Létezik-e „hackeretika” a 90-es években?

Steven Mizrach

Az alábbiakban közölt szövegelemzések célja, hogy a komputerundergroundban született írások vizsgálata segítségével kimutassa azokban *a)* szerzőjük hackeretikára vonatkozó tudásának létét vagy hiányát; *b)* ennek az etikának a fejlődését. Sok szerző, köztük Steven Levy, arról panaszkodik, hogy napjaink hackerei (a komputerunderground) valójában nem érdemlik meg a hacker nevet, mivel nem felelnek meg az eredeti hackeretika által diktált normáknak – etikátlan személyek tehát, akiket találóbb lenne komputerterroristáknak vagy fiatalkorú bűnözőknek neveznünk, semmint hackereknek. Szerettem volna megtudni, hogy a kilencvenes évek új hackerei ismerik-e legalább valamennyire a régi hackeretikát, netán megváltoztatták vagy továbbfejlesztették azt. Azt is szerettem volna kideríteni, miért érezték úgy, hogy tevékenységük más, mint elődeiké. Egyszersmind arra is kíváncsi voltam, hogy ők mit tekintenek etikátlannak, és közülük egyesek miért utasítják el a hackeretikát, vagy általában bármiféle etikát.

Szövegelemző projektem során világossá vált előttem, hogy az új hackerek kialakították a maguk új etikáját. Érdeklődéssel figyeltem, hogy vajon azoknál, akiknél ez az etika valamilyen formában megnyilvánul, kifejeződik-e valami módon a régi is. Kezdettől úgy véltem, hogy egy új etikai normarendszer elfogadása nem jelenti szükségszerűen a régi teljes elvetését, és egyúttal valamiféle kontinuitás meglétét is feltételeztem a két hackergeneráció között, valamint azt is, hogy az új hackerek ismerik a régi eszményeket. S ha létezik ez a kontinuitás, akkor ez azt is jelenti, hogy az új hackerek nem különböznek annyira a régiektől, mint amennyire Levy és néhány más szerző (vagy IT biztonsági szakértő) véli. Ez esetben az új hackerek egyrészt saját etikai normarendszert alakítottak ki, másrészt elődeik egyes etikai alapelveihez is tartják magukat.

Huszonkilenc, a komputerundergroundban született dokumentumot kódoltam online a NUD*IST szövegelemző rendszer segítségével. Nem zártam ki, hogy a NUD*IST által lehetővé tett interaktív keresési és elemzési folyamat során az egyes kódokból újak jöjjenek létre. Néhány olyan tényezőt is kódoltam, amely nem volt ugyan közvetlenül releváns az elemzés szempontjából, de a későbbiekben növelhette mozgásteremet a kutatásban. Végül a kódolás után teszteltem a régi és az új hackeretika közötti kontinuitásra vonatkozó bizonyítékokat.

Kikből áll a komputerunderground?

A komputerundergroundot (KU) nézetem szerint az alább felsorolt hat csoport valamelyikébe sorolható emberek alkotják. A KU-t helyenként a kilencvenes évek hackereinek vagy új hackereknek nevezem, szembeállítva a régi hackerekkel (a szó régi értelmében vett hackerekkel), akik a hatvanas években működtek a régi hackeretika szerint.

1. ***Hackerek*** (crackerek, rendszertörők) – Olyan személyek, akik távoli számítógépek védelmi rendszerét feltörik. Ez a hackerterminus új értelme. A régi értelemben e kifejezés olyan személyeket jelölt, akik úgynevezett hackeket (csapás, oldalvágás) hajtottak végre, vagyis elegánsan és a szokásostól eltérő módon használták a fejlett technológiákat, illetve az azokra vonatkozó ismereteiket. A hackerek jellemzően olyan (online és nyomtatott) magazinokat olvasnak, mint a *2600* vagy az *Iron Feather Journal*.
2. ***Phreakek*** (*ejtsd: frík* – telefonhackerek, blue boxerek) – Olyan személyek, akik telefonvonalakba, illetve rendszerekbe próbálnak technológiai eszközeik és ismereteik alkalmazásával behatolni és/vagy birtokukba venni azokat. Egyik fő eszközük volt egykor a „blue box" vagy hanggenerátor, de ahogy a távközlési cégek áttértek az analógról a digitális központokra, a phreakek tevékenysége egyre hasonlatosabbá vált a hackerekéhez. A phreakek jellemzően olyan (online és nyomtatott) magazinokat olvasnak, mint a *Phrack*, a *Line Noize* és a *Fone Express*.
3. ***Vírusírók*** (trójai falovak, férgek és logikai bombák készítői) – Olyan személyek, akik kódokat írnak, amelyek *a)* megkísérlik más rendszereken a felhasználók engedélye nélkül reprodukálni magukat, és *b)* gyakran mellékhatásokat is produkálnak, például megjelenhet egy üzenet a képernyőn, furcsán kezdhet viselkedni a gép, vagy tönkremehet a winchester. Az agentek és a spiderek alapvetően jóindulatú vírusok, s azt a kérdést vetik fel, vajon mennyire underground tevékenység valójában a víruskészítés. A vírusírók jellemzően olyan (online és nyomtatott) magazinokat olvasnak, mint a *40HEX*.
4. ***Kalózok*** – A kalózkodás elsősorban nem technikai ügy. A tevékenységbe eredetileg a szoftverek másolás elleni védelmének feltörése, a „cracking" is beletartozott. Ma már kevés szoftvergyártó, illetve -forgalmazó használ ilyen védelmet, de még mindig vannak egyszerűbb eljárások, amik arra hivatottak, hogy megakadályozzák a programok és adatok jogosulatlan másolását. A kalózok ezeket a védő mechanizmusokat rendre kiiktatják, és kereskedelmi forgalmazásra szánt szoftvereket terjesztenek ingyen ismerőseik körében. A kalózok általában a *Pirate Newsletter*t és a *Pirate Magazine*-t olvassák.
5. ***Cypherpunkok*** (kriptoanarhisták) – A kriptoanarchisták ingyenesen terjesztenek olyan eszközöket és közölnek eljárásokat, amelyek segítségével bárki erős kódolással (strong encryption) védheti digitalizált anyagait, illetve adatait. Az erős kódolás feltörhetetlen, illetve csak nagyon nagy teljesítményű komputerekkel lehet megfejteni. Mivel az erős kódolással (ez az alapja például a PGP-nek, vagyis a Pretty Good Privacy nevű adatvédelmi eljárásnak) védett adatok még az amerikai Nemzetbiztonsági Hivatal (NSA) és az FBI számára is hozzáférhetetlenek, az olyan programok, amelyek erős kódolást használnak, fegyvernek minősülnek, s a használatukhoz szükséges algoritmusok terjesztése bűncselekmény. Egyes kriptoanarchisták szerint az erős kódolás az állam teljes kizárására alkalmas eszköz, mivel lehetetlenné teszi, hogy a kódot nem ismerők bármilyen üzleti vagy személyes információhoz hozzáférjenek. A kriptoanarchisták általában a *Cyberpunks* levelező listát olvassák.
6. ***Anarchisták*** – törvénysértő (vagy legalábbis morális szempontból kétes megítélésű) információkat terjesztenek. Csak néhány példa: bombakészítési és betörési útmutatók, pornográf anyagok, kábítószer-gyártási eljárások, kalózrádiók, kábeltévés és műholdas tévécsatornák adatai. A komputerunderground szóhasználatában az anarchista elsősorban nem az államhatalom megdöntését célul kitűző személyt jelenti, hanem olyasvalakit, aki minden olyan kísérletet, illetve rendelkezést elutasít, ami

gátolná az információ szabad áramlását. Az anarchisták jellemzően a *Cult of the Dead Cow*-t *(CDC)* és az *Activist Times Incorporated*et *(ATI)* olvassák.

7. ***Kiberpunk*** – általában a fentiek valamilyen kombinációja, plusz érdeklődés a technikai önmodifikáció, a Neuromancer típusú sci-fi, a hardver hacking és a „street tech" iránt. A kiberpunk világa fiatalok önálló szubkultúrája, amely közös jegyeket mutat a „modern primitív" és a „raver" szubkultúrákkal.

A dokumentumok

Az alábbi huszonkilenc szövegfájl a következő forrásokból származik: WELL (Whole Earth 'Lectronic Link) BBS, a MindVox BBS archívuma, más hacker boardok, az alt.2600 Usenet hírcsoport, World Wide Web HTML dokumentumok, a gopher.eff.org hackermagazin archívuma, a cyberpunks.ork ftp site, valamint a „hacker ethic" kifejezésre végzett webes keresés eredményeként kapott dokumentumok egy része. Az elemzett szövegek kiválasztásánál a fő aspektus a téma szempontjából való relevanciájuk volt, következésképpen az elemzést nem teljesen véletlenszerű mintán végeztem.

1. Discussion begins (A párbeszéd kezdete)
2. An unwritten manifesto (Egy meg nem írt manifesztum)
3. Government ethic (Az állam etikája)
4. Hacker theory to practice (A hackelés elmélete és gyakorlata)
5. The Manifesto (A kiáltvány)
6. The MetaForum (MetaForum)

[1990-ben a WELL néven ismert bulletin board rendszer (BBS) működtetői a *Harper's* magazinnal közösen konferenciát rendeztek a hackelés jövőjéről. A szimpóziumra régi és új hackereket is meghívtak. A fenti szövegek a konferencia fő témáira beküldött hozzászólások.]

7. Cracker subculture (Cracker-szubkultúra)
8. Hackers wanted (Hacker kerestetik)

[A WELL Hacker Conference két másik fő témájára beérkezett hozzászólások szövegei.]

9. Assert your rights (Ragaszkodj jogaidhoz!)
10. Defense of Piracy (A kalózkodás védelmében)
11. Revolt (Felkelés)

[A Subvert (Felforgató) álnevű hacker három propagandaszövege, melyekben kísérletet tesz a hackelés morális megalapozására.]

12. From Crossbows to Cryptography: Thwarting the State via Technology (A számszerítjtól a kriptográfiáig: Technológiával az állam ellen)
13. The Crypto Anarchist Manifesto (Kriptoanarchista kiáltvány)

[Ez a két dokumentum a cyberpunkok ftp archívumából származik. Szerzőik az erős kódolás és a kriptoanarchia szószólói.]

14. Pirate (Kalóz)
15. Pirate Newsletter (Kalóz Hírlevél)

[Két e-zine kalózoknak.]

16. Ethics of Hacking by „dissident” (A hackelés etikája. Szerző: dissident)
17. Hack Ethics – A definition of the hacker ethic from the MIT „Fishwrap Gallery” (A hackelés etikája – A hackeretika meghatározása – az MIT „Fishwrap Galleryből”)
18. Jargon File hacker hacker ethic – Definition of „hacker ethic” from the Hacker's Jargon File (online companion to Hacker's Dictionary) 3.0 (A hackeretika meghatározása a Harker Zsargonfájl 3.0-ás kiadásában)
19. The Hacker's Code of Ethics by „Darkman” (Hackeretikai szabálykönyv, szerző: Darkman)

[A fenti négy szöveg a hackeléssel kapcsolatos etikai kérdéseket vizsgálja.]

20. CDC – Cult of the Dead Cow description file (CDC leíró file)
21. Digital Free Press (Szabad Digitális Sajtó – hacker e-zine)
22. Emmanuel Goldstein testimony – A *2600* főnökének vallomása egy a hackelésről tartott kongresszusi meghallgatáson
23. Hacker Manifesto – „The Conscience of a Hacker” by Mentor (Hackerkiáltvány – „A hacker lelkiismerete”)
24. Hacker vs Cracker – „The Difference between Hackers and Crackers” (Hacker kontra Cracker – Mi a különbség a hackerek és a crackerek között? Szerző: CandyMan)
25. Novice's guide to hacking (Bevezetése a hackelésbe kezdőknek. Szerző: Mentor és a Legion of Doom, LOD, 1989 körül)
26. Phrack – Declaration of Grievances of the Electronic Community – (Phrack – Az e-közösség panaszai) A Függetlenségi Nyilatkozat panaszokat felsoroló passzusainak alkalmazása a kiberkorra. A panaszok az állam technológiával kapcsolatos politikájára vonatkoznak.
27. Rebels with a Cause (Okkal lázadók) – Tanja Rosteck antropológia szakos hallgató 1994-ben írt esszéje, melyben hackerekkel készült interjúk és nyilatkozatok átiratai is szerepelnek.
28. What is hacking? (Mi a hackelés?) A Hacker's Haven website-on szereplő definíció.
29. The Anarchist's Guide to the BBS (Anarchisták kézikönyve a BBS-ekhez) – A BBS-ek használata KU célokra.

Egyéb források

A hagyományos hackeretika

Minden foglalkozásnak megvan a maga etikai rendszere, amely azt hivatott sugallni, hogy az adott tevékenységet űzők, illetve szervezeteik, csoportosulásaik képesek az önszabályozásra. Az etikai rendszerben kodifikálódnak az adott tevékenységet végzők közösségének etikai alapelvei, s egyszersmind ez az etikai rendszer biztosít alapot arra, hogy a közvéleményben és az államban bizonyos fokú bizalom ébredhessen a szakma iránt. Egyes szakmai etikai rendszerek igen régiek és formalizáltak. Ilyen például az orvosok hippokratészi esküje. Más normarendszerek modernek és törvény jellegűek, példa erre az alkalmazott és az elméleti antropológusok etikai kódexe. Vannak „underground” etikai rendszerek is (például a 18. századi Kalóz Etikai Kódex vagy a Maffiatagok hűségesküje), amelyek lehetővé teszik, hogy a szubkultúrákhoz tartozók és az underground csoportok tagjai együttműködjenek, és védelmet biztosítanak nekik a kívülállókkal szemben. Megint mások, mint például az eredeti hackeretika, informálisak és egyszerűek – ökölszabályok.

A csoportok különböző módokon érvényesítik etikai rendszerüket. Ha egyes szabályok elavulnak, egyszerűen figyelmen kívül hagyják őket. Ezért van az, hogy a legtöbb orvos nem törődik a hippokratészi eskü abortuszra vagy eutanáziára vonatkoztatható részével, ugyanakkor a legtöbbjük (de nem mindegyikük) nem tagadja meg az alapellátást krízishelyzetben lévő betegtől csak azért, mert az nem tud fizetni érte. Más csoportok, mint például az antropológusok, azért dolgoznak ki etikai rendszert, mert egyes tagjaik viselkedése erre kényszeríti őket. Az ilyen csoportok által kialakított etikai szabályok jobbára kifejezetten a felmerült problémákra irányulnak. A normák megsértése a szakmai közösségből való kizárással járhat. A hackeretika megsértésének következménye rendszerint kiközösítés vagy elszigetelés.

Az eredeti hackeretika egyfajta rögtönzött, informális etikai kód volt, amelyet az MIT és a Stanford régi hackerei alakítottak ki az ötvenes és hatvanas években. Ezek a „hackerek" voltak az első olyan számítógép-programozók, akik időosztásos számítógépes rendszereken dolgoztak, és gyakran ütköztek a legkülönfélébb bürokratikus szabályokba, amelyek meggátolták őket abban, hogy a technológiai rendszerek (komputerek, telefonrendszerek és egyéb eszközök) működését teljes körűen, vagyis az eszközök adta lehetőségek határáig elmenően tanulmányozzák. Az ő etikájukban az ezen akadályokhoz való viszonyuk fejeződik ki, valamint a technológia felszabadító hatásába és hatalmába vetett hit. Következzék most a hackeretika hat alapelve. A felsorolást a fent említett szövegekből származó rövid idézetekkel egészítem ki, amelyek megmutatják, hogyan fejeződik ki az illető alapelv az adott dokumentumban.

Mindezen alapelvek rövid összefoglalását megtaláljuk egyébként Steven Levy 1984-ben megjelent, *Hackers: Heroes of the Computer Revolution* (Hackerek: A számítógépes forradalom hősei) című munkájában. Levy szerint etikai alapállásuk és szokványostól eltérő stílusuk folytán az olyan hackerek, mint Jobs és Wozniak indították el a „számítógépes forradalmat", amelynek során megszületett az első személyi számítógép, az Apple. Ezt a gépet már könnyű volt használni, és az egyént felruházta az önálló programozás hatalmával.

1. *A hozzáférés joga:* Az egyén számára teljes körű hozzáférést kell biztosítani számítógépekhez és egyéb hardverekhez egyaránt. Kategorikus imperativus minden olyan határ és korlátozó tényező megszüntetése, amely az embert akadályozhatja a számítógép használatában, működésének megértésében, legyen az bármilyen nagy, bonyolult, veszélyes, szerteágazó, tulajdon- vagy szerzői joggal védett és nagy teljesítményű.

> Mindenki számára világos, hogy jelenleg nem ez a helyzet. A számítógépes rendszerek kizárólag a nagyvállalatok és az állam kezében vannak. A csodálatos eszköz, amelyet arra szántak, hogy gazdagabbá tegye életünket, fegyverré vált, amely segít elemberteleníteni az embert. Az állam és a nagy cégek számára az ember nem egyéb, mint tárhely a számítógépes adathordozókon, s a kormányok ahelyett, hogy a szegények hatékonyabb megsegítésére használnák a komputerrendszereket, nukleáris fegyvereket irányítanak velük. Az átlagamerikai csak mikrokomputerekhez juthat hozzá, amelyek áruknak töredékét érik csupán. A gyártók elképesztő árakból és bürokráciából emelnek áthatolhatatlan falat az egyén és a legkorszerűbb eszközök közé. Ennek az állapotnak a megváltoztatására alakult ki a hackelés mint tevékenység („Doctor Crash" 1986) [1].

2. *„Az információ szabad és ingyenes akar lenni!"* A „szabad" kifejezést kétféleképpen értelmezhetjük. Jelenthet kötöttség és ellenőrzés nélküliséget (mozgásszabadság = cenzúranélküliség), és irányítástól való mentességet (a változás, a fejlődés szabadsága = nem érvényesek rá a tulajdonjog és a szerzői jog kategóriái). Egyes hackerek odáig mennek, hogy az információt élő entitásnak tekintik, amely szabadon létezik és cselekszik, mint a vírusok, a genetikai algoritmusok és más szoftverek.

Sok információt tekintenek titkosnak. A kormányok tevékenységéről, a vállalatok sötét ténykedéseiről és egyéb „alantas üzelmekről” szóló információkat is hozzáférhetővé kell tenni. Az ilyen információk terjesztése törvényellenes és veszélyes. Szerény véleményem szerint ugyanakkor ez a hackelés egyik leghasznosabb hozadéka. Az információ megszerzésének és terjesztésének alapfeltétele az anonimitás. Azokat, akik a veszélyre felhívják a figyelmet, csak akkor lehet elhallgattatni, ha azonosítani tudják őket…

Az információhoz való hozzáférés joga

A hozzáférés alapvető jog. Mindenkinek jogában áll tudni, ha az állam embereket öl meg, sugárfertőzésnek teszi ki, lehallgatja őket és hazudik nekik. Az embereknek joguk van információhoz jutni a kormányukról. Hiszen a kormány tagjai közülünk kerülnek ki, mi választjuk őket, s a közöttük és köztünk fennálló társadalmi szerződés biztosítja hatalmukat. [2]

3. *Ne bízz a hatalomban!* A kulcsszó a decentralizáció. A hackeretikának ez az alaptétele mutatja az alapállás erősen anarchisztikus, individualista és libertariánus voltát. A hackerek soha nem bíztak semmilyen nagy intézményben. Az olyan eszközökről, mint a PC-k, azt tartják, hogy kiveszik a hatalmat az óriási számítógépes rendszereket alkalmazó nagy szervezetek kezéből, és a „kisember” felhasználót ruházzák fel vele. A „kisember” ethosza sehol nem erősebb, mint az államhatalom-ellenes kriptoanarchisták és az extropiánusok körében.

Valójában a technológia az egyik legígéretesebb eszköz arra, hogy visszaszerezzük szabadságunkat azoktól, akik elrabolták tőlünk. Természeténél fogva a technológia azok számára kedvező eszköz, akik okosak (vagyis akik élni tudnak vele), szemben a butákkal, akik nem képesek. Azoknak kedvez, akik gyorsan képesek alkalmazkodni és váltani (vagyis akik gyorsan meglátják az új dolgok előnyeit), szemben azokkal, akik nehézkesek (vagyis akik a kipróbált régi dolgokhoz ragaszkodnak). Vajon van-e két szó, amely jobban jellemezné az állami bürokráciát, mint a „buta” és a „nehézkes”? [3]

Az állam természetesen megkísérli lelassítani, vagy akár meg is állítani a technológia terjedését, s ehhez nemzetbiztonsági megfontolásokra hivatkozik, vagy arra, hogy az új eszközöket kábítószerkereskedők és adócsalók használják. Gyakori hivatkozási alap még a társadalom szétzilálódásának réme. Az aggályok többsége jogos. A kriptoanarchia megnyitja az utat az államtitkok, a tiltott és lopott anyagok számára, azok így szabadon áramolhatnak és cserélhetnek gazdát. Az anonimitást biztosító számítógépes piacon még a gyilkosság és a zsarolás is a kereskedelem tárgyává válhat. Mindenféle bűnözők és külföldiek használhatják a CryptoNetet. Ez azonban nem szabhat gátat a kriptoanarchia terjedésének. [4]

4. *Elég a mondvacsinált kritériumokból!* A hackereket a tevékenységük alapján kell megítélni, nem pedig olyan „mondvacsinált kritériumok” alapján, mint a fajuk, koruk, nemük vagy pozíciójuk. Sehol sem nyilvánul meg látványosabban ez az ethosz, mint abban, hogy a hackerek túlnyomó többsége szilárdan hisz az internet embereket egyenlővé tevő hatalmában. Az interneten az anonimitás megengedi, hogy az olyan változók, mint valakinek a faja, kora stb. rejtve maradjanak, és az ötleteket, elképzeléseket kizárólag a lényegükhöz tartozó kritériumok alapján bírálják el, mivel az egyéb kontextuális faktorok nem ismertek.

Az internet az egyik legjobb fricska a világon. Folyamatosan megkérdőjelezi az olyasfajta, mélyen gyökerező társadalmi előítéleteket, mint amilyenek a korhoz, fajhoz, vagyoni helyzethez és nemhez társulnak. Az amerikai számítógépes hálózatokon nem ritka, hogy egy tizennégy éves gyerek egy negyvenegy éves felnőttel vitatkozik filozófiai kérdésekről. [5]

5. *„A számítógép az igazság megismerésére és szépség teremtésére alkalmas eszköz.”* A hackerek egyenlőségjelet tesznek a hackelés, valamint a művészet és kreativitás közé. Ráadásul az ethosznak ez az eleme a filozófia szintjére emeli a hackelést (szemben az egy-

szerű pragmatizmussal). A filozófia pedig (legalábbis egyes megnyilvánulásai) az emberiségnek a jó, az igaz és a szép iránti vágyáról szól.

> Nem kérdéses, hogy a jó programozás (hackelés) művészet, és mint minden művészetben, az alkotóknak megvan a maguk sajátos stílusa, kézjegye (amely idővel változhat). [6]

6. *„A számítógép jobbá teheti életünket."* Ez a tétel bizonyos fokig az előzőből következik. Mivel az emberek többsége vágyik a jó, igaz és/vagy szép dolgokra, az a tény, hogy a számítógéppel lehet ilyeneket készíteni, azt is jelentheti, hogy képes megváltoztatni az élet minőségét. Ugyanakkor az idézőjelek közt szereplő mondat egyszerű kijelentés, amelyben – akárcsak az előzőekben – a technológia iránti mélységes szeretet fejeződik ki. Nem állítja explicit módon, hogy a komputereknek mindenképpen és mindig jobbá kell tenniük az ember életét, mint ahogy azt a tételt sem mondja ki, ami egyébként logikusan következne a fenti axiómából, nevezetesen, hogy etikátlan dolog a számítógépet arra használni, hogy az emberek életét rosszabbá tegye… Sok hacker, köztük Emmanuel Goldstein is, hatalmas pozitív erőnek tekinti az internetet.

> Létfontosságú, hogy ne engedjük eluralkodni félelmeinket és aggályainkat, és ne hagyjuk, hogy demokratikus ideáljaink és a magánélettel kapcsolatos értékeink sérüljenek. A kibertér, virtuális világ sok szempontból valóságosabb, mint a valósnak nevezett. Azért gondolom ezt, mert az emberek csak a virtuális világban lehetnek szabadon azok, *akik*, önmaguk szerint valók. Itt véleményt nyilváníthatnak anélkül, hogy büntetéstől kellene félniük; ha akarnak, névtelenek maradhatnak, és részt vehetnek egy olyan dialógusban, ahol a szavaik értelme szerint bírálják el őket, nem pedig a bőrük színe vagy a hangjuk mélysége alapján. Hasonlítsuk ezt össze a „valós" világgal… Az internet a saját törvényei szerint alakult ki és fejlődik, és a világméretű demokrácia erődjévé vált. … A kormányok kötelessége, hogy minden szempontból szabad utat engedjenek számára. [7]

A fentiekből következően a hackeretika alapelvei szerint a hackernek kötelessége, hogy minden gátat leromboljon, szabaddá tegye az információ áramlásának útját, decentralizálja a hatalmat, képességeik alapján ítélje és becsülje meg az embereket, és számítógépe segítségével az ember életminőségét javító dolgokat hozzon létre. Továbbra is nyitott kérdés (interpretáció kérdése), hogy a hackeretikából következik-e a szoftverek terjesztésének teljes szabadsága mint kívánalom (amint ezt Richard Stallman követeli), a számítógépek negatív szándékkal való felhasználásának tilalma (Clifford Stoll), vagy a biztonságos, a bizalmon alapuló hálózatok kialakításának igénye (Steven Levy). A fenti idézetek mindegyike arra utal, hogy az új hackerek tudatában vannak a hackeretika alapelveinek, és – szándékosan vagy ösztönösen – érvényesítik azokat.

Az új hackeretika

Az említett dokumentumok vizsgálata alapján arra a következtetésre jutottam, hogy létezik egy új hackeretika, amelyhez a kilencvenes évek hackerei tartják magukat. Az is látható, hogy a régi hackeretika töredékei átkerültek az új értékrendbe, és ily módon megfigyelhető egyfajta folytonosság. A régihez hasonlóan az új etika is informálisan alakult ki, s ennek egyes elemei sem mentesek az ambiguitástól és bizonyos ellentmondásoktól. Mindez abból fakadhat, hogy az új hackerek jóval többen vannak és elszórtabban tevékenykednek, mint a hatvanas évekbeli elődeik.

1. *„A legfőbb szabály: ne árts!"* Vagyis ha lehet, ne tégy kárt komputerekben és adatokban. Ez hasonló a hippokratészi eskü alaptételéhez.

> A hackeretika szerint kötelező:
> - biztonságosan tevékenykedni,
> - semmiben kárt nem tenni,

- senkiben kárt nem tenni, sem fizikailag, sem szellemileg, sem pedig érzelmileg,
- humorosnak lenni, legalábbis azok többsége számára, akik a hackerek tevékenységének eredményével szembesülnek. [8]

A hackeretikával ellenkezik, hogy a logfájlokon kívül – a rendszerbe való behatoláshoz és nyomaik eltüntetéséhez ez elengedhetetlen – bármilyen adatot megváltoztassanak egy rendszerben. A rossz szándékú crackerekkel szemben a hackerek nem éreznek késztetést, hogy adatokat semmisítsenek meg vagy tegyenek tönkre. Céljuk, hogy az adott rendszert tanulmányozzák, és a lehető legtöbbet megtudjanak róla. A hackereket a csillapíthatatlan, sőt egyre növekvő tudásvágy hajtja. [9]

2. A rendszerekbe való behatolás – ha puszta szórakozásból vagy ismeretszerzés céljából történik – etikailag elfogadható, mindaddig, amíg a hacker nem lop, nem garázdálkodik és nem sért meg bizonyos bizalmas információkra vonatkozó korlátozásokat. [10]

A fenti alaptétellel kapcsolatban a legfőbb probléma, hogy a szándékra alapoz. Nem szabad szándékosan adatokat tönkretenni. De mi a helyzet, ha – ahogy gyakran megtörténik – egy hacker véletlenül töröl vagy változtat meg fájlokat? Vajon ilyenkor etikai vétséget követ el? Az sem egyértelmű, mi minősül „károkozásnak". A legtöbb hacker nem tekinti annak az apróbb csínytevéseket és tréfákat, függetlenül attól, milyen lelki hatást váltanak ki. Ugyanakkor nem biztos, hogy ezt áldozataik is így gondolják, különösen akkor nem, ha értékes időt veszítenek vagy sok munkájuk vész kárba.

A magánadatok védelme

Az embereknek joguk van ahhoz, hogy személyes adataik védve legyenek. Ez annyit jelent, hogy joguk van teljes körű ellenőrzést gyakorolni saját (és családi) adataik felett. De meddig terjed ez a jog? Beleértendő az is, hogy az ember az interneten is anonim létezik? Van-e jogom munkaadóm elől eltitkolni az olyan információkat, mint az egészségi állapotom, priuszom, szexuális szokásaim stb.?

Vannak-e olyan személyek (politikusok, híres személyiségek), akiknek az adatait kevesebb védelem illeti meg, mint másokéit? A személyes adatok sérthetetlenségét hirdető hackerek elveiben rejlő furcsaság, hogy bizonyos információkra vonatkozóan nem tartják érvényesnek a szabad hozzáférhetőség követelményét, s ilyen módon ellentétbe kerülnek az eredeti hackeretikával.

A személyes adatok védelméhez való jog

Úgy véljük, a személyes adatok védelme alapvető jog. Sajnos az [amerikai] alkotmány – ebből szempontból elavult lévén – nem mondja ki egyértelműen ezt a jogot. [11]

A hackerek ugyanakkor rendkívül fontosnak tartják a személyes adatok védelmét, éppen azért, mert manapság rengeteg módon és irányból fenyegetik azokat. Amikor csak lehet, felhívjuk az emberek figyelmét, hogy védjék könyvtáraikat, titkosítsák e-mailjeiket, ne használják mobiltelefonjukat, és tegyenek meg mindent, hogy életüket, az azzal kapcsolatos adatokat megtarthassák maguknak. 1984-ben hackerek kulcsszerepet játszottak abban, hogy kiderült: a TRW amerikaiak millióiról vezetett személyihitel-fájlokat. Az emberek többsége korábban egyáltalán nem hallott a hitelfájlokról. A fájlállományt védő jelszavakat gyakorlatilag nem kezelte titkosan a rendszer. Sőt magukra a hiteljelentésekre is rányomtatták őket. [12]

Érdekes módon a hackerek többsége nem azt kifogásolta, hogy a TRW az emberek tudta nélkül adatokat gyűjtött banki hitelügyleteikről (s így az érintettek azok helytállóságát sem ellenőrizhették), aminek alapján azután a bankok hitel- vagy jelzálogkérelmeiket elbírálták. A hackerek számára az volt elfogadhatatlan, hogy a fájlokat nem védték eléggé, vagyis könnyű volt hozzájuk férni.

„Használd, de ne vedd el!”

A számítógépeknek nem szabad kihasználatlanul állniuk. Etikailag helytelen, ha az emberek nem férhetnek hozzá a számítógépekhez, amikor tulajdonosaik nem használják azokat. Ezt az alapelvet sokan „sétakocsikázó etikának” nevezik. Hiszen nem teszünk-e valójában szívességet, ha kölcsönvesszük valakinek az autóját anélkül, hogy az illető tudna róla, és azután tele tankkal visszavisszük, sőt tanácsokkal is ellátjuk a tulajdonost arra vonatkozóan, hogyan használhatná még jobb hatásfokkal a kocsiját? (És vajon etikai vétség-e, ha egy sorozat kulcsot is csináltatunk az autóhoz, hogy azután bármikor kölcsönvehessük? Ugyanis a hackerek voltaképpen ezt teszik, amikor a rendszergazdák jogosítványait felhasználják.) Ugyanakkor a hackerek többsége érzékeny arra, hogy csak ő használhassa személyi számítógépét.

> Az interneten keresztül körülbelül negyedmillió olyan számítógéphez lehet hozzáférni, amelyek napi tíz órán át kihasználatlanul állnak. Ilyen hatalmas, potenciálisan elvesztegetett kapacitás láttán egy igazi hacker engedélyt kérne a gépek használatára, és semmiképpen sem tartaná vissza, ha esetleg nem kapná meg a jóváhagyást. Ugyanakkor minden lehetséges óvintézkedést megtenne, hogy ne tegyen kárt a rendszerben, amelybe behatol. [13]

Lépd át a határokat!

A hackelés lényegéhez tartozik a határokon való átlépés, a korlátok szétfeszítése. Ezt az alapelvet egyes régi hackerek a Régi Etika hetedik, informális alaptörvényének tekintik. Ha egy hackernek azt mondjuk, hogy valamit nem tud megcsinálni, az illető azonnal erkölcsi kötelességének fogja érezni, hogy nekiveselkedjen. Az extropiánusok hisznek abban, hogy a világban működő egyik fő erő a tágulás, a kiterjedés, a növekedés törvénye. A hackelést extropikus tevékenységnek tekintik, mivel célja a határok átlépése, a technológiát pedig a növekedés eszközének tartják.

> Ahhoz, hogy szabadok lehessünk, át kell lépnünk a középkori erkölcsi szabályokon, át kell hágnunk az igazságtalan törvényeket és el kell felejtenünk a vállalathoz való hűség fogalmát. Lesznek, akik mindezért hűtlennek és bűnösnek mondanak majd bennünket. Egy szabad ember jelenléte demoralizálja a vele egy szobába összezárt rabszolgákat. Szabadítsd fel embertársaidat! Add kezükbe a fegyvert, a tudást, amely segít nekik, hogy az elnyomóval szembeszálljanak! [14]

A kommunikációhoz való jog elve

Az embereknek joguk van szabadon kommunikálni egymással. Az ENSZ Telekommunikációs Szervezete (ITU) több fórumon leszögezte, hogy ezt az alapvető emberi jogot minden országnak és kormánynak tiszteletben kell tartania. Globális szinten ugyanakkor fontos morális probléma, hogy a harmadik világ országainak infrastruktúrája nem elég fejlett ahhoz, hogy polgáraik a szabad kommunikációhoz való jogukat érvényesítsék. Számos ENSZ-felmérés foglalkozik ezzel a problémával.

A hackerek többsége lelkes híve az amerikai alkotmány első kiegészítésének, amely a szólás- és gyülekezési szabadságról szól. A phreakerek (telefonhackerek) még egy lépéssel tovább mennek, és kijelentik, hogy az embereknek joguk van *olcsón* és *könnyen* kommunikálni egymással (hogy a szegények se legyenek elzárva a távolsági beszélgetésektől). Ha a távközlési cégek akadályozzák az olcsó telefonos kommunikációt, a telefonhackelés a megoldás.

Kommunikáljunk!

> Ez a legalapvetőbb emberi jog. A puszta tény, hogy ez a lap létezhet, a bizonyíték arra, hogy a szólásszabadság még létezik. Az állam által garantált védelem ellenére sok dolog veszélyezteti a kommunikációhoz való jogot. [15]

Ne hagyj nyomot!

Ne hagyj magad után semmilyen nyomot, jelet, amely arra utal, hogy behatoltál a rendszerbe. Ne hívd fel magadra a figyelmet! Dolgozz csendben, hogy más is hozzáférhessen ahhoz, amihez te. Ez az etikai alapelv arról szól, hogy a hacker nem csak a saját érdekeit tartja szem előtt, hanem a többieket is védi attól, hogy elfogják őket vagy elvesszen számukra a hozzáférés lehetősége. Természetesen a titokban való tevékenykedés szükségességének elve ellentétben áll az információ szabad áramlására vonatkozó alapszabállyal.

A hackerek az alábbi szabályok szerint dolgoznak:

1. Dolgozz észrevétlenül!
2. Ha gyanakodni kezdenek rád, dolgozz még észrevétlenebbül!
3. Ha vádolnak, tagadj!
4. Ha elfognak, hivatkozz az alkotmány ötödik kiegészítésére. (Amely egyebek közt kimondja, hogy senki nem tartható fogva bírósági ítélet, illetve megfelelő jogi eljárás nélkül és nem kényszeríthető arra, hogy maga ellen tanúskodjon.] [16]

Oszd meg!

Az információ akkor a legértékesebb, ha a lehető legtöbb emberrel megosztják. Ne titkolózz, és ne rejtsd el! Ezt az alapelvet tekinthetjük az eredeti etika egyik tételéből levezetett princípiumnak. A kalózetika szerint a szoftverek értékét növeli, ha az emberek kipróbálhatják őket, mielőtt fizetnének értük. Éppen ezért dicséretes dolog, ha az ember a birtokába került szoftvereket megosztja barátaival.

A kalózok tanulás, információcsere és szórakozás céljából megosztják a WAREZt [szoftvereket] másokkal. A kalózkodás életforma. Egy irodai dolgozó, aki kollégáinak átad egy szoftvert, vagy egy tanuló, aki osztálytársaival megoszt egy floppyt tele programokkal, semmivel sem inkább kalóz, mint egy barát, aki kazettára veszi nekünk a legújabb Depeche Mode-albumot. Az IGAZI kalóz nagyobb közösségekkel áll kapcsolatban, amelynek tagjait a warezek iránti érdeklődés köti össze. A kapcsolattartás leginkább Bulletin Board rendszereken (BBS) keresztül történik. Az alapszabály: „Adj valamit, hogy kapj valamit. Jótett helyébe jót várj!" A kalózok NEM ingyenélők, és csak a lámák [buta kezdők] hiszik, hogy semmiért kaphatnak valamit. [17]

Önvédelem

A hackerekre és a vírusokra szükség van ahhoz, hogy az embereket meg lehessen védeni egy az 1984-ben felvázolt jövőtől, vagy az állam és a nagyvállalatok növekvő hatalmától. Erkölcsi kötelesség a hackelést egyfajta jujitsuként használni arra, hogy a nagy, személytelen, az egyén életének irányítására törekvő erők fölébe kerekedhessünk.

Hiszek abban, hogy a szabadság hívei és az Amerikát alkotmányosságtól megfosztani szándékozók közötti háború egyre hevesebben dúl majd. Ha ez így lesz, minden lehetséges eszközt fel akarok használni, hogy a leskelődő szemekbe homokot szórjak. A vírusok az önvédelem eszközeivé válhatnak egy olyan kormány ellen, amely fél az egyén birtokában lévő számítógéptől. [18]

A hackelés voltaképpen növeli a biztonságot. Hasznos és jótékony dolog megkeresni a biztonsági rendszerek réseit, s azután megmutatni, hogyan kell befoltozni azokat. A hackelés pozitív hatása, hogy megtanítja az embereket arra, hogyan kell a gyenge védelmet megerősíteni, és esetenként – komoly károkozás nélkül – beláttatja velük, hogy nincs tökéletes védelem.

A biztonság növeléséről szóló alapelv másik értelmezése még ellentmondásosabb: Vannak, akik éppen olyan etikátlannak tartják a crackelést, mint a betörést és a magánlaksértést. Ugyanakkor az „etikus" crackelés kizárja a rombolást, s ez legalábbis moderáltabbá teszi az olyan emberek viselkedését, akik „jóságos" crackereknek tartják magukat (lásd még: szamuráj). Ilyen alapon a legmagasabb fokú tisztelet megnyilvánulása, ha az illető *a)* valakinek a rendszerébe behatol, és *b)* elmagyarázza a rendszergazdának – lehetőség szerint a rendszergazda accountjáról küldött e-mailben –, hogyan sikerült bejutnia és hogyan lehetne betömni a rést. [19]

Számos szoftvercég, köztük a Lotus, rendszeresen bíz meg hackereket, hogy teszteljék rendszerüket. Ez azt is jelenti, hogy bizonyos fokig a piac egyes szereplői is érvényesnek ismerik el ezt az etikai alapelvet. Ugyanakkor természetesen még a Lotus sem szeretné, hogy rendszerét olyan hackerek teszteljék, akiket nem a cég alkalmaz.

Bízz, de tesztelj!

Folyamatosan tesztelni és fejleszteni kell a rendszerek védelmét. Ne bízzuk másokra azok karbantartását. Ismerjük meg teljes mélységében az általunk használt rendszert. Ha sikerül olyan módon használnunk, ahogy létrehozói nem is álmodták – annál jobb. Így azontúl csak még jobb rendszereket készítenek majd.

> A demokráciát folyamatosan tesztelik – ez a lényegéhez tartozik. Zászlóégetők, melegjogi aktivisták, ku-klux-klanosok, számítógéphackerek – egyfolytában próbálgatjuk a rendszer tűréshatárát, hogy megtudjuk, mennyire sérülékeny. Hangsúlyozom: NEM csupán azért csináljuk, mert érdekel a dolog bennünket, hanem mert – tágabb kontextusban – a demokrácia hitelességét ellenőrizzük. [20]

A brit hackerek egyik legfontosabb kézikönyve, a „Beating the system" szerint ahogy a rendszerek (például a telefonhálózat) egyre bonyolultabbá válnak, egyre kevésbé lehetséges centralizáltan, egy irodából működtetni őket. A hackelés így nemcsak hogy lehetségessé, hanem szükségessé is válik. A hackerek etikai kötelessége, hogy teszteljék a rendszereket, nehogy azok a legkritikusabb pillanatban omoljanak össze (ahogy ez 1990-ben az AT & T központokkal történt).

Röviden összefoglalva tehát az új hackeretika szerint a hackerek, vagyis a komputerunderground kötelessége 1. az adatok és a hardverek védelme; 2. a személyes adatok tiszteletben tartása és védelme; 3. a mások által elvesztegetett kapacitás kihasználása; 4. a felesleges korlátok átlépése; 5. az emberek kommunikációhoz való jogának védelme és érvényre juttatása; 6. nyom nélkül tevékenykedni; 7. az adatokat és szoftvereket megosztani; 8. éberen őrködni, nehogy a hatalom a kibertérben is központosítottá váljon; 9. a számítógépes rendszerek védelmének tesztelése.

Mi tilos?

Miután láttuk, mi kötelező, az alábbiakban áttekintjük, mi az, amit tilt az új hackeretika. Az, hogy mi számít etikátlannak, sok esetben levezethető a kötelezőnek tekintett alapelvekből, és megfordítva; abból, hogy mit tekintenek tiltottnak, következtethetünk arra, hogy mit gondolnak kívánatos magatartásnak.

1. Orgazdaság és kereskedelmi szemlélet, kalózkodásból származó szoftver eladása, hackelés anyagi haszonszerzés céljából, önkiárusítás. Az orgazdaság ellentétes az új hackeretika megosztásról szóló, és a régi normarendszer profitszerzés céljából történő szoftvergyártást kizáró alaptételével.

> A profitszerzés lehetősége időnként a kereskedelem felé csábítja a hackereket. Máskor úgy vélik, hogy a kereskedelem az egyetlen csatorna, amelyen munkájuk gyümölcsét eljuttathatják a tömegekhez. Ha sikerrel járnak, meg is gazdagodnak, és fokozatosan eltávolodnak a hackerléttől, hivatalnokokká válnak, és nem boldogok többé. [21]

> Az orgazdák úgy viszonyulnak a kalózokhoz, mint a bontott autók kereskedői a hobbi-autószerelőhöz. Az orgazdák ugyanis személyes hasznot szereznek a lopott holmi ELADÁSából. A kalózok hitványabbaknak tekintik őket, mint a pedofileket. [22]

Az orgazdaság ellentétes a hackeretikának az információ és szoftverek megosztására vonatkozó 7. alapelvével.

2. Freeloading (Ingyenes és korlátozás nélküli letöltés). A freeloader mindig elvesz, de soha nem tesz hozzá. Használja mások munkájának a gyümölcsét anélkül, hogy ő maga a legcsekélyebb mértékben is hozzájárulna vagy tökéletesítené. Ez szintén ellent mond a 7. alapelvnek.

> A kalózok valójában a minőségi termékek legjobb reklámozói, mivel a megosztás alapelve lehetővé teszi, hogy a felhasználók először kipróbálják az árukat, és csak azután válasszák ki a számukra legmegfelelőbbet. Neem, a kalózok nem freeloaderek. Sőt kifejezetten ellenzik a freeloadolást. [23]

3. Rendszerek megkárosítása, tönkretétele, hardver megrongálása olyan tevékenység, amelyből más felhasználóknak káruk származik, vandalizmus, romboló vírusok, trójai falovak, logikai bombák írása, illetve terjesztése… Nem tilos, viszont bosszantó (nem teljesen ártalmatlan) játékokat játszani a rendszergazdákkal és magukkal a rendszerekkel… Mindez egyenesen következik a „Ne árts!" alapelvből.

> I. Ne tégy kárt semmilyen rendszerben! A BBS-eseket lebombázni helytelen, egyszerű és buta dolog.
> II. Ne változtass meg egyetlen rendszerfájlt sem azokon kívül, amelyekre feltétlenül szükséged van a bejutáshoz, a menekküléshez, az észrevétlenül maradáshoz, illetve a rendszerbe való visszatéréshez. [24]

> Ha van dolog, amit utálok, az az, hogy egyes önjelölt hackerek úgy törnek be rendszerekbe, hogy közben mindent tönkretesznek, ami az útjukba kerül, s ezzel az összes hacker hírnevét tönkreteszik… Aki szétzúz egy rendszert, az semmivel sem méltóbb a hacker névre, mint a nagyanyám. [25]

4. A szélsőséges önzés, a saját érdekek elébe helyezése mindenki másénak, olyan bűnös viselkedés, amelyből egyéb negatív megnyilvánulások is következnek… Itt megint a hackeretika mélyén élő kettősséget figyelhetjük meg: a hacker mélységesen individualista, ám egyszersmind rendkívül erős közösségi érzés is hajtja. Az öntörvényűség nem egyenlő az önzéssel.

> Meg kell húzni a határt hackerek és bűnözők között. Az előbbiek kutatnak és felfedeznek, az utóbbiakat viszont csak saját önös érdekeik motiválják. Persze időnként a hackerek is áthágnak törvényeket, de nem hiszem, hogy ettől mindjárt bűnözőkké is válnának – legalábbis morális szempontból nem feltétlenül követnek el bűnt. [26]

> Vannak hackerek, akiknek igencsak túlméretezett az egójuk … Az egyik ilyen a Corporal Punishment [Testi Fenyítés] nevű… Egy csomószor összeakadtam már vele. Az a fickó Istennek képzeli magát, és mindenkit a földbe tipor… Egyesek azt hiszik, hogy ha másokon átgázolnak, akkor ők nagyobbak lesznek. Bocs, fiúk, de az a helyzet, hogy ettől még nem látszotok nagyobbnak, csak önző disznóknak, akiket viszont el kell tiporni… [27]

> Ne feledkezzünk meg arról, hogy a hackereknek, crackereknek, chippereknek, cruncherekneknek és egyebeknek bizony van egójuk, és engem csak egyetlen dolog zavar a hackeretikában, nevezetesen, hogy nem számol az egóval és az önérdekkel. Mert hát mi mással magyarázhatnánk, hogy a crackerek időnként lopott szoftvert árulnak, vagy hogy egyébként intelligens emberek vírusokat szabadítanak a számítógép-felhasználókra illetve -rendszerekre, remélve, hogy a lehető legnagyobb kárt sikerül okozniuk. És mi más lenne a magyarázata annak, hogy hackerek betörnek a rendszerekbe és csak úgy, a tréfa kedvéért kitörölnek fájlokat? Az emberek szórakozásból hatolnak be idegen rendszerekbe, és még azért, mert így erősnek érezhetik magukat, nem pedig azért, mert kihasználatlanul áll némi számítógép-kapacitás. [28]

5. A (szelektív) Lopásellenes Etika. Az információ, a szolgáltatások és a szoftverek nem számítanak magántulajdonnak, a hardverek, a kézzel fogható javak, a pénz és az ahhoz kapcsolódó szolgáltatások (hitelkártya, digitális pénz, a telefonkártya-számok stb.) viszont igen. Az utóbbiakat ellopni bűn. A lopás tárgyától függ, hogy a cselekedet megengedhető-e. Telefonszolgáltatásokat lopni nagyvállalatoktól vagy az államtól – az

rendben van. Magánszemélytől vagy kis nonprofit szervezettől lopni ugyanezeket – az helytelen. Az új hackeretika így nem támogatja a lopást, hanem egyszerűen bizonyos dolgokat nem tekint tulajdonnak, más esetekben pedig egyes cselekedeteket inkább „kölcsönvételnek" minősít, mint lopásnak.

> Hol húzódik tehát a határ a hackerek és a bűnözők világa közt? Számomra ez mindig egyértelmű volt. Mindannyian tisztában vagyunk azzal, hogy kézzel fogható tárgyakat ellopni bűn. Azt is tudjuk, hogy a vandalizmus negatív jelenség, mint ahogy az sem helyes, ha valakinek a személyes szférájába betörünk. Mindezek a hackerek világán is kívül esnek. [29]

6. Feltűnési viszketegség, nagyzolás, hencegés. Elfogadható, ha egy hacker zárt körben henceg és feltűnősködik, az viszont semmi esetre sem, ha olyan helyen vagy közösségben teszi ezt, ahol kívülállók is tanúi lehetnek. Aki a médiának vagy más nem hackereknek dicsekszik, az megsérti a „Ne hagyj nyomot!" alapelvet.

> Természetesnek tűnhet, ha valaki egy sikeres hackelés után büszkélkedik tettével. Csakhogy ne feledjük: ezzel felhívjuk magunkra a figyelmet, és bizony nem csak a híveink és csodálóink hallják meg, amit mondunk. Így azután barátainkat is bajba sodorhatjuk, és mindenki mást, aki ugyanabba a rendszerbe akar bejutni. [30]

> Az igazi hacker halk szavú… nem dicsekszik. Ha elszólod magad egy barátodnak, vagy egy levelezőlistán nem tudod fékezni magad, hamarosan mindenki tudni fogja, mit tettél, ki vagy, és hogy eltűntél… [31]

7. Helytelen dolog kémkedni, leselkedni, másokat megfigyelni és behatolni a magánszférájukba, például elolvasni az e-mailjeiket. Ez az új hackeretikának a személyes adatok védelmét kívánatosnak kimondó alapelvből is levezethető. Ugyanakkor egy hacker mindennapi gyakorlatának része, hogy jelszavakat kémlel ki és biztonsági rendszereken keres réseket. Itt újra megfigyelhető a magánadatok védelméről és az információáramlás szabadságáról szóló alaptételek közötti ellentmondás.

> Egyes hackerek éppen az ellenkezőjére használják a számítógépet, mint amire az első hackerek szánták: először is korlátozzák a komputer- és telefonrendszereken átfutó információk és adatok áramlását. Másodszor, gépeiket mások megfigyelésére és a róluk való információgyűjtésre használják. [32]

8. Spicliskedés. Etikátlan dolog más hackereket besúgni. A hackeretikának ez a tétele megegyezik más törvényen kívüli csoportok, szubkulturális közösségek, börtöntársak, kábítószer-élvezők és prostituáltak etikai kódjával. Ugyanakkor a hackerek esetében plusz probléma, hogy sok hacker egy idő után számítógép-biztonságtechnikai szakértőként vállal munkát.

> Senki sem alávalóbb a spiclinél. Azok, akik más hackereket felnyomnak, rohadékok. Persze, védettséget és mentelmet ígérnek nekik, ha beköpik a barátaikat. Aki megteszi, az helytelenül cselekszik és árt a hackertársadalomnak. Össze kell tartanunk, annál is inkább, mert valójában senki sem áll a mi oldalunkon. [33]

> És végül vannak hackerek, akik más hackereket felnyomnak a zsaruknak, vagy más hatóságoknak. A spicliskedés manapság egyre divatosabbá válik. Azt mondhatja erre valaki: „Ugyan már, egy normális hacker soha nem nyomna fel egy másikat." És való igaz, aki ezt teszi, nem igazi hacker, maximum annak tartja magát. [34].

A változás okai

A szövegekben különböző magyarázatok szerepelnek arra, miért érzik egyesek, hogy a hackeretika megváltozott.

1. *„Több cucc."* Rendkívüli mértékben megnőtt a komputerek száma, ráadásul sokkal nagyobb a teljesítményük, mint a korábbiaké, hálózatban üzemelnek, fontosabb szere-

pet töltenek be, és elterjedtebbek. Mindez komolyabb lehetőséget biztosít a társadalom ellenőrzésére, ezáltal több lehetőség adódik a korrupcióra és a pozitív kezdeményezésekre is.

> Szinte senki sem tudta, hogy létezik hackeretika, amíg lehetetlen volt betörni a nagy és bonyolult számítógépes rendszerekbe… Most, hogy mindenki össze van kötve mindenkivel, a kísérletezők és felfedezők korábban lokális érvényű és méretű munkája az egész világra kiterjedhet. [35]

> A számítógép korában élünk. Mindent hatalmas rendszerek irányítanak: a vízhálózattól a vasútig, a légi közlekedéstől az áramellátásig és a telefonszolgáltatásig. Képzeljük csak el, milyen kitűnően elszórakozhat egy hacker egy ilyen rendszerben. Betörni egy hálózatba esetenként hatalmas teljesítmény lehet. De én sokkal inkább arra szeretném felhívni a figyelmet, mi mindent csinálhat egy hacker, ha már bejutott a rendszerbe. [36]

2. *A társadalom.* A társadalom rossz irányban változik. Vagy arról van szó, hogy a régi hackerek egy sokkal védettebb, több támogatást nyújtó és hálásabb környezetben tevékenykedtek (például az MIT laboratóriumaiban, ahol mindenük megvolt, amit csak kívántak, és ráadásul még vezetőik és társaik elismerése is támogatta őket), vagy pedig arról, hogy tágabb közösségben léteztek (az ötvenes évek Amerikája), amely a mainál sokkal jobban épült a bizalomra és a becsületre.

> A hackerjelenség bonyolult és szerteágazó, és legalábbis valamennyi köze van a társadalom növekvő elidegenedettségéhez és ahhoz, hogyan találja meg a módját a kisember, hogy a maga számára is hasznosítsa a dolgokat. [37]

> Meggyőződésem, hogy a hackerek nem változtak. A társadalom viszont annál inkább, mégpedig negatív irányba. A régi idők hackereit a környezetük elismerte, amiért kísérleteztek, új dolgokat próbáltak ki. [38]

3. *A számítógépipart kiárusították.* A kereskedelmi szoftverek fejlesztői nem hisznek már a hackeretikában. Szabadalmaztatják a szoftvereket, féltve őrzik az adatokat és az algoritmusokat. Az új hackerek nem tesznek mást, mint hogy minderre reagálnak. Nem kellene azt tenniük, amit tesznek, ha a komputeripar a nyitott szabványokat, a szabadon hozzáférhető rendszereket és a nyílt forráskódokat tekintené a fejlődés irányának.

> Végül is nem marad más számomra, mint hogy levonjam a következtetést: a számítógépes forradalom véget ért, és az emberek vesztettek. A számítógépes közösséget már nem a tudásvágy hajtja, hanem a pénzéhség. A lángoló tekintetű, tudásukat mindenkivel megosztó programozók egykori kis cégeit felváltották a mamutvállalatok, amelyeket öltönyös, nyakkendős üzletemberek és szerzői jogi szakértők irányítanak. [39]

4. *Generációváltás.* Az új generációs hackerek, akárcsak a többi fiatal (Generation X), sokkal elidegenedettebbek, pesszimistábbak, önzőbbek, hanyagabbak és pragmatikusabbak. Nem a társadalom, a technológia vagy a számítógépes gyakorlat változott meg, hanem arról van szó, hogy az új hackerek egy olyan generációhoz tartoznak, amely másképp nevelkedett, mint az előző, és más hatások érték.

> A GenX tagjai sokkal önzőbbek, jóval valószínűbb, hogy a megszerzett információkat mindenekelőtt a saját érvényesülésükhöz vezető eszközként használják fel, és úgy érzik, hogy az idősebbek kib...nak velük… Így aztán nem meglepő, hogy másképp gondolkodnak, mint a Baby Boom-generációhoz tartozó elődeik. [40]

A régi etika tagadása

Érdekes megfigyelni, milyen módokon tagadják meg a kilencvenes évek hackerei az eredeti hackeretika normáit, vagy hogyan utasítanak el mindenfajta etikát. A tagadás fő tételei a következők:

1. *Csalás.* A hackeretika csalás, a régi hackerek agyszüleménye, túlságosan idealista ahhoz, hogy a gyakorlatban is működjön.
2. *Individualizmus.* A magányos individualisták általában nem követnek semmiféle közösségi etikát. Sok hacker úgy véli, hogy a hackelés eleve individualista, és nem csoportos gondolkodás eredménye. A hackertársadalom így inkább egymást támogató, megerősítő individuumok társasága, mint közös ideológia köré szerveződő közösség.
3. *Nem egy, hanem sok.* Nem létezik egyetlen hackeretika. Szélsőséges módon szemlélve: minden hackernek megvan a saját etikája.
4. *Profizmusellenesség.* Egy etikában általában szakmai követelmények is megfogalmazódnak. A hackerek eredendően profizmusellenesek, és jobbára tevékenységük során pontról pontra alakulnak szabályaik.
5. *Természetes evolúció.* A többi hithackeretikának idővel fejlődnie kell. Butaság lenne azt gondolni, hogy bárki fenntarthatja a régi etikát, ha minden más (különösen a technológiák) olyan elképesztő sebességgel változik.

Elemzési eredmények

A fenti szövegeket a NUDIST kódoló program segítségével elemezve arra a következtetésre jutottam, hogy a vizsgált huszonkilenc dokumentumból tizenötben, vagyis az összes ötvenkét százalékában vannak jelen mindkét etikai normarend elemei…

Jóllehet mindkét etika alapelemei megjelennek a szövegek többségében, valószínűtlen, hogy ez együtt vagy akár egy gondolaton belül történjen.

Következtetések

1. A kilencvenes évek hackerei nem etikátlanok. Nem ismeretlen számukra az eredeti hackeretika, ugyanakkor megvan a saját etikai rendszerük, amely a hatvanas évek hackeretikájának tételeit ötvözi néhány új elemmel. A hackerek jelentőséget tulajdonítanak az etikának – ez abból is látszik, hogy a crackereket és a rosszindulatú hackereket „negatív jelenségeknek” tekintik, olyanoknak, akik megsértik a normákat.
2. Négy területen érdemes vizsgálni a régi és az új hackeretika közötti változásokat. Annak felmérése, milyen mértékben fejlődött a két időszak között a számítógépes technológia, a társadalom, a komputeripar gyakorlata és a népesség különböző mutatói, magyarázatot adhat a hackerek ideológiai rendszerében bekövetkezett fordulatra.
3. Vannak hackerek, akik teljes egészében elutasítják az eredeti hackeretikát és egyáltalán bármilyen etika lehetőségét. Érdekes lenne megtudni, milyen személyes jellemzőik (kor, háttér, tapasztalat, nem, társadalmi osztály stb.) korrelálnak azzal, hogy vajon elutasítják a hacker etikát, vagy nem. Kell, hogy legyen valamilyen módszer arra, hogy megjósolható legyen, vajon egy hacker elfogadja vagy elutasítja az etikát.
4. A régi és az új hackeretika nem teljesen idioszinkratikus. Sok lényegi elemük hasonlít az amerikai kultúra és a demokratikus alkotmányosság ideáljaihoz, csakúgy, mint informális alapelvekhez.
5. A régi és az új hackeretika közötti hasonlóság arra utal, hogy az új hackerek nem egy, a régi hackerekétől független hagyományból táplálkoznak. Sőt az etikai folyto-

nosság demográfiai folytonosságra is utal. Nem lehet akkora különbség a hatvanas és a kilencvenes évek hackerei között, annak ellenére, hogy az idősebb generáció tagjai gyakran kijelentik: a fiatalabbak nem méltók a hacker névre.

Hivatkozások

(Az idézett szövegek weboldalakról, levelezőlistákról és internetes fórumokból származnak)

1. Rebels with a Cause (Okkal lázadók)
2. Revolt (Felkelés)
3. From Crossbows to Crypto (A számszeríjtól a kriptográfiáig)
4. Cryptoanarchist Manifesto (Kriptoanarchista kiáltvány)
5. Declaration of Grievances of the Electronic Community (Az elektronikus közösség panaszai)
6. The Manifesto (A kiáltvány)
7. Emmanuel Goldstein testimony (Emmanuel Goldstein tanúvallomása)
8. Hack Ethics (Hackeretika)
9. Hacker vs. Cracker (Hacker kontra cracker)
10. Jargon file – hacker ethic (Zsargonfájl – hackeretika)
11. Assert your rights (Ragaszkodj jogaidhoz!)
12. Emmanuel Goldstein testimony (Emmanuel Goldstein tanúvallomása)
13. Discussion begins (A párbeszéd kezdete)
14. Revolt (Felkelés)
15. Assert your rights (Ragaszkodj jogaidhoz!)
16. What is hacking? (Mi a hackelés?)
17. Pirate Newsletter (Kalóz Hírlevél)
18. Government ethic (Az állam etikája)
19. Jargon file - hacker ethic (Zsargonfájl – hackeretika)
20. The Manifesto (A kiáltvány)
21. Discussion begins (A párbeszéd kezdete)
22. Pirate Newsletter (Kalóz Hírlevél)
23. Pirate Newsletter (Kalóz Hírlevél)
24. Novice's guide to hacking (Bevezetés a hackelés titkaiba)
25. The Hacker's Code of Ethics (A hacker etikai kódexe)
26. Cracker subculture (Cracker-szubkultúra)
27. The Hacker's Code of Ethics (A hacker etikai kódexe)
28. The Manifesto (A kiáltvány)
29. Emmanuel Goldstein testimony (Emmanuel Goldstein tanúvallomása)
30. What is hacking? (Mi a hackelés?)
31. Ethics of Hacking (A hackelés etikája)
32. Government ethic (Az állam etikája)
33. What is hacking? (Mi a hackelés?)
34. The Hacker's Code of Ethics (A hacker etikai kódexe)
35. Discussion begins (A párbeszéd kezdete)
36. The Hacker's Code of Ethics (A hacker etikai kódexe)
37. Cracker subculture (Cracker-szubkultúra)
38. Digital Free Press #2 (Szabad digitális sajtó, 2. szám)
39. Discussion begins (A párbeszéd kezdete)
40. Anarchist's Guide to the BBS (Anarchisták kézikönyve a BBS-ekhez)