragrafu 1030 o „počítačích federálního zájmu“.

Shadowhawk zajisté nebyl fanouškem „počítačů federálního zájmu“ jako takových. Naopak, Shadowhawk, jež vlastnil domácí počítač AT&T, směřoval své výboje zejména proti této společnosti. Na undergroundových boardech „Phreak Klass 2600“ a „Dr. Ripco“ se vytahoval svými schopnostmi a úmyslem shodit celostátní telefonní síť AT&T. Jeho tirád si všiml Henry Kluepfel z bezpečnostního odboru Bellcore, postrach pirátských boardů, který měl dlouholeté a úzké kontakty s Chicagskou operační skupinou.

Operační skupina před soudem úspěšně prokázala, že na nezletilého Shadowhawka se vztahuje paragraf 1030, navzdory námitkám jeho obhájce. Shadowhawk vnikl do počítače „ve vlastnictví“ Amerických raketových vojsk, jež byl pouze „spravován“ AT&T. Vnikl také do počítače AT&T umístěného na letecké základně Robbins v Georgii. Útoky na AT&T byly předmětem „federálního zájmu“, ať už to měl Shadowhawk v úmyslu či nikoli.

Operační skupina také přesvědčila soud, že software AT&T, který Shadowhawk ilegálně získal z Bellových laboratoří, tzv. „Expertní systém s umělou inteligencí C5“, měl cenu rovný milión dolarů. Shadowhawkův obhájce tvrdil, že Shadowhawk tento program neprodal a nezískal ze své kořisti žádný zisk. A ostatně expertní systém C5 byl experimentální a neměl reálnou tržní cenu, protože se prostě nikdy nedostal na trh. Jeden milión dolarů, na který AT&T odhadla cenu nehmotného vlastnictví AT&T, byl však soudem bez námitek akceptován. Soud rovněž souhlasil se žalobou, že Shadowhawk měl zjevný „úmysl defraudovat“, ať už získal nějaké peníze či nikoli. Shadowhawk dostal nepodmíněný trest.

Dalším slavným triumfem Chicagské operační skupiny bylo usvědčení a odsouzení Kyrie. Kyrie, skutečná obyvatelka digitálního podsvětí, byla šestatřicetiletá Kanaďanka, usvědčená a odsouzená za telekomunikační podvod v Kanadě. Po svém propuštění z vězení uprchla před hněvem společnosti Canada Bell a Královské kanadské jízdní policie a nakonec se usadila, velmi nemoudře, v Chicagu.

Kyrie, jež si také říkala „Informace o dálkových linkách“, se specializovala na zneužívání hlasové pošty. Shromažďovala ve velkém přístupové kódy umožňující dálkové hovory a pak je četla do různých systémů hlasové pošty velkých společností. Kyrie a její přátelé byli elektroničtí squatteři v systémech hlasové pošty, které používali, jako kdyby to byly pirátské boardy. Když jejich repetění celý systém zahltilo a majitelé nezbytně přijali protiopatření, odstěhovali se telefandové o dům dál. Kyriina družina byla volnou partou asi stopadesáti lidí, kteří sledovali její pirátskou stopu od počítače k počítači a s vášnivým zápalem loudili její znalosti a zkušenosti.

Kyriini učedníci jí předávali ukradená čísla kreditních karet výměnou za její „informace o dálkových linkách“. Někteří z jejích klientů platili v hotovosti, peněžními zálohami na kreditní karty ukradenými Western Unionu.

Kyrie neustále cestovala, většinou na letenky a do hotelových pokojů, které získala na ukradené kreditní karty. Unavovalo ji to, takže posléze našla útočiště u své známé z telefandovských kruhů v Chicagu. Kyriina hostitelka byla, jako překvapující množství telefandů, slepá. Byla i fyzicky handicapována. Kyrie údajně využila situace tak, že pod falešným jménem, jako kvalifikovaná ošetřovatelka, úspěšně požádala o státní podporu na starost o ni.

Nejsmutnější bylo, že Kyriiny dvě děti z jejího bývalého manželství zmizely v podzemí spolu s ní; tito malí digitální uprchlíci neměli žádnou legální americkou identitu a v celém svém životě nestrávili ani den ve škole.

Kyrii fascinovalo technické mistrovství a její vlastní chytrost; byla závislá na zbožňování svých nezletilých učedníků. Šla tak daleko, že zatelefonovala Gail Thackerayové v Arizoně, aby se vychloubala, chvástala a naparovala a nabídla jí, že se stane její informátorkou. Ale Thackerayová už o Kyrii ledacos věděla a opovrhovala jí jako dospělým zločincem svádějícím nezletilé, jako ekvivalentem pasáka. Thackerayová předala své pásky s Kyriiným chlubením Tajné službě USA.

Kyriin byt byl prohledán a ona sama zatčena v Chicagu v květnu 1989. Přiznala se k mnoha trestným činům.

V srpnu 1990 dostal Cook a jeho kolegyně z Chicagské operační skupiny Colleen Coughlinová Kyrii za mříže na 27 měsíců za počítačový a telefonní podvod. Podle obvyklých standardů hackerských procesů, v nichž byli viníci spíše jen „plácáni přes ruku“, to byl výjimečně přísný trest. Sedm Kyriiných nejpřednějších učedníků bylo rovněž obžalováno a odsouzeno. Kyriin „pouliční techno-gang“, jak ho nazval Cook, byl zlikvidován. Cook a jeho kolegové byli první, kdo poslal někoho do vězení za zneužívání hlasové pošty. Jejich průkopnická snaha jim vynesla veřejnou pozornost a chválu.

Ve svém článku o Kyrii předal Cook čtenářům časopisu *Security Management*, periodika pro bezpečnostní experty soukromých společností, nedvojsmyslnou zprávu. Tento případ, napsal, a Kyriin přísný trest, „odrážejí novou realitu pro hackery a oběti počítačových zločinů v devadesátých letech.... Soukromé osoby a společnosti, které oznámí počítačové a telefonní zločiny, mohou nyní očekávat, že jejich spolupráce s federálními orgány povede k vynesení účinných trestů. Společnosti i veřejnost jako celek musejí oznamovat zločiny páchané s pomocí počítače, jestliže chtějí, aby žalobci a soudy chránili jejich práva k hmotnému i nehmotnému vlastnictví, vyvíjenému a uloženému na počítačích.“

Cook si dal záležet, aby vytvořil tuto „novou realitu pro hackery“. Dal si také záležet na tom, aby vlastnická práva společností k jejich nehmotnému majetku byla trestně chráněna.

Kdyby byla Nadace elektronického pohraničí „fondem na obhajobu hackerů“ v obvyklém významu tohoto pojmu, patrně by se zastala Kyrie. Její rozsudek skutečně vyslal „signál“, že muži zákona vytáhli proti „hackerům“. Ale Kyrie nenašla v EFF žádné zastánce - a ostatně ani nikde jinde. EFF nebyla fondem na kauce pro elektronické zloděje.

Případ Neidorfa byl v jistých ohledech analogický případu Shadowhawka. Cenu „ukradeného“ majetku opět určila oběť. Kluepfel byl opět jak vyšetřovatelem, tak technickým poradcem. Opět nedošlo k žádným finančním transakcím, ale „úmysl defraudovat“ byl ústřední.

Již v počáteční fázi se objevily některé slabiny obžaloby. Chicagská operační skupina původně hodlala prokázat, že Neidorf byl hlavní postavou celostátního zločinného spiknutí Legion of Doom. Redaktoři *Phracku* pořádali každé léto srazy, jichž se zúčastnili hackeři z celých Spojených států, zpravidla asi dva tucty přispívatelů a čtenářů časopisu, jichž si redakce vážila. (Takováto setkání byla v hackerské komunitě běžná - například časopis *2600* pořádal veřejná setkání hackerů v New Yorku každý měsíc.) Hvězdy LoDu byly na těchto „letních conech“, sponzorovaných *Phrackem*, vždy silně zastoupeny.

V červenci 1988 navštívil arizonský hacker jménem „Diktátor“ con v Neidorfově rodném St. Louis. Diktátor byl jedním z informátorů Gail Thackerayové; jeho undergroundový board ve Phoenixu byl nastraženým boardem Tajné služby USA. Diktátor přivedl na con inkognito tým agentů Tajné služby USA. Agenti vyvrtali otvory skrz zeď Diktátorova hotelového pokoje a natočili bavící se hackery jednosměrným zrcadlem. Jenže na videokazetách nebylo, s výjimkou pití piva několika nezletilými, nic ilegálního. Letní cony byly společenskou událostí, nikoli zlověstným spiknutím. Na kazetách bylo patnáct hodin nevázaného smíchu, jedení pizzy, soukromých vtipů a plácání po zádech.

Neidorfův právník Sheldon Zenner viděl kazety Tajné služby před zahájením procesu. Byl šokován dokonalou neškodností tohoto setkání, jež Cook dříve charakterizoval jako nebezpečné celostátní spiknutí podvodníků. Zenner chtěl ukázat kazety z conu v St. Louis porotě. Chicagská operační skupina musela dlouho manévrovat, aby prezentaci „irelevantních“ kazet zabránila.

I Dokument 911 se projevil jako slabé místo. Původně byla jeho cena stanovena na 79 449 dolarů. Ovšem na rozdíl od Shadowhawkova tajuplného, uměle inteligentního lupu nebyl Dokument 911 žádný program, ale anglický text. Lidé obeznámení s počítači pokládali takovou cenu dvanáctistránkového úředního dokumentu za doslova neuvěřitelnou. Ve svém manifestu EFF „Zločin a tajemství“ to Barlow komentoval: „Patrně se nikdy nedovíme, jak, či kým, bylo tohoto čísla dosaženo, ale já si představuji hodnotící tým složený z Franze Kafky, Josepha Hellera a Thomase Pynchona.“

Ve skutečnosti byl Barlow přehnaně pesimistický. EFF nakonec zjistila, jak přesně bylo tohoto čísla dosaženo a kým - ale až v roce 1991, dlouho po skončení Neidorfova procesu.

Kim Megahee, bezpečnostní manažer společnosti Southern Bell, určil jeho cenu prostým součtem „cen spojených s produkcí“ Dokumentu 911. „Ceny“ byly následující:

1. Byl najat pisatel technických textů, aby shromáždil potřebné údaje a napsal Dokument 911. 200 hodin práce po 35 dolarech na hodinu stálo 7 000 dolarů. Pisatele kontroloval manažer projektu. Jeho 200 hodin po 31 dolarech na hodinu stálo 6 200 dolarů.
2. Týden psaní na stroji stál 721 dolarů. Týden formátování dalších 721 dolarů. Týden grafického formátování 742 dolarů.
3. Dva dny konečné úpravy stály 367 dolarů.
4. Krabice nálepek stála pět dolarů.
5. Příprava objednávky na Dokument 911, včetně psaní na stroji a získání písemného potvrzení od zodpovědného úředníka BellSouth, stála 129 dolarů.
6. Tisk stál 313 dolarů. Rozeslání Dokumentu padesáti lidem zabralo sekretářce padesát hodin a stálo 858 dolarů.
7. Zařazení Dokumentu do indexu zabralo dvěma sekretářkám po hodině práce, celkem 43 dolarů.

Samotné organizační výdaje tedy údajně byly 17 099 dolarů. Podle pana Megaheeho zabralo opsání dvanáctistránkového dokumentu na stroji celý týden. Jeho psaní zabralo pět týdnů, a to i dohližiteli, jež zjevně pět týdnů nedělal nic jiného než pozoroval autora při práci. Konečná úprava dvanácti stran zabrala dva dny. Vytištění a rozeslání elektronického dokumentu (který už byl dostupný v síti Southern Bell každému zaměstnanci, jež ho potřeboval), stálo více než tisíc dolarů.

Ale to byl jen začátek. Byly zde ještě *hardwarové výlohy*. Osm set padesát dolarů za počítačový monitor VT220. *Jednatřicet tisíc dolarů* za výkonný počítač VAXstation II. Šest tisíc dolarů za počítačovou tiskárnu. *Dvaadvacet tisíc dolarů* za kopii softwaru „Interleaf“. Dva a půl tisíce dolarů za software VMS. To všechno k vytvoření dvanáctistránkového dokumentu.

Plus deset procent ceny softwaru a hardwaru za údržbu. (Ve skutečnosti nebyla cena za údržbu, ačkoli byla uvedena, připočtena k celkové sumě 79 449 dolarů, zjevně v důsledku milosrdného přehlédnutí.)

Dopis pana Megaheeho byl poslán přímo Williamu Cookovi, do chicagského úřadu federálních žalobců. Vláda Spojených států amerických akceptovala tato čísla poskytnutá telefonní společností bez jediné otázky.

Jak se nevěřícný úžas šířil, byla hodnota Dokumentu 911 oficiálně revidována směrem dolů. Robert Kibler z bezpečnostního odboru BellSouth odhadl cenu těchto dvanácti stran na pouhých 24 639 dolarů a 5 centů - údajně na základě „výdajů na výzkum a vývoj“. Ale ani tento odhad, přesný až do jediného nikláku, skeptiky nepřesvědčil; vyprovokoval jen pohrdavé úsměšky a záplavu sarkastických vtipů.

Finanční otázky kolem krádeží copyrightovaných informací byly vždy sporné. Dá se tvrdit, že společnost BellSouth především nikdy *nepřišla* o svůj Dokument 911, a tedy neutrpěla jeho „krádeží“ žádnou peněžní škodu. A Sheldon Zenner při Neidorfově procesu také tvrdil, že Prophetův čin nebyl „krádeží“, ale spíše ilegálním kopírováním.

Žádné ze stran ovšem v tomto procesu ve skutečnosti nešlo o peníze. Cookovou strategií nebylo přesvědčit porotu, že Dokument 911 měl velkou cenu a že jeho krádež by měla být potrestána především z tohoto důvodu. Jeho strategií bylo argumentovat, že Dokument 911 je *nebezpečný*. Měl v úmyslu přesvědčit soud, že Dokument 911 je „mapou“ systému tísňového volání. Neidorf úmyslně a nezodpovědně distribuoval nebezpečnou zbraň. Neidorfa ani Propheta nezajímalo (nebo jim tato zlověstná představa dokonce dělala radost), že Dokument 911 může být hackery zneužit k poškození systému 911, „záchranného pásu nejen pro všechny obyvatele regionu společnosti Southern Bell, ale i pro mnoho jiných komunit po celých Spojených státech“, podle vlastních Cookových slov. Neidorf ohrozil životy lidí.

Při manévrování před zahájením soudu Cook dosáhl toho, že Dokument 911 byl uznán za příliš nebezpečný, než aby byl zařazen do veřejných materiálů Neidorfova procesu. Ani *porota* neměla tento dokument nikdy spatřit, aby nepronikl do oficiálních soudních záznamů, a tedy do rukou veřejnosti, a tedy, případně, do rukou zlovolných hackerů, kteří by ho mohli smrtelně nebezpečným způsobem zneužít.

Ukrýt Dokument 911 před porotou mohlo být vtipným právnickým manévrem, ale tento postup měl vážnou chybu. Existovaly totiž stovky a možná tisíce lidí, kteří již měli Dokument 911, přesně v té formě, v níž ho *Phrack* publikoval. Jeho pravá podstata byla již zřejmá podstatné části veřejnosti zaujaté případem (a mimochodem, všichni tito lidé byli, aspoň teoreticky, společníky gigantického podvodného spiknutí). Prakticky každý člen elektronické komunity, jež měl modem a třeba jen minimální zájem na Neidorfově případu, už měl kopii Dokumentu 911. Ve *Phracku* byl dostupný už více než rok.

Lidé, včetně naprosto normálních lidí, kteří neměli žádné zvláštní sklony špiclovat zakázané vědění, nezavřeli hrůzou oči při myšlence, že vlastní „nebezpečný“ dokument telefonní společnosti. Naopak, zpravidla se spolehli na svůj vlastní úsudek a Dokument 911 si prostě přečetli. A neudělal na ně valný dojem.

Jedním z těchto lidí byl John Nagle. Nagle byl jednačtyřicetiletý profesionální programátor, který vystudoval informatiku na Stanfordské univerzitě. Pracoval pro Ford Aerospace, kde vynalezl techniku propojování počítačů do sítě známou jako „Naglův algoritmus“, a pro celosvětově známou kalifornskou firmu Autodesk, specializující se na počítačovou grafiku, jejímž byl významným akcionářem.

Nagle byl také váženou osobností na WELLu, kde byl respektován pro své technické znalosti.

Nagle pečlivě sledoval debatu o občanských právech, protože byl vášnivým přívržencem elektronické komunikace. Nebyl žádným zvlášt-

ním příznivcem lidí pronikajících do počítačů, ale věřil, že elektronické publikace mohou být pro celou společnost velkým dobrodiním, a pokusy o omezení jejich růstu či svobody elektronického projevu vzbuzovaly jeho rozhodný odpor.

Neidorfův případ a Dokument 911 byly detailně rozebírány na Internetu, v elektronické publikaci *Telecom Digest* („Telekomunikační výběr“). Nagle, který se Internetu již dlouho věnoval, byl jeho pravidelným čtenářem. Nagle nikdy neviděl časopis *Phrack*, ale okolnosti případu ho znepokojovaly.

V jednom stanfordském knihkupectví si Nagle při hledání knih o robotice všiml knihy *The Intelligent Network* („Inteligentní síť“). Při náhodném listování narazil na celou kapitolu, důkladně popisující detaily systému tísňového volání 911. Tento podrobný text byl normálně prodáván, a mladému muži v Illinois přitom hrozilo vězení za publikaci útlého šestistránkového dokumentu o systému 911.

Nagle zveřejnil v *Telecom Digestu* v tomto smyslu ironickou poznámku. To vedlo k jeho spojení s Mitchem Kaporem, a posléze s Neidorfovými právníky.

Sheldon Zenner byl velice potěšen, že našel experta na telekomunikace, ochotného podpořit Neidorfa a přitom žádného pochybného nezletilého „hackera“. Nagle byl výmluvný, dospělý a vážený občan; svého času měl federální oprávnění zacházet s tajnými informacemi.

Nagle byl požádán, aby přiletěl do Illinois a přidal se k týmu obhajoby.

Nagle se stal expertním svědkem obhajoby, přečetl si celý Dokument 911 a dospěl ke svým vlastním závěrům o jeho potenciální hrozbě.

***

A nyní nastal čas, abyste se vy, čtenáři, sami podívali na Dokument 911. Tento šestistránkový text byl oficiálním důvodem federálního soudu, jež mohl dostat elektronického vydavatele do vězení na třicet nebo dokonce šedesát let. Byl oficiálním důvodem domovní prohlídky a zabavení počítačů Steva Jacksona, legitimního vydavatele tištěných knih. Byl i oficiálním důvodem prohlídky a zabavení Mentorova boardu „Projekt Fénix“ a pro razii u Erika Bloodaxe. Měl také mnoho co dělat se zabavením unixovského Jolnetu Richarda Andrewse a odpojením nodu AT&T spravovaného Charlesem Boykinem. Dokument 911 byl tím nejdůležitějším jednotlivým důkazem Zátahu na hackery. Nelze postupovat jinak než předložit dokument samotný.

```
==Phrack Inc.==

Svazek 2, číslo 24, soubor 5 z 13

Struktura Kontrolního odboru
pro rozšířené služby
zvláštním službám a významným zákazníkům 911

autor: Eavesdropper

březen 1988


Popis služby
~~~~~~~~~~~~
Kontrolní odbor  systému tísňového volání  911 je v  souladu
s existujícími standardními procedurami zařazen pod některou
z následujících center:

o  Centrála speciálních služeb (CSS)
o  Centrála významných zákazníků (CVZ)
o  Pomocná testovací centrála (PTC)
o  Centrála kontroly poplatků (CKP)

Označení CSS/CVZ je v  tomto dokumentu používáno zaměnitelně
pro všechny čtyři tyto centrály. Centrály speciálních služeb
(CSS) a Centrály významných zákazníků (CVZ) byly koncipovány
jako kontaktní místa pro hlášení problémů pro všechny
zákazníky  systému 911  (VBVB), kteří  hlásí problémy.
Předplatitelé,  kteří  mají  problémy  uskutečnit  hovor
v systému  911 budou i nadále  kontaktovat místní opravářské
služby  (COSRB), které  podají o  problémech zprávu CSS/CVZ,
kdykoli to bude na místě.

Vzhledem  ke  kritické  důležitosti  služeb  systému  911 je
vyžadováno  řízení a  včasné opravy  problémů. Jako primární
kontakt  pro zákazníky  911 má  CSS/CVZ nejvhodnější  pozici
k monitorování stavu problémů a zajištění jejich řešení.

Přehled systému
~~~~~~~~~~~~~~~
Číslo  911  je  koncipováno  jako  celostátní  univerzální
telefonní  číslo,  poskytující  veřejnosti  přímý  přístup
k Veřejným bezpečnostním vstupním bodům (VBVB). VBVB je také
označován  jako  Kancelář  tísňových  služeb  (KTS). VBVB je
organizace  či  úřadovna,  autorizovaná  místními  orgány
přijímat a  reagovat na žádosti o  služby policie, požárníků
a/nebo rychlé  lékařské pomoci. V úřadovně  VBVB je přítomen
jeden nebo  více služeb, kteří  přijímají a vyřizují  hovory
```

```
tísňové povahy v souladu s požadavky místních orgánů.

Důležitou výhodou systému tísňového volání 911 je zlepšená
(zkrácená) doba odezvy na tísňová volání. Také úzká
spolupráce mezi institucemi poskytujícími různé služby
v nouzových situacích je cenným rysem systému 911.

Základem sítě 911 jsou ústředny 1A, směrující všechny hovory
911 do příslušného (primárního) VBVB, přiřazeného volající
stanici. Vlastnost 911 byla vyvinuta zejména proto, aby
umožnila směrování všech hovorů 911 příslušnému VBVB.
Speciální směrování umožňuje, aby byl hovor 911 z konkrétní
stanice umístěné v konkrétním okrsku, zóně či městě směrován
primárnímu VBVB, jež má sloužit této stanici bez ohledu na
hranice telefonních obvodů. Speciální směrování tedy
eliminuje problém hranic telefonních obvodů, jež se
nepřekrývají s hranicemi okrsků či jiných politických území.

V systému 911 jsou dostupné mj. následující služby:

Nucené přerušení spojení      Implicitní směrování
Alternativní směrování        Noční služba
Selektivní směrování          Automatická čísla
Identifikace (ANI)
Selektivní transfer           Automatická lokalizace
Identifikace (ALI)

Úvodní a instalační procedury
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
Po podepsání kontraktu na systém 911 má Síťový marketing
zodpovědnost za vytvoření výboru pro implementaci
a přípravné práce, v němž by měl být zástupce CSS/CVZ.
Povinnosti Implementačního týmu 911 zahrnují koordinaci
všech fází uvádění systému 911 do provozu a zformování
stálého podvýboru pro údržbu 911.

Marketing je zodpovědný za poskytnutí následujících
informací o zákazníkovi CSS/CVZ, dříve než bude zahájen
zkušební provoz:

o Všechny VBVB (jméno, adresa, místní kontakt)
o Síťová identifikační čísla všech VBVB
o Žádost o systém 911, formulář 1004 včetně detailních
  požadavků VBVB na služby VBVB (1004, sekce K, L, M)
o Konfigurace sítě
o Veškeré informace o prodejcích (číslo, telefon, vybavení)
[...]
```

Čtenáři je nutno prominout, byl-li zcela neschopen tento dokument přečíst. [A čtenář tohoto překladu to snad promine překladateli - kompletní text je dostupný v anglickém originále.] John Perry Barlow si na jeho účet užil ve „Zločinu a tajemství“ spoustu legrace: „Byrokratický žargon nepřekonatelné nesrozumitelnosti... Přečíst celý text na jeden zátah a nezkolabovat vyžaduje buď stroj, nebo člověka, jež má příliš mnoho praxe ve strojovém myšlení. Každý, kdo mu dokáže okamžitě a plně porozumět, změnil své vědomí natolik, že navždy ztratil schopnost číst Blakea, Whitmana či Tolstého... Tento dokument nemůže zaujmout nikoho kromě studenta pokročilé organizační paralýzy.“

Ale s Dokumentem 911 při ruce, přesně v té formě, v níž byl (zkrácený na šest stran) publikován ve *Phracku*, si čtenář může ověřit několik tvrzení o jeho povaze. Za prvé, v dokumentu není žádný počítačový kód. Není to programovací jazyk jako Fortran či C++, je psán anglicky; všechny věty mají podněty a přísudky a interpunkci. Nevysvětluje, jak proniknout do systému 911. Nemluví o cestách k jeho zničení či poškození.

V Dokumentu 911 nejsou žádné přístupové kódy a žádná počítačová hesla. Nevysvětluje, jak se vyhnout placení dálkových hovorů. Nevysvětluje, jak se vloupat do telefonní ústředny. Není v něm nic o používání počítače či modemu, ať k dobrému či zlému.

Pečlivé studium ukáže, že tento dokument není o strojích. Dokument 911 je o *organizaci*. Popisuje, jak se vytvářejí a spravují jisté organizační jednotky telekomunikační byrokracie: Centrály speciálních služeb a Centrály významných zákazníků (CSS/CVZ). Popisuje, jakými cestami mají tyto centrály distribuovat zodpovědnost za provoz systému 911 jiným organizačním jednotkám v hierarchii telekomunikační společnosti. Popisuje, kdo odpovídá na stížnosti zákazníků, kdo přebírá hovory, kdo podává zprávy o poruchách techniky, kdo na ně reaguje, kdo se stará o údržbu, kdo vede podvýbory, kdo dává rozkazy, kdo je plní, *kdo* *komu* říká, co má dělat. Dokument 911 není „mapou“ ukazující cesty k počítačům. Dokument 911 ukazuje cesty *k lidem*.

Jako pomůcka pro pronikání do počítačových systémů je tento dokument *k ničemu*. Jako pomůcka k obtěžování a klamání spojařů by ale mohl být užitečný (zvláště se svým glosářem, který zde není uveden). Důkladným a dlouhodobým studiem Dokumentu 911 a jeho glosáře, spolu s mnoha dalšími takovými dokumenty, by se člověk mohl naučit mluvit jako zaměstnanec telefonní společnosti. A zaměstnanci telekomunikací *žijí* řečí - telefonními hovory. Když je v telefonu dokážeš přesvědčit, že jsi jedním z nich, můžeš na nich uplatnit „sociální inženýrství“. Když je dokážeš podvést, můžeš mezi nimi způsobit chaos. Můžeš je donutit, aby přestali věřit jeden druhému; můžeš v nich vypěstovat paranoiu. Můžeš přerušit svazky, které drží jejich komunitu pohromadě. A lidé budou bránit svoji komunitu s větším nasazením než

sebe samé.

Toto byla pravá, skutečná hrozba časopisu *Phrack*. Boj se ve skutečnosti vedl o kontrolu jazyka spojařů a jejich znalostí. Byl to boj o membránu oddělující jejich komunitu, o materiál zdí jejich slonovinové věže. Bránili žargon, který jim umožňuje poznat jeden druhého a odhalit šarlatány, zloděje a plebs. A obžaloba to veřejně konstatovala. Opakovaně upozorňovali na hrozbu, jež pro profesionální spojaře představuje „sociální inženýrství".

Nicméně Craig Neidorf nebyl souzen za to, že se učil mluvit jako profesionální odborník na telekomunikace. Craig Neidorf byl souzen za podvod s použitím přístupového zařízení a přepravu kradeného majetku. Byl souzen za krádež údajně velmi citlivého dokumentu, jež měl údajně cenu desítek tisíc dolarů.

John Nagle si přečetl Dokument 911. Dospěl ke svým vlastním závěrům. A ukázal Zennerovi a jeho týmu krabici plnou podobného materiálu, získaného zejména z technických knihoven Stanfordské univerzity. Během soudu studoval tým obhajoby - Zenner, půl tuctu dalších právníků, Nagle, Neidorf a specialistka na počítačovou bezpečnost Dorothy Denningová - Dokument 911 řádek po řádku.

Odpoledne 25. července 1990 začal Zenner s křížovým výslechem Billie Williamsové, manažerky pro služby Southern Bellu v Atlantě. Paní Williamsová byla zodpovědná za Dokument 911 (Nebyla jeho autorkou - jeho původním „autorem" byl personální manažer Southern Bellu Richard Helms. Nicméně z existence Dokumentu 911 by neměl být viněn jen on; přispělo k němu mnoho úředníků Southern Bellu a lidí starajících se o údržbu sítě. Dokument 911 nebyl ani tak „napsán" jediným autorem jako sestaven příslušným výborem z betonových bloků žargonu.)

Paní Williamsová byla povolána jako svědek obžaloby a energicky se pokoušela objasnit základní technickou strukturu systému 911, pomáhajíc si několika diagramy.

Teď byla řada na Zennerovi. Nejdříve objasnil, že značka „důvěrné", kterou společnost BellSouth použila na Dokumentu 911, byla dávána na *každý* dokument, který byl v BellSouth napsán - na *tisíce* dokumentů. „Nepublikujeme nic jiného než dokumenty pro společnost," vysvětlila paní Williamsová. „Každý dokument tohoto druhu je společností považován za důvěrný." Nikdo neměl na starosti vybírání speciálních, zvláště citlivých materiálů, jimž by byla věnována speciální, zvláště důkladná ochrana. *Všechny* byly speciální, i ty nejtriviálnější, bez ohledu na to, co v nich bylo - jakmile byl nějaký dokument napsán, byl označen jako důvěrný, a toto označení nebylo nikdy odstraňováno.

Zenner se zeptal, jsou-li diagramy, jež používala při vysvětlování principů systému 911, také „důvěrné". Nebo byly tyto diagramy a předložená fakta o VBVB, ALI, uzlech a místních koncových ústřednách *veřejnou informací*? Mohl vzít tyto diagramy na ulici a ukazovat je kolemjdoucím, „aniž by se to příčilo nějaké představě, kterou má společnost BellSouth o svém vlastnictví?"

Paní Williamsová projevila určitou nerozhodnost, ale nakonec souhlasila s tím, že diagramy jsou vskutku veřejné.

„Ale copak to, co jste řekla, není v podstatě to, co se objevilo ve *Phracku*?

Paní Williamsová to odmítla.

Zenner nyní zdůraznil, že verze Dokumentu 911 publikovaná ve *Phracku* byla pouze poloviční ve srovnání s originálem (jak ho získal Prophet). Polovina byla smazána - vypuštěna Neidorfem.

Paní Williamsová namítla, že „většina informací v textovém souboru je redundantních."

Zenner pátral dál. Přesně které informace v Dokumentu 911 byly ve skutečnosti veřejnosti neznámé? Umístění počítačů systému 911? Telefonní čísla zaměstnanců společnosti? Složení stálých podvýborů pro údržbu? Neodstranil Neidorf většinu těchto informací?

Pak udeřil. „Jste obeznámena s Technickou referenční příručkou Bellcore, dokumentem TR-TSY-000350?" Jeho oficiální název byl, jak Zenner vysvětlil, „Rozhraní Veřejného bezpečnostního vstupního bodu mezi ústřednou 1-1AESS a vybavením zákazníka v systému 911". Obsahoval vysoce detailní a specifické technické informace o systému 911. Byl publikován Bellcore a dostupný veřejnosti asi za dvacet dolarů.

Ukázal svědkyni katalog Bellcore, v němž byly tisíce dokumentů od Bellcore a všech ostatních následnických společností Bellu včetně BellSouth. Katalog, jak Zenner zdůraznil, byl zdarma. Každý majitel kreditní karty mohl zavolat Bellcore (hovor byl placen volaným) a objednat si kterýkoli z těchto dokumentů, jež byly zákazníkům rozesílány bez jakýchkoli otázek. Včetně, například, „Rozhraní BellSouth pro vybavení zákazníka ve Veřejném bezpečnostním vstupním bodě systému 911".

Zenner dal svědkyni kopii „Rozhraní BellSouth", jež stála, jak zdůraznil, 13 dolarů, objednanou podle katalogu. „Podívejte se na ni pečlivě," vyzval paní Williamsovou, „a řekněte mi, zdali neobsahuje asi tak dvakrát více detailů o systému 911 společnosti BellSouth, než se objevilo kdekoli ve *Phracku*.

„Vy chcete, abych..." Paní Williamsová se zajíkla. „Nerozumím."

„Podívejte se pečlivě," naléhal Zenner. „Prohlédněte si tento dokument, a až s tím budete hotova, řekněte mi, zdali vskutku neobsahuje mnohem více detailů o systému 911, než se objevilo ve *Phracku*."

„*Phrack* nevycházel z tohohle," řekla paní Williamsová.

„Prosím?" řekl Zenner.

„*Phrack* nevycházel z tohohle."

„Neslyším vás," řekl Zenner.

„*Phrack* nevycházel z tohoto dokumentu. Nerozumím vaší otázce."

„Asi opravdu ne," řekl Zenner.

Případ obžaloby utrpěl smrtelnou ránu. Paní Williamsová byla upřímně nešťastná a zmatená. *Phrack* nevycházel z žádného veřejně dostupného dokumentu BellSouth. Dokument 911 zveřejněný ve *Phracku* byl ukraden z počítačů její vlastní společnosti, z textových dat její vlastní společnosti, která napsali a pečlivě revidovali její vlastní kolegové.

Ale *hodnota* Dokumentu 911 byla v troskách. Nestál za osmdesát tisíc dolarů. Podle Bellcore stál za třináct. A zlověstná hrozba, kterou údajně představoval, byla odhalena jako bezmocný strašák. Samotné Bellovy laboratoře prodávaly mnohem detailnější a „nebezpečnější" materiál komukoli, kdo měl kreditní kartu a telefon.

Ve skutečnosti Bellcore nedávalo své informace jednoduše komukoli. Dávalo je *komukoli, kdo o ně požádal*, ale žadatelů nebylo mnoho. Nebylo mnoho lidí, kteří věděli, že Bellcore má katalog a číslo placené volaným. John Nagle to věděl, ale průměrný nezletilý telefanda určitě ne. Tuc, Neidorfův přítel a příležitostný přispěvatel *Phracku*, to věděl, a byl za scénou velmi užitečným pomocníkem obhajoby. Ale členové Legion of Doom to nevěděli - jinak by nikdy neztráceli tolik času vybíráním popelnic. Cook to nevěděl. Foley to nevěděl. Kluepfel to nevěděl. Pravá ruka Bellcore nevěděla, co dělá levá. Pravá nelítostně stíhala hackery, zatímco levá distribuovala duševní vlastnictví Bellcore každému, koho zajímaly technické detaily telefonů - zjevně jen pár excentrikům.

Digitální underground byl tak amatérský a špatně organizovaný, že tento nehlídaný poklad nikdy neobjevil. Slonovinová věž telecomu byla tak zahalena mlhou své vlastní technické komplikovanosti, že mohla mít všechna okna otevřená a dveře dokořán. A nikdo si toho nevšiml.

Zenner si vzal další hřebík do rakve. Předložil číslo časopisu *Telefonní technika a management*, významného tištěného periodika specializovaného na telekomunikace, vydávaného dvakrát měsíčně a stojícího ročně 27 dolarů. Toto konkrétní číslo *TT&M* se jmenovalo *Novinky 911* a obsahovalo záplavu technických detailů o systému 911 a glosář mnohem rozsáhlejší než ve *Phracku*.

Proces pokračoval v podstatě už jen svou vlastní setrvačností. Tim Foley svědčil o tom, jak vyslýchal Neidorfa. Neidorfovo písemné přiznání, že věděl, že Dokument 911 byl získán ilegálně, bylo oficiálně přečteno do soudního záznamu.

Objevila se zajímavá vedlejší otázka: Terminus kdysi poslal Neidorfovi unixovský program společnosti AT&T, zpracovávající přihlašování uživatelů, rafinovaně upravený tak, aby umožňoval zachycování hesel. Program sám byl ilegálně zkopírovaným majetkem AT&T, a způsob, jakým ho Terminus upravil, ho změnil na nástroj pro usnadňování průniků do počítačů. Terminus sám se nakonec přiznal ke krádeži tohoto programu a Chicagská operační skupina ho za to poslala do vězení. Ale jeho význam v Neidorfově případě byl pochybný. Neidorf onen program nenapsal. Nebyl obviněn z toho, že by ho kdy použil. A nebyl obžalován z krádeže softwaru ani z vlastnictví nástroje na zachycování hesel.

Další den přešel Zenner do útoku. Ochránci občanských práv teď nasadili svou vlastní neobvyklou a nevyzkoušenou zbraň - Zákon o soukromí v elektronické komunikaci z roku 1986, paragraf 2701 a následující. Podle paragrafu 2701 je zločinem úmyslně a bez oprávnění vniknout do zařízení poskytujícího elektronickou komunikaci - v zásadě je to zákon proti elektronickým štěnicím a odposlechu telefonů, jehož účelem je rozšířit tradiční ochranu telefonů na další elektronické formy komunikace. Ovšem kromě trestů pro amatérské čmuchaly vymezuje paragraf 2701 i několik procedurálních požadavků na policejní štěnice a odposlech.

Tajná služba USA, reprezentovaná Timem Foleym, předložila Richardu Andrewsovi, v rámci svého pronásledování Propheta, Dokumentu 911 a Terminusovy sítě pro šíření softwaru, předvolání před federální velkou porotu. Ale podle Zákona o soukromí v elektronické komunikaci má „poskytovatel dálkových počítačových služeb“ právní nárok na „předchozí upozornění“ vlády, než je použito předvolání. Richard Andrews a jeho sklepní unixovský node Jolnet nedostali žádné „předchozí upozornění“. Tim Foley údajně porušil Zákon o soukromí v elektronické komunikaci a spáchal počítačový zločin! Zenner usiloval o svolení soudu ke křížovému výslechu Foleyho o jeho vlastním elektronickém másle na hlavě.

Cook argumentoval, že Jolnet Richarda Andrewse byl soukromým boardem a nespadal pod Zákon o soukromí v elektronické komunikaci. Soudce Bua uznal žádost vlády o zákaz křížového výslechu k tomuto bodu a Zennerova ofenzíva ztratila dech. Šlo nicméně o první vážné zpochybnění legality akcí samotné Chicagské operační skupiny - první tvrzení, že oni sami porušili zákon a mohou být, možná, voláni k zodpovědnosti.

V každém případě Zenner Zákon o soukromí v elektronické komunikaci nijak zvlášť nepotřeboval. Místo toho zahnal Foleyho do defenzívy otázkami o nepřehlédnutelných rozporech v údajné ceně Dokumentu 911. Prezentoval také trapnou skutečnost, že údajně smrtelně nebezpečný Dokument 911 ležel několik měsíců na Jolnetu, s Kluepfelovým vědomím, a Kluepfel se nijak nesnažil něco s tím udělat.

Odpoledne byl přiveden Prophet, jež měl svědčit pro obžalobu. (Prophet, jak známo, byl v tomto procesu rovněž obžalován jako Neidorfův partner při podvodu.) V Atlantě se Prophet už přiznal k jednomu spiknutí, jednomu telefonnímu podvodu a jedné mezistátní přepravě kradeného majetku. Obvinění z telefonního podvodu a z mezistátní přepravy kradeného majetku se přímo týkala Dokumentu 911.

Dvacetiletý Prophet se choval melancholicky. Na otázky odpovídal zdvořile, ale tak potichu, že skoro nebyl slyšet, a jeho hlas se na konci vět vytrácel. Byl neustále vyzýván, aby mluvil hlasitěji.

Cook, vyslýchající Propheta, ho přiměl k přiznání, že měl kdysi „potíže s drogami“ - zneužíval amphetaminy, marihuanu, kokain a LSD. Mohlo to přesvědčit porotu, že „hackeři“ jsou, nebo mohou být, špinavé odpudivé trosky, ale také to mohlo poškodit Prophetovu věrohodnost. Zenner později prohlásil, že drogy mohly narušit Prophetovu paměť. Objevil se i pozoruhodná skutečnost, že Prophet se nikdy fyzicky nesetkal s Craigem Neidorfem. Neznal ani jeho příjmení - přinejmenším do zahájení procesu.

Prophet potvrdil základní fakta o své hackerské kariéře. Byl členem Legion of Doom. Zneužíval přístupové kódy, reprogramoval telefonní ústředny a přesměrovával hovory, připojoval se na pirátské boardy. Vnikl do počítače systému AIMSX společnosti BellSouth, zkopíroval Dokument 911, uložil ho na Jolnetu a poslal Neidorfovi. Spolu s Neidorfem ho editovali a Neidorf věděl, odkud dokument pochází.

Na Zennerovu výzvu ale také potvrdil, že Neidorf nebyl členem Legion of Doom a nenaváděl Propheta, aby se vloupal do počítače BellSouth. Neidorf po Prophetovi nikdy nechtěl, aby někoho podvedl či něco ukradl. Prophet také připustil, že mu není známo, že by Neidorf kdy pronikl do nějakého počítače. Prophet řekl, že žádný člen Legion of Doom nikdy nepovažoval Craiga Neidorfa za „hackera“. Neidorf nebyl odborníkem na Unix a jednoduše neměl znalosti a schopnosti potřebné k pronikání do počítačů. Neidorf prostě vydával časopis.

V pátek 27. července 1990 se případ proti Neidorfovi zhroutil. Cook požádal o zrušení procesu, z důvodu „nových informací, jež nám před podáním obžaloby nebyly dostupné“. Soudce Bua pochválil obžalobu za tuto akci, již nazval „velmi zodpovědnou“, propustil porotu a prohlásil soud za zmatečný.

Neidorf byl volný. Ale jeho obhajoba přišla jeho i jeho rodinu draho. Ztratil několik měsíců života ve víru nebezpečné krize; jeho nejbližší přátelé se k němu obrátili zády jako k počítačovému zločinci. Dlužil svým právníkům více než sto tisíc dolarů, i když Mitch Kapor velkoryse přispěl na jeho obhajobu.

Neidorf nebyl shledán nevinným. Jeho proces byl prostě zrušen. Nicméně 9. září 1991 uznal soudce Bua Neidorfovu žádost o „výmaz a zapečetění“ záznamu o jeho obžalobě. Tajná služba USA dostala příkaz odstranit a zničit všechny otisky prstů, fotografie a ostatní záznamy o zatčení a dalších procesních úkonech souvisejících s Neidorfovým obviněním, včetně písemných dokumentů a počítačových záznamů.

Neidorf se vrátil do školy, skálopevně rozhodnut stát se advokátem. Po pohledu zblízka na práci justičního systému ztratil mnoho ze svého entuziasmu pro pouhou technickou moc. V době vzniku této knihy pracuje Craig Neidorf ve Washingtonu jako rešeršér pro American Civil Liberties Union.

Výsledek Neidorfova procesu přes noc změnil EFF z hlasu volajícího na poušti na mediální reprezentaci nové země.

Z čistě právního hlediska nebyl Neidorfův případ triumfem žádné zúčastněné strany. Nebyly stanoveny žádné ústavní principy. Otázky „svobody slova“ elektronických vydavatelů nebyly řešeny. Na veřejnosti se šířily mýty o tomto případu. Mnoho lidí si myslelo, že Neidorf byl shledán nevinným a Kapor zaplatil jeho advokátům všechny jeho dluhy. Pravdou bylo, že vláda prostě odstoupila od projednávání jeho případu a Neidorfova rodina se těžce zadlužila, aby ho mohla podpořit.

Ale Neidorfův případ poskytl jeden zničující citát: *Policajti tvrdili, že to má cenu osmdesát tisíc dolarů, a přitom to stálo třináct.*

Toto je nejpamětihodnější okolnost Neidorfova procesu. Žádná seriózní zpráva o něm nevynechala tento komentář. Ani policajti si ho nemohli přečíst, aniž by se zarazili a smutně potřásli hlavou. Důvěryhodnost organizátorů zátahu byla v troskách.

Zátah sám ovšem ještě pokračoval. Dvojice Prophetových obvinění, založená na Dokumentu 911, byla při jeho odsouzení tiše vynechána - přestože Prophet se k nim už přiznal. Georgijští federální žalobci důrazně žádali nepodmíněné tresty pro Atlantskou trojku, argumentujíce „nutností vyslat hackerům signál“, který „jejich komunita po celé zemi potřebuje slyšet“.

V odůvodnění jejich rozsudku bylo věnováno mnoho místa různým ohavným věcem, které spáchali různí jiní hackeři (i když členové Atlantské trojky sami se těchto zločinů nedopustili). Bylo v něm také mnoho spekulací o strašlivých věcech, které Atlantská trojka *mohla*

udělat a *byla schopna* udělat (i když ve skutečnosti je neudělali). Argumentace obžaloby byla úspěšná. Členové Atlantské trojky byli posláni do vězení: Urvile a Leftist dostali po čtrnácti měsících, a Prophet, který už byl trestán, 21 měsíců.

Atlantské trojce byly také vyměřeny neuvěřitelné pokuty na „náhradu škody“: každému 233 000 dolarů. Společnost BellSouth tvrdila, že obžalovaní „ukradli“ „asi za 233 000 dolarů“ „důvěrných informací o přístupu k počítačům“ - konkrétně počítačových hesel a připojovacích adres. Fantastická suma, na kterou společnost BellSouth ocenila svá vlastní počítačová hesla a adresy, byla georgijským soudem beze zbytku akceptována. Navíc (jakoby pro zdůraznění její teoretické povahy) nebyla tato částka mezi Atlantskou trojku rozdělena, ale každý z nich musel zaplatit celou.

Pozoruhodnou částí rozsudku nad členy Atlantské trojky byl výslovný zákaz používat počítače jinde než v práci nebo pod dohledem. Zbavit hackery domácích počítačů a modemů dává smysl, jsou-li považováni za „počítačové narkomany“, ale EFF, vystupující v procesu jako zainteresovaná strana, podala stížnost na neústavnost tohoto trestu, který podle ní zbavil Atlantskou trojku svobody spolčování a projevu prostřednictvím elektronických médií.

„Dokonalý hacker“ Terminus byl nakonec v důsledku vytrvalé snahy Chicagské operační skupiny poslán na rok do vězení. Zločinem, k němuž se přiznal, bylo šíření unixovského odchytávače hesel. Jeho cena byla AT&T stanovena na 77 000 dolarů, což vyvolalo zásadní pochybnosti lidí obeznámených s unixovskými programy login.c.

Odsouzení Terminuse a atlantských legionářů soudného dne ale nevyvolalo v EFF žádné pocity porážky či prohry. Naopak, hnutí ochránců občanských práv rychle nabíralo na síle.

Jedním z jeho prvních mocných přívrženců byl senátor Patrick Leahy, demokrat z Vermontu, jež byl navrhovatelem Zákona o soukromí v elektronické komunikaci. Ještě před Neidorfovým procesem Leahy veřejně obhajoval hackery a „svobodu klávesnice“: „Nesmíme nepatřičně omezovat zvídavého třináctiletého chlapce, který, smí-li dnes experimentovat, může zítra vyvinout telekomunikační či počítačovou technologii, jež povede Spojené státy do jednadvacátého století. Představuje naši budoucnost a naši největší nadějí, že Amerika zůstane technologicky vyspělým státem.“

Bylo to pěkné prohlášení, jehož účinnost byla patrně ještě podpořena faktem, že organizátoři zátahu *neměli* žádné senátory mluvící v jejich prospěch. Naopak, jejich utajené akce a taktika, všechna ta „zapečetěná povolení“ a „přísně tajné průběhy vyšetřování“ jim mohly vynést krátký ohňostroj publicity, ale v dlouhodobé ideologické válce byly zásadními nevýhodami. Gail Thackerayové zbyly jen prázdné hrozby. „Někteří z těch lidí, co teď křičí nejhlasitěji, se prostě vytratí,“ předpovídala v časopise *Newsweek* - až všechna fakta vyjdou najevo a policisté budou ospravedlněni.

Ale ne všechna fakta vyšla najevo, a ta, jež vyšla, nebyla příliš lichotivá. A policisté nebyli ospravedlněni. A Gail Thackerayová přišla o místo. Před koncem roku 1991 opustil i William Cook veřejný sektor.

Rok 1990 patřil Zátahu, ale už v roce 1991 se jeho protagonisté dostali do defenzívy a ochránci občanských práv zahájili vítězné tažení. A jejich kauza získávala nové příznivce.

Zvláště zajímavým spojencem byl Mike Godwin z Austinu v Texasu. Godwin byl osobností popsatelnou téměř stejně obtížně jako Barlow; byl šéfredaktorem studentského časopisu Texaské univerzity, prodejcem počítačů, programátorem, a v roce 1990 byl opět ve škole a usiloval o titul advokáta.

Godwin byl také znalcem BBS. V austinské komunitě uživatelů boardů byl velmi dobře znám pod svým pseudonymem „Johnny Mnemonic“, jež přijal podle cyberpunkové sci-fi povídky Williama Gibsona. Godwin byl vášnivým fanouškem cyberpunkové sci-fi. Já, jako austinský rodák blízkého věku a blízkých zájmů, jsem Godwina společensky znal už mnoho let. Když jsme s Williamem Gibsonem psali naši společnou sci-fi novelu *The Difference Engine* („Diferenční motor“), byl Godwin naším technickým poradcem při propojování počítačů Apple, na nichž vznikala, z Austinu do Vancouveru. Gibson a já jsme byli tak potěšeni jeho nezištnou odbornou pomocí, že jsme jednu z postav novely nazvali na jeho počest „Michael Godwin“.

Handle „Mnemonic“ se ke Godwinovi dobře hodila. Jeho erudice a přehled o drobných faktech vzbuzovaly nejen respekt, ale přímo ohromení; jeho vášnivá zvídavost se zdála neukojitelná, a touha debatovat a argumentovat byla patrně hlavní hybnou silou jeho života. Godwin dokonce založil v Austinu svoji vlastní debatní společnost, známou pod ironickým názvem „Klub natvrdlých“. V osobním styku mohl být Godwin zničující - polyhistor s absolutní pamětí, který se od žádné myšlenky nedokázal odtrhnout. Ale médiu boardů Godwinovy logicky vystavěné, jazykově vytříbené a erudované zprávy vyhovovaly; na místních boardech se stal známou osobností.

Mike Godwin byl z největší části zodpovědný za celostátní zveřejnění případu Steva Jacksona. Zabavení Izenbergova vybavení v Austinu se nevěnoval vůbec žádný list. Raziím 1. března u Mentora, Bloodaxe a ve firmě Steve Jackson Games byl věnován krátký článek na první straně listu *Austin American-Statesman*, jež byl ale zmatený a špatně informovaný; povolení k domovní prohlídce byla zapečetěna a Tajná služba USA mlčela. Vypadalo to, že Steve Jackson je odsouzen k zapomnění. Jackson nebyl zatčen; nebyl obviněn ze žádného zločinu; nebyl souzen. V průběhu vyšetřování přišel o nějaké počítače - no a co? Jackson se snažil informovat o skutečném rozsahu svých problémů, ale bezúspěšně; nikdo, kdo by mu mohl pomoci, zjevně nechápal podstatu sporu.

Ale Godwin byl výjimečně, téměř zázračně kvalifikován pro prezentaci Jacksonova případu okolnímu světu. Godwin byl milovník boardů, fanoušek sci-fi, bývalý novinář, prodejce počítačů, budoucí právník a obyvatel Austinu. Ještě neuvěřitelnější shodou náhod se Godwin ve svém posledním ročníku právnické školy specializoval na federální žaloby a vyšetřovací procedury. Jen pro svou satisfakci sestavil Godwin informace o případu pro novináře, shrnující sporné otázky a užitečné kontakty pro reportéry. Jeho snaha v zákulisí (kterou vyvinul v podstatě proto, aby dokázal své tvrzení v debatě na místním boardu) přivedlo příběh opět do *Austin American-Statesmanu* a posléze do *Newsweeku*.

Život Mika Godwina se tím zásadně změnil. Když se zapojil do vznikající debaty o občanských právech na Internetu, bylo všem zúčastněným jasné, že přišel člověk, který, uprostřed všeobecného tápání a zmatku, *opravdu rozumí všemu, o čem mluví*. Nesouvislé prvky Godwinovy diletantské kariéry do sebe náhle zapadly jako části hlavolamu.

Když přišel čas najmout právníka EFF na plný úvazek, byl Godwin prvním kandidátem. Složil texaskou právnickou zkoušku, opustil Austin, přestěhoval se do Cambridge v Massachusetts, stal se placeným, profesionálním ochráncem počítačových občanských práv a brzy z pověření EFF jezdil po celých USA a pořádal dobře přijímané přednášky o těchto otázkách publikům tak rozdílným, jako univerzitní hodnostáři, průmyslníci, fanoušci sci-fi a federální policisté.

V současnosti je Michael Godwin hlavním právním poradcem Nadace elektronického pohraničí.

Jedním z dalších vlivných účastníku kontroverze, kteří se přidali mezi prvními, byla Dorothy Denningová. Profesorka Denningová byla mezi zájemci o počítačový underground výjimečná v tom, že nevstoupila do debaty s žádnými politickými motivy. Byla profesionální kryptografkou, tedy odbornicí na šifry, a specialistkou na počítačovou bezpečnost; její primární zájem o hackery byl *studijní*. Měla bakalářský a magisterský titul z matematiky a doktorský titul z počítačových věd na univerzitě v Purdue. Pracovala pro SRI International, kalifornský výzkumný institut, jež byl i domovem zakladatele počítačové bezpečnosti Donna Parkera, a napsala často citovaný text *Kryptografie a bezpečnost dat*. V roce 1990 pracovala profesorka Denningová pro společnost Digital Equipment Corporation v jejím Systems Reseach Cen-

ter. Její manžel, Peter Denning, byl také odborníkem na počítačovou bezpečnost, pracujícím pro Research Institute for Advanced Computer Science, součást NASA. Sestavil ceněnou knihu *Útok na počítače: průniky, červi a viry*.

Profesorka Denningová se rozhodla kontaktovat digitální underground z víceméně antropologického zájmu. Zjistila, že hackeři, pronikající do počítačů, kteří byli charakterizováni jako nemorální, nezodpovědní a pro společnost nebezpeční, mají ve skutečnosti svou vlastní subkulturu a svá vlastní pravidla. Nebyla to příliš promyšlená pravidla, nicméně lepší než nic. V zásadě byla dvě: nebrat peníze a neničit.

Její suché zprávy o sociologických výzkumech byly velmi důležité při ovlivňování seriózních počítačových profesionálů - těch lidí, kteří jen obraceli oči v sloup, když slyšeli rapsódie o cyberspace Johna Perryho Barlowa.

Pro mladé hackery z digitálního undergroundu bylo setkání s Dorothy Denningovou vpravdě nepředstavitelným zážitkem. Tahle úhledná, usedle oblečená, subtilní osůbka připomínala většině hackerů jejich maminky či tety. Jenže uměla programovat systémy IBM, měla hluboké odborné znalosti o počítačových architekturách a zabezpečování informačních toků a osobní přátele v FBI a NSA.

Dorothy Denningová byla zářným příkladem osobnosti americké matematické intelektuální elity, vskutku inteligentní osoba ze středu akademických počítačových kruhů. A teď se laskavě vyptávala divokých dvacetiletých telefandů na hluboké etické důsledky jejich chování.

Při setkání s touto opravdu milou paní se hackeři většinou slušně posadili a ze všech sil se vynasnažili zjemnit anarchistickou atmosféru na co nejslabší zápach síry. Nicméně hackeři *byli* připraveni vést s Dorothy Denningovou vážnou diskusi o vážných otázkách. Byli ochotni vyslovit nevyslovitelné, obhajovat neobhajitelné a postavit se za své přesvědčení, že informace nemůže být vlastnictvím a že databáze vlád a velkých organizací jsou hrozbou pro práva a soukromí jednotlivců.

Články Denningové objasnily mnohým, že „hackeři“ nejsou prostě vandalové či ďábelská klika psychopatů. Nejsou nepřirozenou hrozbou, jež bude zažehnána, bude-li se ignorovat, či zlikvidována zavřením několika vůdců. Ve skutečnosti jsou hackeři symptomem rostoucího, zásadního sporu o znalosti a moc v informačním věku.

Denningová zdůrazňovala, že postoje hackerů jsou přinejmenším částečně sdíleny nekonvenčními teoretiky managementu, lidmi jako Peter Drucker a Tom Peters. Peter Drucker ve své knize *Nové reality* konstatuje, že „kontrola informací vládou není nadále možná. Informace je nyní vskutku transnacionální. Nemá, podobně jako peníze, žádnou ‚vlast‘.“

A expert na teorii řízení Tom Peters kritizoval důraz velkých společností na copyright a kontrolu informací ve svém bestselleru *Vláda chaosu*: „V americkém průmyslu, jak ve službách, tak ve výrobě, je běžné křečkování informací, zvláště politicky motivovanými strukturami chránícími svoji moc, jež bude nesnesitelným břemenem pro organizace zítřka.“

Dorothy Denningová narušila sociální izolaci digitálního undergroundu. Zúčastnila se Neidorfova procesu, připravena svědčit jako expert obhajoby. Byla šedou eminencí za organizací dvou z nejdůležitějších celostátních setkání ochránců počítačových občanských práv. Dorothy Denningová není fanatikem jakékoli cesty, a snad právě proto dokázala přivést disparátní prvky elektronické komunity k překvapivému a plodnému setkání.

V současnosti je Dorothy Denningová vedoucí katedry počítačových věd na Georgetownské univerzitě ve Washingtonu.

V komunitě ochránců občanských práv bylo mnoho výrazných osobností. Její nejvlivnější postavou byl však bezesporu Mitchell D. Kapor. Jiní lidé mohli mít formální tituly, vládní pozice, více zkušeností se zločinem, nebo se zákonem, nebo s hlubinami počítačové bezpečnosti či ústavní teorie. Ale v roce 1991 Kapor přesáhl všechny takové úzké role. Z Kapora se stal „Mitch.“

Mitch se stal vrchním ad-hokratem ochránců občanských práv. Povstal první, mluvil hlasitě, přímo, se zápalem a hněvivě a vsadil svou vlastní reputaci a vlastní naprosto nezanedbatelný kapitál. V polovině roku 1991 byl Kapor nejslavnějším advokátem své kauzy, *osobně* známým prakticky každému člověku v Americe s nějakým přímým vlivem na otázku občanských práv v cyberspace. Mitch budoval mosty, překonával propasti, měnil paradigmata, vymýšlel metafory, telefonoval a rozdával vizitky s tak dramatickým efektem, že pro každého, kdo chtěl v „hackerské otázce“ něco podniknout, bylo nemožné nepřemýšlet, co si o tom Mitch bude myslet, co řekne a co poradí svým přátelům.

EFF „zesíťovala“ nový status quo. To také bylo od počátku její promyšlenou strategií. Barlow i Kapor nesnášeli byrokracie a vědomě se rozhodli pracovat téměř výhradně s elektronickou pavučinou osobních kontaktů.

Po roce činnosti EFF měli Barlow a Kapor při pohledu zpět všechny důvody ke spokojenosti. EFF založila svůj vlastní internetovský node, eff.org, s dobře zásobeným archivem dokumentů o elektronických občanských právech, otázkách soukromí a akademické svobodě. EFF také publikovala tištěný čtvrtletník *EFFector* a elektronický *EFFector Online* s více než 1200 odběrateli. I na WELLu se EFF rozvíjela.

EFF měla sídlo v Cambridgi v Massachusetts a stálé zaměstnance. Měla řádné členy a veřejnou podporu. Měla také podporu asi třiceti advokátů specializovaných na občanská práva, připravených a ochotných k neplacené práci na obraně ústavy v cyberspace.

Ve Washingtonu a v Massachusetts EFF úspěšně lobbovala za změnu státních a federálních zákonů o počítačových sítích. Zvlášť Kapor se stal žádaným odborným svědkem a členem Výboru pro počítačové vědy a telekomunikace Národní akademie pro vědu a výzkum.

EFF sponzorovala akce jako „Počítače, svoboda a soukromí“ a kulatý stůl organizovaný Computer Professionals for Social Responsibility. Uskutečnila publicistickou kampaň, která, slovy časopisu *EFFector*, „změnila názor veřejnosti na počítačové sítě a zvrátila vlnu ‚hackerské hysterie‘, jež se začala společnosti zmocňovat.“

Pomohla zabránit odsouzení Craiga Neidorfa.

A, nakonec, ale rozhodně nikoli v poslední řadě, podala Nadace elektronického pohraničí federální žalobu jménem Steva Jacksona, společnosti Steve Jackson Games a tří uživatelů boardu Illuminati. Obžalovaní byli, a jsou, Tajná služba USA, William Cook, Tim Foley, Barbara Goldenová a Henry Kluepfel.

Případ, jež je v čase vzniku této knihy ve stadiu předběžných procedur před federálním soudem v Austinu, je civilní žalobou o náhradu škody za údajné porušení prvního a čtvrtého dodatku ústavy Spojených států amerických, stejně jako Zákona o soukromí a Zákona o soukromí v elektronické komunikaci.

EFF prokázala, že má serióznost. Prokázala také, že má zuby.

Na podzim roku 1991 jsem se vydal do Massachusetts k osobnímu rozhovoru s Mitchem Kaporem. Bylo to mé poslední interview pro tuto knihu. [...]

Kapor mě srdečně vítá ve své kanceláři. Je mu něco málo přes čtyřicet, je ženatý a otcem dvou dětí. Má kulatou tvář, vysoké čelo, rovný nos a mírně rozcuchanou hřívu černých vlasů postříkaných šedí. Jeho velké hnědé oči jsou posazené daleko od sebe, zamyšlené, skoro by se dalo říci oduševnělé. Pohrdá kravatami a obvykle nosí pestrobarevné košile s tropickými motivy, ani ne tak křiklavé jako spíš veselé a jen trošku nezvyklé.

Mitch Kapor vyzařuje jen slabý odlesk hackerského ohně. Možná nemá ono jezdecké, černě kožené, kytarové charisma svého wyomingského kolegy Barlowa, ale přesto je v něm cosi, co nutí člověka k zamyšlení. Má vzhled velkoměstského šviháka v anglickém klobouku - zasněného, Longfellowa citujícího hráče pokeru, který prostě *zná* přesnou matematickou šanci své výhry. I mezi svými kolegy z počítačové branže, kteří jsou stěží pověstní pomalým myšlením, působí Kapor silným dojmem inteligentního muže. Mluví rychle, s důraznými gesty a jeho bostonský přízvuk je občas vystřídán ostrými nosovými zvuky jeho mládí na newyorském Long Islandu.

Kapor, jehož Kaporova rodinná nadace uskutečňuje mnoho z jeho filantropické práce, významně podporuje Bostonské počítačové muzeum. Kaporův zájem o historii jeho průmyslu mu přinesl několik pozoruhodných kuriozit, například „byte“ před dveřmi jeho kanceláře. Tento „byte“ - osm digitálních bitů - byl zachráněn z trosek elektronkového počítače pretranzistorového věku. Je to bronzová krabice asi velikosti malé mikrovlnné trouby; má osm zdířek s ručně pájenými obvody, v nichž jsou elektronky velikosti palce. Kdyby vám spadl ze stolu na nohu, snadno by vás mohl zmrzačit, ale ve čtyřicátých letech to byl vrchol počítačové techniky. (Pro uchování první části této knihy by bylo třeba přesně 157 184 těchto pravěkých konstrukcí.)

Je zde i svíjející se pestrobarevný šupinatý drak, vytvořený nějakým osvíceným techno-punkovým umělcem jen z tranzistorů, kondenzátorů a drátů s barevnou plastikovou izolací.

V kanceláři Kapor žádá o okamžik strpení, chápe se myši a chvilku se věnuje domácím pracem na svém osobním Macintoshi IIfx. Kdyby byla jeho přerostlá obrazovka otevřeným oknem, jen trochu pružný člověk by jí dokázal prolézt. U Kaporova lokte je hrnek na kávu, suvenýr z jeho nedávné cesty do východní Evropy, na němž je reprodukována černobílá fotografie s popiskem TURNÉ KAPITALISTICKÝCH TROUBŮ. To je Kapor, Barlow a dva jejich známí kalifornští specialisté na zakládání nových podniků, čtyři rozcuchaní, šklebící se šviháci z poválečné generace v kožených sakách, kovbojských botách a džínách, s batohy, na přistávací dráze nějakého letiště za bývalou železnou oponou. Tváří se, jako kdyby se v životě tak dobře nebavili.

Kapor má nostalgickou náladu. Chvilku se bavíme o jeho mládí - o „matematickém knihomolství“ na střední škole, o sobotách na kursech pro pokročilé studenty pořádaných Kolumbijskou univerzitou, kde poprvé zkoušel programovat. IBM 1620, v roce 1965 a 66. „Hrozně mě to zaujalo,“ říká Kapor. „A pak jsem šel na vysokou a zlákaly mě drogy, sex a rokenrol, jako tehdy každého, kdo neměl v hlavě úplně prázdno!“ Po škole se několik let věnoval progresivnímu rocku jako discjockey v Hartfordu v Connecticutu.

Ptám se, jestli mu někdy nechybí jeho rokenrolové dny - jestli si někdy nepřál vrátit se do rádia.

Rozhodně vrtí hlavou. „Přestal jsem uvažovat o tom, že bych byl znova DJ, den po Altamontu.“

V roce 1974 se Kapor přestěhoval do Bostonu a začal pracovat jako programátor na sálových počítačích v COBOLu. Vůbec ho to nebavilo. Dal výpověď a stal se učitelem transcedentální meditace. (Kaporův dlouholetý zájem o východní mystiku dal světu značku „Lotus“ („Lotos“)).

V roce 1976 odjel Kapor do Švýcarska, kde si sdružení Transcedentální meditace pronajalo obrovský viktoriánský hotel v St-Moritz. Byla to výhradně mužská skupina - sto dvacet lidí - rozhodnutá dosáhnout osvícení nebo krachu. Kapor se snažil o transcedenci ze všech svých sil. „Fanatičnost v organizaci“ ho začínala odpuzovat. „Učili lidi levitovat,“ říká, dívaje se na podlahu. O oktávu hlubším hlasem rozhodně dodává: „*A nelevitují*.“

Kapor si vybral krach. Vrátil se do Ameriky a získal diplom v psychologickém poradenství. Chvilku pracoval v nemocnici, ale ani tam nedokázal vydržet. „Povídalo se o mně,“ říká, „že jsem hrozně chytrý kluk s ohromnými možnostmi, který se nemůže najít. Skoro třicet. Tak nějak ztracený.“

Kapor byl nezaměstnaný, když si koupil svůj první osobní počítač - Apple II. Prodal stereo, aby na něj měl, a jel ho koupit do státu New Hampshire, aby nemusel platit daň.

„Den potom, co jsem si ho koupil,“ říká mi Kapor, „jsem postával v jednom počítačovém obchodě a viděl nějakého člověka, asi čtyřicátníka, dobře oblečeného, a odposlechnul jsem jeho rozhovor s prodavačem. O počítačích nevěděl vůbec nic. Já dokázal programovat v BASICu. Naučil jsem se to. Tak jsem šel k němu a prostě ho přesvědčil, aby mě přijal jako konzultanta.“ Okamžik mlčí. „Nevím, kde jsem k tomu sebral odvahu. Bylo to nenormální. Prostě jsem řekl ‚Myslím, že vám mohu pomoci. Poslouchal jsem vás, potřebujete to a to a já to pro vás mohu udělat.‘ A on mě přijal! To byl můj první klient. Stal jsem se počítačovým konzultantem den potom, co jsem si koupil Apple II.“

Kapor našel svou životní dráhu. Získal pro svou konzultantskou živnost další klienty a založil organizaci uživatelů počítačů Apple.

Kaporův přítel Erik Rosenfeld, student posledního ročníku MITu, měl problém. Dělal diplomovou práci o jisté komplikované metodě finanční statistiky, ale nedokázal se dostat k vytíženým sálovým počítačům MITu. (Zde je možno poznamenat, že kdyby se pan Rosenfeld zachoval nepočestně a do počítačů MITu se vloupal, Kapor vůbec nemusel vyvinout Lotus 1-2-3 a vývoj obchodu s osobními počítači se mohl zpozdit o celá léta!) Ale Erik Rosenfeld měl Apple II a napadlo ho, že problém by se dal řešit v menším měřítku. Kapor mu napsal, jako přátelskou službu, program, který to zvládl.

Pak ty dva z čista jasna napadlo, že onen program by se dal *prodat*. Distribuovali ho sami, v plastických obalech, kus asi za sto dolarů, na objednávku poštou. „Garážový obchod bezvýznamného konzultanta,“ říká Kapor hrdě. „Vážně jsem začínal takhle.“

Rosenfeld, jež se později stal velmi významným mužem na Wall Street, přesvědčil Kapora, aby se zapsal na studium ekonomie na MITu a zkusil získat MBA. Kapor tam vydržel sedm měsíců, ale titulu nedosáhl. Naučil se ledacos užitečného - hlavně pravidla účetnictví - a, podle svých vlastních slov, „mluvit jako ekonom“. Pak toho nechal a přestěhoval se do Silicon Valley.

Vývojáři programu VisiCalc, prvního finančního programu pro Apple, projevili o Mitche Kapora zájem. Kapor pro ně šest měsíců pilně pracoval, nasytil se Kalifornie a vrátil se do Bostonu, kde měli lepší knihkupectví. Vývojáři VisiCalcu udělali kritickou chybu, když se spojili s „profesionálním managementem“. „To jim přistřihlo křídla,“ říká Kapor.

„Jo, o VisiCalcu není poslední dobou moc slyšet,“ uvažuji.

Kapor vypadá překvapeně. „No, Lotus... my jsme je koupili.“

„Vy jste je *koupili*?“

„Jo.“

„Jako Bell koupil Western Union?“

Kapor se zakření. „Jo, jo. To je přesně ono!“

Mitch Kapor nebyl svrchovaným pánem počítačového průmyslu ani svého osudu. Nejlukrativnějším softwarem na počátku 80. let byly *počítačové hry* - zdálo se, že Atari dobude domov každého kluka v Americe. Kapor se dal na finanční programy prostě proto, že pro počítačové hry mu chyběl cit. Ale byl výjimečně rychlý, otevřený novým myšlenkám a důvěřoval svým instinktům. A jeho instinkty se osvědčily. Vybral si dobré spolupracovníky - talentovaného programátora Jonathana Sachse (spoluautora Lotusu 1-2-3), finančního kouzelníka Erika Rosenfelda, ostříleného wallstreetského analytika a specialistu na zakládání nových podniků Bena Rosena. Kapor se stal zakladatelem a ředitelem společnosti Lotus, jednoho z nejslavnějších a nejúspěšnějších podniků druhé poloviny dvacátého století.

Nyní je neobyčejně bohatým mužem. Ptám se ho, zda ví, kolik peněz ve skutečnosti má.

„Ano,“ říká. „Přesně na procento nebo dvě.“

Kolik tedy?

Potřásá hlavou. „Hodně. Hodně. To není nic, o čem bych mluvil. Peníze a postavení jsou věci, které mají příliš velký vliv.“

Nenaléhám. Je to od věci. Nezdvořile by se dalo předpokládat, že Kapor má přinejmenším čtyřicet milionů - to vydělal ten rok, kdy opustil Lotus. Lidé, kteří by to měli vědět, tvrdí, že Kapor má asi sto padesát milionů, v závislosti na běžné ceně jeho akcií. Kdyby se Kapor držel Lotusu, jako se jeho kolega, přítel a rival Bill Gates držel své společnosti Microsoft, měl by asi stejné jmění, jaké má Gates - okolo tří miliard,

plus mínus pár set milionů. Mitch Kapor má tolik peněz, kolik chce. Peníze pro něj ztratily všechno kouzlo, které kdy mohly mít - a nejspíš ho ostatně nikdy moc neměly. Když se společnost Lotus stala příliš sešněrovanou, příliš byrokratickou, příliš vzdálenou od toho, co ho těší, Kapor ji opustil. Prostě s ní přerušil veškeré styky. Každý nad tím žasl - kromě těch, kteří ho dobře znali.

Kapor nemusel přetěžovat své finanční zdroje, aby mohl transformovat politiku v cyberspace. První roční rozpočet EFF byl kolem čtvrt milionu dolarů. Kapor ji platí ze svého kapesného.

Kapor mi zdůrazňuje, že on sám se necítí být ochráncem občanských práv v pravém smyslu slova. Poslední dobou trávil s opravdovými ochránci občanských práv mnoho času a jejich ‚political correctness' ho dráždí. Zdá se mu, že věnují neúměrně velkou energii právnímu hnidopišství a na vlastní uplatňování občanských práv v reálném světě jim už nezbývá.

Kapor je manažer. Jako všichni hackeři dává přednost přímému, osobnímu a bezprostřednímu přístupu. „Je velká věc, že EFF má node na Internetu. Jsme vydavatelé. Distribuujeme informace." Mezi informacemi dostupnými na eff.org jsou i stará čísla *Phracku*. V EFF se o tom rozvinula vnitřní debata, nicméně nakonec se rozhodli, že je zveřejní. Mohou zpřístupňovat i další undergroundové publikace, ale, jak říká, „v každém případě budeme mít Donna Parkera a cokoli, co chce šířit Gail Thackerayová. Dáme to do veřejné knihovny, ta má nejrůznější využití. Vyvíjí se tak, aby umožnila lidem vytvořit si svůj vlastní názor." Zašklebí se. „Všechny redakční články se pokusíme označit."

Kapor je odhodlán ve veřejném zájmu překonat technickou složitost Internetu. „Problém je, že když máte dneska node na Síti, musíte k němu přivázat technického specialistu. My máme na krocení té potvory Chrise Davise. Sami bysme to nikdy nezvládli!"

Odmlčí se. „Takže jeden směr, ve kterém se technologie musí vyvíjet, jsou mnohem standardizovanější stavební prvky, které budou vyhovovat i netechnikům. Je to ten samý posun jako od minipočítačů k osobním počítačům. Představuju si budoucnost, kdy každý člověk může mít node na Síti. Každý člověk může být vydavatel. To je lepší než média, která máme teď. A je to možné. Pracujeme na tom."

Kapor je nyní ve svém živlu, mluví plynně a své téma dokonale ovládá. „Když řeknete hardwarovému hackerovi na Internetu, že každý by měl mít na Síti svůj vlastní node," pokračuje, „úplně automaticky vám odpoví, že ‚IP není rozšiřitelný'!" (IP je „interface protocol" neboli formát komunikace Internetu. Jeho současná podoba nemá schopnost nekonečného růstu; počet možných adres je omezený a nelze ho zvětšit.) „Odpověď," tvrdí Kapor, „je *zdokonalte protokol*! Dejte dohromady chytré lidi a vymyslete řešení. Přidat ID? Přidat nový protokol? Neříkejte jen, že ‚to nejde'."

Dávat dohromady chytré lidi a vymýšlet řešení je činnost, ve které Kapor jasně vyniká. Oponuji mu, že lidé na Internetu jsou dost pyšní na svůj elitní technický status a pro demokratizaci Sítě se zjevně nehodlají přetrhnout.

Kapor souhlasí a projevuje opovržení. „Říkám jim, že je to snobství puritánů na *Mayflower*, dívajících se svrchu na lidi, kteří přijeli do Ameriky *až druhou lodí*! Jen proto, že se tam dostali rok, nebo pět let, nebo deset let před ostatními, nejsou majiteli cyberspace! Jakým právem?"

Podotýkám, že i spojaři mají elektronickou síť a své specializované vědomosti si žárlivě střeží.

Kapor opáčí, že telefony a Internet jsou úplně jiné světy. „Internet je otevřený systém, všechno je publikováno, o všem se diskutuje, v podstatě s každým, kdo se chce přidat. Z větší části je tenhle systém tak exkluzívní a elitářský jen proto, že je tak těžce zvládnutelný. Udělejme ho přístupnější."

Na druhé straně, uznává a rychle mění důraz, i ti takzvaní elitáři mají kus pravdy. „Než přijdou noví lidé, začnou předkládat návrhy a kritizovat Síť jako ‚úplně zpackanou'... Měli by investovat nějaký čas do pochopení její kultury, podívat se na ni zevnitř. Má svou historii, která by se neměla ignorovat. V tomhle jsem konzervativec."

Internet je Kaporovým paradigmatem pro budoucnost telekomunikací. Je decentralizovaný, neřízený, téměř anarchistický. Nejsou v něm žádní šéfové, žádná hierarchická struktura, žádná tajná data. Má-li každý node obecné standardní rozhraní, je centrální autorita sítě prostě nadbytečná.

Znamená to snad, ptám se, že AT&T jako instituce je odsouzena k zániku?

Taková vyhlídka Kapora nijak nezaráží. „Mají velkou výhodu, v současné době, že jim patří všechny dráty. Ale probíhají dvě změny. Každý, kdo má příležitost, pokládá vlastní kabely. Železnice, třeba Southern Pacific, a podobně - existuje spousta ‚temného vlákna'." („Temné vlákno" je optický kabel, jehož ohromná kapacita natolik převyšuje současné požadavky, že většina vláken dosud vůbec nepřenáší signály - jsou „temná", čekají na použití v budoucnosti.)

„A druhá změna je, že místní přenosy začínají být bezdrátové. Každý od Bellcore přes majitele kabelových televizí po AT&T chce poskytovat to, čemu říkají ‚osobní komunikační systémy'. V místních hovorech může být konkurence - spousta lidí, v různých lokalitách, staví antény. A další lidi pokládají temné vlákno. Takže co bude s telefonními společnostmi? Jsou pod obrovským tlakem, z obou stran.

Čím víc se na to koukám, tím víc věřím, že v postindustriálním, digitálním světě je princip regulovaných monopolů špatný. Až to pro lidi bude minulost, řeknou, že v 19. a 20. století byla myšlenka komunálních sítí rozumným kompromisem. V zemi musely být jen jedny dráty. Jiné možnosti byly ekonomicky neefektivní. A to znamenalo, že je bude řídit jedna organizace. Ale teď, když jsou části sítě bezdrátové, budou spojení realizována přes obecná rozhraní, ne přes dráty. Chci říct, že *na nejnižší úrovni* budou dráty - ale dráty jsou prostě surovina. Jako optické vlákno, jako frekvence rádia. Už *není třeba* komunální síť."

Vodovod? Rozvod plynu?

Ty jsou samozřejmě pořád nezbytné, souhlasí. „Ale když hýbete s informací, ne s hmotnými látkami, můžete se řídit jinými pravidly. Teď je právě formulujeme! Doufejme, že je možné vytvořit mnohem decentralizovanější systém a trh s větší konkurencí.

Úkolem vlády bude zajistit, aby nikdo nepodváděl. Vytyčit příslovečnou ‚hrací plochu'. Politiku, která zabrání monopolizaci. Výsledkem by měly být lepší služby, nižší ceny, větší výběr a rozvoj samosprávy." Usmívá se. „Jsem velkým příznivcem samosprávy."

Kapor má vizi. Je to velmi neotřelá vize a on i jeho kolegové ji propracovávají detailně a s velkou energií. Já, jako temný, cynický a morbidní cyberpunker, uvažuji i o pochmurnějších implikacích „decentralizovaných, nehierarchických a samospráv- ných" sítí.

Poznamenávám, že někteří teoretikové soudí, že elektronická komunikace - faxy, telefony, malé kopírky - hrála důležitou úlohu v nahlodávání moci centralizovaného komunismu a byla jednou z příčin kolapsu Varšavské smlouvy.

Socialismus je dokonale zdiskreditován, říká Kapor, který se právě vrátil z Východní Evropy. Představa, že to udělaly faxy, samy o sobě, to je prostě přání otcem myšlenky.

Napadlo ho, že elektronické sítě mohou rozežrat průmyslovou a politickou infrastrukturu Ameriky do té míry, že se stane neovladatelnou a nefunkční - a staré pořádky se prostě zhroutí, jako ve Východní Evropě?

„Ne," říká Kapor přesvědčeně. „Podle mého je to extrémně nepravděpodobné. Taky proto, že před deseti patnácti lety jsem choval podobné naděje o osobních počítačích - a velice jsem se zklamal." Zašklebí se, pak se jeho oči zúží. „*Nemám rád* technoutopie. Kdykoli nějakou vidím, uteču, nebo ji zkusím zlikvidovat."

Dochází mi, že Mitch Kapor se nepokouší změnit svět v zájmu demokracie. Rozhodně se ho nepokouší změnit v zájmu anarchistů a sníků, a ze všeho nejméně v zájmu lidí pronikajících do počítačů a elektronických šidičů. O co se opravdu snaží je změnit svět v zájmu budoucích Mitchů Kaporů. Svět decentralizovaných, snadno získatelných nodů s okamžitým a globálním rozsahem pro ty nejlepší a nejchytřejší

by byl dokonalým prostředím pro „garážové“ kapitalisty s minimálním rozpočtem, pro podnikatele, jakým byl ve svých začátcích i Mitch Kapor.

Kapor je velice inteligentní muž. Má vzácnou kombinaci vizionářského zápalu se smyslem pro realitu. Členové Rady Nadace elektronického pohraničí - John Barlow, Jerry Berman z American Civil Liberties Union, Stewart Brand, John Gilmore, Steve Wozniak a Esther Dysonová, první dáma amerického počítačového průmyslu - sdílejí jeho schopnosti, jeho vizi a jeho talent pro vytváření organizačních struktur v elektronických sítích. Jsou to děti 60. let, zocelení tehdejšími konflikty a odměnění bohatstvím a vlivem. Jedni z nejlepších a nejchytřejších představitelů elektronické komunity. Ale dokáží se prosadit ve skutečném světě? Nebo jenom sní? Je jich tak málo. A tak mnoho stojí proti nim. [...]

„Počítače, svoboda a soukromí.“ Čtyři stovky lidí ze všech představitelných složek americké elektronické komunity. Jako autor sci-fi jsem se svého času zúčastnil několika *dost* podivných srazů, ale před tímhle prostě blednou. I samotný „Cyberthon“, organizovaný Point Foundation a nazývaný „Woodstockem cyberspace“, kde se sanfranciská psychedelie střetla se vznikajícím světem virtuální reality, připomíná ve srovnání s touto ohromující akcí schůzi sokolského spolku.

„Elektronická komunita“ dosáhla zenitu. Byli přítomni prakticky všichni hrdinové této knihy. Ochránci občanských práv. Počítačoví policajti. Digitální underground. Dokonce i pár nenápadných zaměstnanců telecomu. Jsou rozdávány barevné nálepky na jmenovky. Svoboda slova. Zákon. Počítačová bezpečnost. Soukromí. Žurnalisté. Právníci. Lektoři. Knihovníci. Programátoři. Stylově černé nálepky pro hackery a telefandy. Téměř každý účastník nosí osm nebo devět nálepek, specializuje se na šest nebo sedm odborností.

Je to komunita. Možná trochu jako Libanon, ale stejně - digitální společenství. Lidé, kteří spolu celý rok vedli tiskové polemiky a chovali nejtemnější podezření o motivech a etice svých protivníků, sedí nyní u jednoho stolu. Bylo mnoho důvodů k předpovědi, že se konference „Počítače, svoboda a soukromí“ zvrhne v ošklivou konfrontaci, ale navzdory tomu na ní vládla překvapivě srdečná atmosféra, jen s malými erupcemi kryptických nesmyslů z extremistického okraje komunity. Konference připomínala svatební obřad, v němž mladý pár, hysterická novomanželka a šarlatánský novomanžel, vstupují do svazku jasně odsouzeného ke katastrofě.

Oběma rodinám - a ostatně i sousedům a náhodným hostům - je jasné, že tento vztah nemůže vydržet, ale novomanželé se jednou mají rádi a nehodlají vyčkávat. Prostě si nemohou pomoci. Bude létat nádobí, řev z jejich společné domácnosti bude budit celý blok, rozvod se vznáší nad hlavou jako sup nad Kalahari, ale teď mají svatbu a budou mít děti. Tragédie končí smrtí, komedie svatbou. Zátah na hackery končí svatbou. I děti budou.

Průběh konference je od počátku netypický. Mezi přítomnými je i John Perry Barlow, rančer cyberspace. Jeho barevná fotografie v magazínu *New York Times*, na které stojí v chmurné krajině zasněženého Wyomingu, v dlouhém černém kabátě, tmavém klobouku, s Macintoshem SE30 postaveným na ohradě a hrozivou hraničářskou puškou přes rameno, je tím nejpůsobivějším fotografickým obrazem Zátahu na hackery. Je čestným hostem konference - spolu s Gail Thackerayovou z FCIC! Co proboha čekají, že tihle hosté společně předvedou? Valčík?

Barlow se ujímá slova jako první. Kupodivu chraptí - dlouhá šňůra projevů ho vyčerpala. Jeho řeč je krátká. Mluví srdečně, vyzývá k usmíření a má bouřlivý aplaus.

Pak vystupuje na pódium Gail Thackerayová. Je viditelně nervózní. Poslední dobou strávila hodně času na WELLu. Četla Barlowovy zprávy. Následovat Barlowa je výzva. Na počest slavného textaře Grateful Dead, oznamuje vysokým napjatým hlasem, přečte - *báseň*. Báseň, kterou sama složila.

Je to hrozná báseň, rýmovačka v nejhorší anglosaské tradici, nicméně opravdová báseň. Jmenuje se *Balada elektronického pohraničí* a je o Zátahu na hackery a fantastické nepravděpodobnosti konference „Počítače, svoboda a soukromí“. Je plná vtipů pro zasvěcené. Asi dva tucty policajtů v obecenstvu, sedící pohromadě v nervózním hloučku, doslova šílí. Gailina báseň je ta nejsrandovnější věc, jakou kdy slyšeli. Hackeři a aktivisté, kteří si Thackerayovou představovali zhruba jako Ilsu-vlčici z SS, zírají s ústy dokořán. Ani v nejdivočejším výtrysku jejich fantazie je nenapadlo, že je schopna udělat něco tak spontánního. Viditelně „restartují“ své mysli. Proboha! Ta ženská je hackerský originál! *Je zrovna jako my!* To úplně mění situaci!

Al Bayse, počítačový technik FBI, se jako jediný policajt zúčastnil kulatého stolu Computer Professionals for Social Responsibility, kam ho přes jeho protesty zatáhla Dorothy Denningová. Tam byl ostražitý a málomluvný; „lev předhozený křesťanům“.

Na konferenci „Počítače, svoboda a soukromí“, se skupinou kolegů v zádech, je Bayse náhle řečník, dokonce bavič. Popisuje „NCIC 2000“, gigantický digitální katalog kriminalistických záznamů založený FBI, tónem George Orwella zkříženého s Georgem Gobelem. Nenápadně udělá matematický vtip o statistické analýze. Aspoň třetina posluchačů se rozchechtá.

„Při mém posledním projevu se tomu nesmáli,“ poznamenává Bayse. Tehdy mluvil k policajtům - *normálním* policajtům, ne od počítačů. Dá se předpokládat, že to bylo platné a užitečné setkání, ale nic jako *tohle*. *Nikdy* nebylo nic jako tohle. Bez jakéhokoli ponoukání, bez přípravy, začínají lidé v obecenstvu klást otázky. Vlasatci, pochybné zjevy, matematikové. Bayse, odpovídající zdvořile, ochotně a podrobně, jako by se vznášel. Sálem se šíří atmosféra sureálna. Advokátka za mnou se potí a kolem jejích paží se šíří horký závan překvapivě silného pižmového parfému.

Lidé se baví jako o pouti. Jsou zaujati až k fascinaci, mají rozšířené a tmavé zřítelnice, jako by byli eroticky vzrušení. V sálech, kolem baru, na schodištích se formují nepravděpodobné kroužky: policajti s hackery, aktivisté s FBI, Tajná služba USA s telefandy.

Gail Thackerayová vypadá skvěle v bílém vlněném svetru s malým logem Tajné služby USA. „Potkala jsem u telefonů Phiber Optika - když viděl můj svetr, změnil se v solný sloup!“ šklebí se.

Phiber podrobně rozebírá svůj případ s policistou, který ho zatýkal, Donem Delaneym z newyorské policie. Po hodinovém rozhovoru ti dva vypadají, že se co nevidět dají do sborového zpěvu. Phiber se konečně odhodlává k vyslovení své největší stížnosti. Nejde ani tak o zatčení. Ale to *obvinění*. Kradení služeb z čísel, na která se dá volat zadarmo. Já jsem *programátor*, prohlašuje Phiber. Takovéhle ubohé obvinění mi zkazí reputaci. Bylo by fajn být přistižen při něčem velkém, jako pronikání do důležitého počítače. Možná nějaký zločin, který byl sotva vymyšlen. Ale mizerná krádež služeb. Fuj.

Delaney se tváří lítostivě. Měl k dispozici bohatý výběr trestných činů, ze kterých mohl Phiber Optika obžalovat. Stejně se přizná. Je to poprvé, to se vždycky přiznávají. Mohl ho obvinit celkem z čehokoli, a výsledek by byl nakonec stejný. Vypadá to, že Delaneyho opravdu mrzí, že Phiberovi tuto nevinnou radost nedopřál. Teď už je pozdě. Phiber už se přiznal. Loňský sníh. Co se dá dělat?

Delaney rozumí hackerské mentalitě. Na tiskové konferenci, pořádané poté, co dopadl několik nezletilých členů Masters of Deception, se ho nějaký reportér zeptal: „Nazval byste tyto lidi *génii*?“ Delaneyho chladná odpověď byla dokonalá: „Ne, nazval bych je *obviněnými*.“ Delaney chytne kluka, který získává přístupové kódy automatickým vytáčením čísel. Řekne tisku, že moderní NYNEX umí tohle zjistit naprosto bez problémů a že kluk musí být *trouba*, když dělá něco, na co se tak snadno přijde. Opět do černého - hackerům nevadí, když mají u veřejnosti pověst Čingischána, ale jestli jim něco nedělá dobře, tak jsou-li nazýváni *hlupáky*.

Příště už to pro Phibera nebude taková legrace. Po opakovaném zločinu půjde do vězení. Hackeři překračují zákon. Nejsou géniové a budou obvinění. A přesto, uvažuje Delaney nad skleničkou v hotelovém baru, zjistil, že se k nim nemůže chovat jako k obyčejným zločincům. Delaney zná zločince. Ale tihle kluci jsou jiní - nemají zločineckou vizáž, ten pravý odér, nejsou prostě tak *zlí*.

Delaney zažil dost. Byl ve Vietnamu. Stříleli po něm, a on střílel do nich. Je z oddělení vražd v New Yorku. Vypadá jako chlap, který nejen viděl spoustu špíny, ale žil a pracoval v ulicích, ve kterých se hromadila a kvasila po celá léta. Ví, jak to na světě chodí.

Poslouchá, jak Steve Jackson vypráví svůj příběh. Zasněný tvůrce her dostal špatný list. Hrál s ním, jak nejlépe dokázal. Pod jeho vizáží introvertního fanouška sci-fi je jádro ze železa. Jeho přátelé říkají, že Steve Jackson věří na pravidla, na fair play. Nikdy se nezpronevěří svým principům, nikdy se nevzdá. „Steve“, říká mu Delaney, „ať se proti tobě pustil kdokoli, troufli si dost. Máš pravdu!“ Užaslý Jackson se zarazí a doslova zardí potěšením.

Neidorf během posledního roku pořádně vyrostl. Učí se rychle, to mu nemůžete upřít. V obleku, který mu vybrala jeho maminka, módní ředitelka celostátní sítě obchodů s oděvy, předčí missourský student a počítačový fanoušek svou elegancí všechny přítomné s výjimkou těch nejmondénnějších advokátů z východního pobřeží. Železná tlama vězení zaklapla bez něho a nyní mu mává právnická škola. Vypadá jako budoucí kongresman.

Žádný hacker, pan Neidorf. Informatika ho nezajímá. Proč by měla? Nechce psát až do smrti programy v C, a kromě toho viděl, kam směřuje proud. Pro svět informatiky byl on a *Phrack* jen kuriozitou. Ale pro svět zákona... Naučil se, jak to na světě chodí. Svůj notebook s novinovými výstřižky nosí všude s sebou.

Phiber Optik si dělá z Neidorfa legraci a říká mu, že je prérijní krtek, když věří, že Acid Phreak jede acid a poslouchá acid rock. Houby! Acid nikdy nezkoušel acid. Acid poslouchá *acid house*. Ježíšikriste. Ta představa, zkoušet LSD. Naši *rodiče* zkoušeli LSD, ty komiku.

Thackerayová náhle obrací celou svoji zářivou pozornost na Craiga Neidorfa a zahajuje odhodlaný půlhodinový pokus *získat ho na svoji stranu*. Johanka z Arku počítačového zločinu *doporučuje kariéru Knight Lightningovi*! „Vaše zkušenosti by byly velmi užitečné - opravdový přínos,“ říká se svou nezaměnitelnou srdečností. Neidorf je fascinován. Naslouchá s nelíčeným zájmem. Kývá a říká ano, madam. Ano, Craigu, i ty můžeš zapomenout na peníze a vstoupit do zářivého a příšerně špatně placeného světa ELEKTRONICKÉ POLICIE! Můžeš dostávat své bývalé přátele do vězení - aj...

Nemůžete věčně bojovat přes drát. Nemůžete ztřískat protivníka do bezvědomí srolovanými novinovými výstřižky. Dříve nebo později musí dojít k osobní konfrontaci. Nicméně už samo uskutečnění tohoto shromáždění zásadně změnilo celou situaci. John Quarterman, autor knihy *The Matrix*, vysvětluje na své panelové diskusi Internet. Je to největší informační síť na světě, překotně roste, ale její velikost se nedá změřit, protože Internet nelze zastavit. Nelze ho zastavit, protože na celém světě není nikdo, kdo by k tomu měl oprávnění. Mění se, to ano, roste, prostupuje postindustriálním, postmoderním světem a vyvolává k životu nové komunity, a to všechno dělá sám od sebe.

Phiber je jedinečný. Velmi fin de siÎcle. Barlow říká, že vypadá jako dandy z edwardiánské Anglie, a má pravdu. Vyholený krk, vlasy po stranách lebky po rapersku sestříhané, rozcuchaná černá hříva nad nimi vypadá napomádovaná, zůstává vzhůru do čtyř ráno, vynechává všechny přednášky a pak se potlouká kolem veřejných telefonních automatů se svým akustickým propojovačem a drze PRONIKÁ DO SYSTÉMŮ ROVNOU UPROSTŘED NEJDRSNĚJŠÍCH POČÍTAČOVÝCH POLICAJTŮ V AMERICE, nebo to aspoň *předstírá*...

Není jako Frank Drake. Drake, který napsal Dorothy Denningové, požádal ji o interview pro svůj laciný cyberpunkový fanzin a začal se jí vyptávat na její etiku. Vytáčela se... Drake, vysoký jako strašák, s blond čírem, rozpadajícími se teniskami a černou koženou bundou s červeným nápisem ILLUMINATI má nezaměnitelný vzhled bohémského intelektuála. Drake je ten typ, co čte anglické časopisy o průmyslovém designu a oceňuje Williama Gibsona za literární kvality jeho prózy. I kdyby až do smrti nesáhl na telefon či klávesnici, pořád by mu zůstal jeho kroužek v nose, zašedlé fanziny z fotokopírky a pásky s industriální hudbou. Radikální punker s počítačovým vydavatelstvím na stole a adresou na Internetu. Vedle Draka vypadá malý Phiber jako by vypučel z telefonní linky. Zrozen pro telefon.

Dorothy Denningová se náhle obrací na Phibera. Ti dva jsou přibližně stejně vysocí a stavění. Modré oči Denningové se blýskají za skly jejích brýlí. „Proč jste řekl, že jsem ‚graciézní‘“? ptá se graciézně.

Je to dokonale přiléhavý popis, ale Phiber je zmaten... „No, já, víte...“

„Já si také myslím, že jste graciézní,“ spěchám mu na pomoc s novinářskými tlachy... Je úhledná a živá a přitom má v sobě tajemství, něco jako Panna Marie za olovnatým sklem; kdyby byla šest palců vysoká, hodila by se Dorothy Denningová skvěle mezi porcelánové panenky... Kryptografka... Kryptografička... Tak něco... Je neuvěřitelné, jak podobný je Peter Denning své manželce, dokázali byste ho poznat mezi tisíci muži jako polovičku Dorothy Denningové. Oblečený ve sportovních kalhotách na míru, zářivě čistém chlupatém svetru v univerzitních barvách a s úhlednou akademickou kravatou... Zdá se, že tento elegantní, vybraně zdvořilý, dokonale civilizovaný pár přišel z nějakého čistšího a jemnějšího paralelního vesmíru, v němž je smyslem existence lidstva psát hádankářský sloupek v časopise Scientific American. Proč se tato dáma stýká s tak pochybnými zjevy?

Protože k tomu nastal čas. Protože v tom, co dělá, je nejlepší ze všech.

Je tu i Donn Parker, „Velký plešatý orel počítačového zločinu“... Vizionářský pionýr, vysoký, s holou hlavou a obrovskýma lincolnovskýma rukama, pluje mezi obyčejnými smrtelníky jako ledoborec... Jeho oči jsou upřeny do budoucnosti s nehybností bronzové sochy... Nakonec, říká svým posluchačům, budou všechny zločiny bílých límečků počítačové, protože všechny obchody půjdou přes počítač. „Počítačový zločin“ jako speciální kategorie zanikne.

Do té doby budou vzkvétat a upadat a mizet krátkodeché senzace... Parkerův velitelský, zvučný hlas zní jako hlas Sfingy, vše je nazíráno z jakési neskutečné výspy radikální historické abstrakce... Vynořily se a zase zmizely, bubliny vzrušení ve světě počítačů... Třeba skandál s rádiovým vyzařováním... KGB, MI5, CIA to dělají každý den, je to snadné, ale nikdo jiný to nikdy nezkoušel... Salámová metoda zpronevěry, v podstatě mýtus... Říká jim „krimoidy“. Současným šampiónem krimoidů jsou počítačové viry, mnohem méně nebezpečné, než si většina lidí myslí, ale už přestávají být novinkou a v současnosti se čeká na další krimoid, média zjevně hladoví po něčem drastičtějším... Velký muž nám předkládá několik svých spekulací o možných kandidátech... Počítačové padělatelství! To je něco... Počítače ukradené jen kvůli datům, které v nich jsou - únosy dat! To se před nedávnem stalo v Anglii, možná se to rozšíří... Falešné uzly Internetu!

Parker vkládá obrázky do svého projektoru, jako by sloužil mši... Má na sobě šedivý dvouřadový oblek, světlemodrou košili a velice usedlou kravatu s jemným hnědo-modrým vzorkem... Pronáší aforismy s pomalým, těžkým důrazem... Neexistuje nic takového jako spolehlivě bezpečný počítač, když proti vám stojí dostatečně mocný protivník... Odstrašování je společensky nejužitečnější aspekt bezpečnosti... Hlavní slabinou všech informačních systémů jsou lidé... Celé základy počítačové bezpečnosti musí být posunuty směrem vzhůru... Nikdy neporušujte svou bezpečnost veřejným popisem vašich bezpečnostních opatření...

Lidé v publiku se začínají nespokojeně vrtět, ale přece jen - na klasické čistotě filozofie tohoto člověka je něco, co vzbuzuje respekt... Parker zní tak trochu jako jediný racionální člověk v záchranném člunu. Ten, který umí nevyvratitelně odvodit, z hlubokých morálních principů, že tady Harvey, se zlomenou nohou a pochybnou minulostí, musí být, ehm... tedy, pan Harvey je v té nejlepší pozici k vykonání nezbytné oběti pro bezpečnost a samo přežití zbytku posádky tohoto člunu... Počítačová bezpečnost, říká Parker smutně, je ošklivé téma, a všichni si přejeme, abychom ji nepotřebovali... Odborník na bezpečnost, ozbrojený metodou a logikou, musí přemýšlet - představte si to - o všem, co by mohl udělat jeho protivník, dříve, než to udělá. Jako by temná zločinecká mysl byla rozsáhlým podprogramem v zářivé lebce Donna Parkera. Je Sherlock Holmes, jehož Moriarty dosud v podstatě neexistuje a tedy musí být dokonale simulován.

Konference „Počítače, svoboda a soukromí“ je šťastná událost, šťastný konec. Má atmosféru svatby a hvězdné účastníky, kteří vědí, že

tuto noc se jejich svět mění navždy, a jsou hrdí, že jsou u toho, že o tom mluví, přemýšlejí a pomáhají tomu.

Ale jak se stmívá a dav se shromažďuje pod lustry, se skleničkami vína a zákusky, objevuje se elegická nálada. Něco tu končí, mizí navždy, a chvilku trvá pojmenovat to.

Je konec amatérů.