

Kibernetična kriminaliteta – (kiber)kriminološke in (kiber)viktimološke posebnosti »informatijske avtoceste«

Aleš Završnik*

Kibernetična kriminaliteta kot spremljajoč pojav »informatijske revolucije« in njenega najbolj slavnega proizvoda, internetne »informatijske avtoceste«, je zmuzljiv pojem. Poleg dilem, ki spremljajo kriminaliteto nasploh, je za kibernetično kriminaliteto značilna specifična narava prizorišča. Gre za virtualen prostor, kar vpliva na fenomenologijo kriminalitete in viktimitete. Prispevek se pri analizi kibernetične kriminalitete opira na družboslovne refleksije kibernetičnega prostora in kibernetične (proti)kulture, ki so pomembne za razumevanje kriminološko/viktimološke dvojice: storilcev in hekerske kulture ter žrtev in viktimoloških posebnosti. (Proti)kulturno ozadje kiberprostora sodi v miselne tokove postmodernistične teorije, saj so jima skupna vprašanja o posameznikovi identiteti ter vzgibih za iskanje skupnosti in oseb v internetnem prostoru. Prispevek zato obravnava vprašanje »prava o identiteti« v internetnem »laboratoriju za konstrukcijo identitete« in krajo identitete oziroma identitetno prevaro. Sledi prikaz kibernetičnih skupnosti, ki so posledica osvobajajočega potenciala kibernetičnega prostora, po drugi strani pa pacifikacija in izolacija osamljenih, v ekran boljšečih monad. Osrednji del je namenjen posebnostim viktimizacij kibernetične kriminalitete in kibernetičnim deviantom (»konzolnim kavbojem« ali hekerjem). Po analizi socialne konstrukcije hekerske dejavnosti in njenih akterjev prispevek prikaže ideološki boj za prevlado nad kibernetičnim prostorom: boj med protikulturnimi vrednotami, ki so vtakane v sam nastanek internetnega prostora, in vrednotami postmoderne »digitalnega kapitalizma«; boj za prevlado med računalniškim »podzemljem« in varnostno industrijo.

Ključne besede: kibernetična kriminaliteta, kriminologija, viktimologija, storilci, žrtve

UDK: 343.3/7:681.324

1. Uvod

Stopnja ranljivosti današnje »informatijske družbe« je še vedno precejšnja uganika: gospodarstvo, državna administracija in civilna družba so v veliki meri odvisni od učinkovitosti in varnosti moderne informatijske tehnologije. Za državni birokratski aparat in aparat nadnacionalnih tvorb, kot je Evropska unija, postaja medmrežje¹ več kot zgolj oglasna deska za predstavitev predlogov, razglas novosprejetih pravnih aktov, razpise programov pomoči, predstavitev shem organov ipd. Zdi se, da tovrstnim hipernormiranim »veleprojektom« ustreza ravno informatijska tehnologija in z njim povezan kibernetični prostor, ki omogoča nepregledno razraščanje sistema in s tem pravzaprav omogoča njegov obstoj. V gospodarstvu poteka večina denarnih transakcij prek računalnikov, ki avtomatično beležijo prilive in odlive denarnih tokov, njihove prerezpore-

ditve, upravljanje s sredstvi (npr. zastavo, rezervacijo) itd. Elektronsko poslovanje gospodarskih subjektov in vsakogar izmed nas je odvisno od varnosti sistemov za denarne transakcije po računalniških mrežah. Tudi proizvodnja je velikokrat v celoti odvisna od pravičnega delovanja podatkovnih sistemov in od shranjenih podatkov v elektronski obliki. Varnost pomorskega in zračnega kontrolnega sistema in drugih javnih infrastrukturnih sistemov (električnega sistema, telekomunikacijskega omrežja, zdravstvenega sistema itn.) je prav tako odvisna od računalniškega sistema. Ne nazadnje sta računalništvo in medmrežje nekaj, s čimer mlajše generacije prepričljivo »prehitvajo« starejše, njihova socializacija, izobraževanje in (zlasti) preživljanje prostega časa je veliki meri povezano z modernim računalniškim sistemom. Mednarodne računalniške mreže so tako postale živčevje gospodarstva, javnega sektorja in civilne družbe. V tem je torej razlog zavzemanja za varnost in pravno regulacijo računalništva in z njim povezanih mrežnih sistemov komunikacije, z eno besedo – kibernetičnega prostora.² Vendar, kako daleč in za kakšno ceno?

* Aleš Završnik, univerzitetni diplomirani pravnik, mladi raziskovalec na Inštitutu za kriminologijo pri Pravni fakulteti, Poljanski nasip 2, Ljubljana.

¹ V besedilu bodo pri strokovnih terminih v zvezi z računalniško tehnologijo v največji možni meri uporabljeni prevodi v slovenščino, tam kjer bi prevodi v besedilu povzročali nepotrebno zmedo, pa bodo uporabljeni termini v obliki, kot se pojavljajo v strokovni, tehnični rabi (t. j. v angleščini).

² Nakaj z uporabo kibernetičnega prostora povezanih statističnih podatkov: *število uporabnikov interneta*: 90.000 uporabnikov (jan. 1989), 500.000 (jan. 1991), 2.000.000 (jan. 1993), 7.000.000 (jan. 1995), 20.000.000 (jan. 1997), 70.000.000 (jan. 1999), 100.000.000 (jan. 2001),

Medmrežje nam je v veliki meri približala šele njegova komercializacija v začetku 90. let prejšnjega stoletja, a čas velikega buma njegove komercializacije, razcvet »(med)mrežne« oziroma »nove ekonomije« in njunih ožji spremeljevalk, t. i. *dot.com* ekonomije (ki poteka po zvezi – *on-line*), *e-businessa* oziroma vzpona »digitalnega kapitalizma« (Schiller) iz sredine 90. let prejšnjega stoletja je neizbežno za nami. To dejstvo nam daje večje možnosti za bolj umirjeno družboslovno refleksijo, ki je kljub umirjanju ekonomske sfere (še vedno) pod pritiskom skorajda dnevno porajajoče se tehnologije, ki je poročila vero v idejo o kibernetičnem prostoru (*cyberspace*) kot o možnosti novega nivoja eksistence. Smo torej v času, ko je libidinalna energija mita o zmožnosti informacijske in komunikacijske tehnologije (ICT – *information and communication technology*) za družbene transformacije v veliki meri usahnila, zato so (lahko) družbeno-psihološke refleksije o učinkih nove, tokrat »informacijske revolucije«, toliko bolj uravnoteženi.

V prispevku bomo prikazali nekatere družbene in psihološke določilnice kibernetičnega prostora, ki se zdijo nujni predpogoj pravnega urejanja dinamike vsakovrstnih (tudi kriminalnih) transakcij v tem novem »prostoru«. V skladu z načelom *ultima ratio societatis* pri uporabi kazenskopravnega interveniranja in načelom subjektivne odgovornosti je poznavanje psihičnih določilnic kibernetičnega prostora nujno za opredeljevanje mej dopustnega in (kazenske) odgovornosti vseh udeležencev v tem prostoru, t. j. uporabnikov, ki nastopajo v vlogi žrtve, internetnih ponudnikov (ISP – *Internet Service Providers*), uporabnikov, ki jim očitamo storilstvo kaznivega dejanja in odgovornosti države. V prispevku nas bodo zanimala predvsem širše družboslovne refleksije kibernetičnega prostora, ki so relevantne za razumevanje kriminološko/viktimološke dvojice: storilcev in njihove specifične kulture (t. i. hekerske kulture) in žrtev in viktimoloških posebnosti kibernetične kriminalitete.

2. Opredelitev kibernetične kriminalitete in sorodni pojmi/pojavi

Za lažjo orientacijo v »novem prostoru« bom uporabljal terminologijo družboslovnih tekstov, ki kot epistemološki rezi omo-

gočajo nadgradnjo za kriminološko in/ali viktimološko analizo. Tudi zato se ne bom omejeval le na morebitne pravne opredelitve posameznih deviantnih ravnanj, kot so določene v domači ali tuji pravni ureditvi. Pravna ureditev bo postavljena ob bok vsem drugim družboslovnim refleksijam kibernetičnega prostora.

Pojem računalniška kriminaliteta je izraz, ki se je najprej pojavljal v normodajnih aktih. Vsa prepovedana dejanja kibernetične kriminalitete so res povezana z računalniki, saj brez računalnika oziroma vsaj dveh računalnikov ni mogoče vzpostaviti njune povezave in s tem generiranja novega polja – virtualnega oziroma kibernetičnega prostora. Kljub temu pa je navedeni termin iz vsebinski in formalnih razlogov neustrezen. Zlasti gre za poimenovanje te vrste kriminalitete po uporabljenem sredstvu, kar običajno ni bila praksa. Kazenskopravna teorija³ predlaga uporabo pojma kriminaliteta v zvezi z računalniki (*computer-related crime*), ki upošteva dejstvo, da je računalnik »samo orodje v človekovih rokah«, vanjo pa uvršča vsa kazniva dejanja, pri katerih računalnik nastopa kot orodje ali kot predmet napada, za izvršitev ali poskus izvršitve kaznivega dejanja pa je potrebno določeno znanje iz računalništva ali informatike. Glede na pogoj, da ima storilec določeno znanje iz računalništva (tehnika informatike) ali informatike (uporabna informatika) nekateri predlagajo tudi uporabo pojma kriminaliteta v informatiki.⁵

Danes velja v literaturi besedna zveza računalniška kriminaliteta (in njene različice) za preozko. Računalniki oziroma njihovi osnovni elementi – mikroprocesorji so že skoraj povsod: v ročnih urah, gospodinjskih aparatih itd. Bistveni opredelilni element kibernetične kriminalitete je zato mreža, ki nastane s povezavo več računalnikov. Zato je primernejša uporaba pojma kriminaliteta informacijsko (tele)komunikacijske tehnologije (ICT – *information communication technology*). Načini, ki omogočajo povezovanje računalnikov v medmrežje pa so danes zelo razviti, od fiksnih⁶ do brezžičnih⁷ povezav.

Najprimernejši pojem za poimenovanje kaznivih dejanj v zvezi z računalniki in njihovimi mrežami je po našem mnenju

200.000.000 (l. 2002), cca. 1 milijarda (l. 2005) in cca. 2 milijardi (l. 2010). (vir: A. M. Rutkowski, *Center for Next Generation Internet*, 1999; povzemam po: Peter Grabosky: *Computer crime: a criminological overview*, str. 37; Manuel Castells: *The Internet Galaxy*, str. 3); *ustvarjen dobiček z e-poslovanjem (e-commerce)* (v milijardah ameriških \$): 3\$ (l. 1996), 22 \$ (l. 1997), 38\$ (l. 1998), 95\$ (l. 1999), 226\$ (l. 2000), 459\$ (l. 2001), 826\$ (l. 2002), 1.324 \$ (l. 2003), 1.976 \$ (l. 2004), 2.754\$ (l. 2005) (vir: Real Numbers Behind »Net Profits 1999«, ActivMedia Research LLC 1999; povzemam po: Peter Grabosky: *Computer crime: a criminological overview*, str. 38). Zgovorna je tudi primerjava z dosežanji tehnološkimi pridobitvami: medmrežje (www – World Wide Web) je potrebovalo 3 leta, da je doseglo svojih prvih 50 milijonov uporabnikov, televizija 15 let, radio pa 37 let. (Tako John Naughton: *A Brief History of the Future: The Origins of the Internet.*)

³ Glej Vid Jakulin: *Kazenskopravni vidiki računalniškega piratstva.*

⁴ Tako Bogo Brvar: *Pojavne oblike zlorabe računalnika*, str. 94.

⁵ Glej supra op.

⁶ Med fiksne povezave sodijo: telefonske povezave (*dial-up-modem* povezava, *ISDN-integrated services digital network*, *ADSL-asymmetric digital subscriber line*), širokopasovne (*broadband*) povezave, »trajne« povezave (*always-on connection*), kabelske povezave, dostopi prek LAN (*local area network*).

⁷ Brežžične povezave so: povezave prek WAP (*wireless application protocol*), ki ga uporabljajo PDA (*personal digital assistant*) naprave, kot so dlančniki, prenosni računalniki, pagerji in prenosni telefoni, povezave t. i. tretje generacije (3G), kot je UMTS (*universal mobile telecommunications system*), povezave prek Bluetooth (standarda za brezžično povezavo kratkega radijskega dometa), povezave prek Packet radio (PR), satelitske povezave, povezave prek WLAN (*wireless local area network*).

pojmem kibernetična kriminaliteta. Ta pojem upošteva, da gre za kriminaliteto v zvezi z računalniki, ki je storjena v kibernetičnem kontekstu (*cyberspace*). Druga pojma, ki se uporabljata za poimenovanje kibernetične kriminalitete sta še internetna kriminaliteta in virtualna kriminaliteta. Prvi pojem se nanaša na globalni internet oziroma medmrežje (*www – world wide web*), drugi pa na nov prostor, nastal s povezavo dveh ali več računalnikov. Pojma sta v uporabi v družboslovnih refleksijah, za uporabo na pravnem področju, zlasti kazenskem, na katerem velja postroženo načelo zakonitosti (*lex certa*), pa zaradi nedoločenosti nista primerna.⁸

Pojem informacijska kriminaliteta je širši od kibernetične kriminalitete, saj poleg računalniške kriminalitete zajema tudi področja brez računalnikov.

Pri urejanju civilnopравnih razmerij je zaslediti tudi pojem e-komunikacije, ki zajema tri področja: digitalno komunikacijo (televizija, telefon), digitalno obdelavo, zajem in shranjevanje tekstovnih podatkov (knjižnice) in digitalno obdelavo zvočno-slikovnih podatkov (video). Kriminaliteta v medmrežju spada po tej razdelitvi v del digitalne komunikacije.

⁸ V kibernetično kriminaliteto po Konvenciji Sveta Evrope o kibernetični kriminaliteti (*Convention on Cybercrime*) uvrščamo: protipravni dostop (*illegal access*), protipravno prestrazanje (*illegal interception*), motenje podatkov (*data interference*), motenje sistemov (*system interference*), zlorabo naprav (*misuse of devices*), računalniško ponarejanje (*computer-related forgery*), računalniško goljufijo (*computer-related fraud*), kazniva dejanja, povezana z otroško pornografijo (*offences related to child pornography*), kazniva dejanja, povezana s kršitvijo avtorske in sorodnih pravic (*offences related to infringements of copyright and related rights*). Vir: URL: <http://conventions.coe.int/treaty/EN/Treaties/Html/005.htm>. Na ta prvi multilateralni instrument, ki ureja kibernetično kriminaliteto, so vplivali pravni akti, ki jih je mogoče razdeliti v naslednje tri skupine: 1.) Priporočila EU: *Recommendation N° R (85) 10*, ki operacionalizira uporabo Evropske konvencije o vzajemni pomoči v kazenskih zadevah, glede prisluškovanja telefonskim pogovorom; *Recommendation N° R (88) 2* glede kršitev avtorske in sorodnih pravic; *Recommendation N° R (87) 15*, ki ureja zbiranje in uporabo osebnih podatkov za policijske namene; *Recommendation N° R (95) 4*, ki ureja zaščito osebnih podatkov na področju telekomunikacijskih storitev in zlasti telefonskih storitev; *Recommendation N° R (89) 9* glede kriminalitete povezane z računalništvom in navodil nacionalnim zakonodajalcem glede opredeljevanja kibernetičnih kaznivih dejanj in *Recommendation N° R (95) 13*, ki ureja določene kazensko-procesne pravne probleme povezane z informacijsko tehnologijo; 2.) Resolucije EU: *Resolution No. 1* evropskih ministrov za pravosodje (Praga, junij 1997), s katero podpirajo Evropski komite za probleme kriminalitete (CDPC) glede prizadevanja na področju kibernetične kriminalitete, z namenom usklajevanja nacionalnih kazenskih zakonodaj za učinkovitejše preiskovanje in mednarodno sodelovanje; 3.) Akcijski načrt Sveta Evrope (Strasbourg, oktober 1997), ki poziva države k iskanju skupnega odziva na razvoj informacijske tehnologije, osnovanega na vrednotah Sveta Evrope. Podrobnejša pravna analiza v: Cédric J. Magnin: *The 2001 Council of Europe Convention on cyber-crime: an efficient tool to fight crime in cyber-space?*, str. 42 in nasl.

Kibernetično kriminaliteto je mogoče obravnavati na dva načina. Za to področje je mogoče uporabljati obstoječa pravna pravila, ki jih je potrebno razširiti na novo področje. V tem primeru govorimo o medmrežju in pravu. Drug pristop, radikalnejši, pa izhaja iz dejstva, da gre pri kibernetični kriminaliteti za takšne (kvalitativne) novosti, da je za ta »prostor« potrebna oblikovati nova pravila. V tem primeru je govor o pravu interneta (*cyberlaw*, *Online-Recht*, *droit des reseaux*).

Temeljne (razlikovalne) značilnosti kibernetične kriminalitete so tehnična zapletenost (daje uporabniku občutek varnosti na eni in strah pred »velikim bratom« na drugi strani), hitrost sprememb, avtomatizacija, odprtost, brezmejnost in decentralizacija internetnega prostora (povečuje ranljivost in odpira možnosti za zlorabo), kriptografija (kot zaščita in hkrati ovira za odkrivanje storilcev). Novosti, ki jih vključuje pojem kibernetične kriminalitete, se torej pojavljajo na naslednjih ravneh: nov (virtualen) prostor (*crime scene*); deviantna ravnanja: stara v novi obliki (npr. tatvina podatkov) in povsem nova kibernetična dejanja (npr. *cracking*, *hacking*, napadi z virusi in črvi); nove metode za odkrivanje kaznivih dejanj (*law enforcement*) in nova pravila za določanje pristojnosti sojenja in kaznovanja: *e-jurisdikcija*, *e-kaznovanje*.

Za boljše razumevanje kibernetične kriminalitete, predvsem njenega psiho-socialnega ozadja, je koristno razumevanje temeljnih ontoloških konceptov kibernetičnega prostora, ki so nastali s kiberpunk (*cyberpunk*) gibanjem v 80. letih prejšnjega stoletja. Besedo kibernetični prostor (*cyberspace*) je skoval William Gibson z leta 1984 izdanim romanom *Neuromancer*, kar je desetletje pred nastankom svetovnega spleta (*www – world wide web*). Avtor je tako zasnoval jezik⁹ in imaginarij tega novega sveta še pred dejanskim nastankom prihajajoče »informacijske revolucije«. Zanimive so implicitne premise literarnega kiberpanka, ki je del znanstveno-fantastične kulture. Označuje ga namreč vera v tehnologijo in naraščajoč individualizem, »samodoločeno delovanje« (Kanduč), samooblikovanje in izbiranje identitnih pozicij glede na družbeni kontekst, nevraščanost in določenost s tradicijo. Gre torej za značilno postmodernistične značilnosti kiberpanka, ki se je v 90. letih prejšnjega stoletja razširil čez meje znanstveno-fantastične kulture v pojem kibernetične kulture (*cyberculture*). Izvor kibernetične kulture pa lahko najdemo že v revolucionarnih, protikulturnih 60. letih prejšnjega stoletja z uporabo znanosti in tehniki in v kasnejši transformaciji v 80. letih, ko se je to protikulturno gibanje (paradoksalno) združilo s tehnologijo, ki naj posamezniku nudi možnost pobega iz povečano nadzorovalne družbe. Kibernetična kultura ima v tem smislu

⁹ Pojmi, ki jih pripisujemo protikulturnemu kiberpankovskemu kontekstu, kot so klon, kiborg, simulaker, simulacija, matrika, hiperrealno itd. so večinoma nastali v umetniški produkciji, večinoma literarni in filmski, šele kasneje pa so prodrli v družbeno kritične (znanstvene) refleksije.

naboj težnje po svobodi, ki jo vedno bolj omejujejo veliki, nad-/transnacionalni sistemi, ki preraščajo in si podreajo nacionalne države, nastale na identitenih vzorcih kolektivnih entitet. Telesnost je v optiki kiberpankovske kulture dojeta le še kot »ječa lastnega mesa«.¹⁰

Literarni kiberpank kot anticipacija kibernetičnega prostora je tako blizu postmodernistični teoriji, ki jo označuje predvse bivanjskost subjekta, vprašanja njegove identitete, vprašanja kloniranih jazov, hiperrealnosti (Baudrillard) in simulakrov. Ta ontološka nestabilnost sveta in identiteta destabilizirata pa je eden izmed bistvenih psiholoških fenomenov kibernetičnega prostora in s tem tudi pomembna določilnica deviantnega ravnanja v tem prostoru.

3. Psihološka in psihoanalitična fenomenologija kibernetičnega prostora

Zastavili si bomo vprašanje, za katerega Jones¹¹ meni, da je pomembno pri raziskovanju specifične narave kibernetičnega prostora in njegovega vpliva na udeležence v tem prostoru: kakšni so posameznikovi vzgibi po iskanju skupnosti in oseb v internetnem prostoru oziroma, kdo smo, kadar smo povezani (*on-line*)?

3.1. Kibernetična realnost

Najbolj v oči bijoča posebnost kibernetične kriminalitete je njena pojavnost v neki drugi, virtualni realnosti. Slednjo pojmuje kot realnost, kjer naj bi bili vsi videni ali slišani objekti zgolj »simbolni«; niso niti fizični, niti niso nujno reprezentacije fizičnih objektov, ampak so lahko tudi simbolizacije objektov, ki so skonstruirane v tej realnosti. V Baudrillardovem jeziku bi dejali, da gre za simbolne reprezentacije drugega reda.¹² Vir-

¹⁰ Značilen odlomek iz romana *Nevromant*: »Za Casea, ki je živel le za breztelesno vzvišenost kiberprostora, je bil to Padeč. V lokalih, kamor je zahajal kot vrhunski (konzolni; dodal A.Z.) kavboj, so nekako zviška gledali na vse, kar je bilo povezano z mesenim. Telo je bilo meseno. Case je zdaj postal ujetnik lastnega mesa.« William Gibson: *Nevromant*, str. 10.

¹¹ Steven G. Jones: *The Internet and its Social Landscape*, str. 9.

¹² Francoski sociolog – poststrukturalist Jean Baudrillard, je avtor paralelnih umetnih resničnosti, konceptov kloniranja, implozije, simulacije, hiperrealnosti. Za našo predstavitev je pomemben koncept hiperrealnosti in sociološka teorija o simulaciji in simulakrih. Za njegov pojem hiperrealnosti je značilno, da ta ni nerealna, temveč tista realnost, ki je realnejša od samega realnega, je učinek stvari, postavljenih v umetno stopnjevanost, v ekstatično potenco. Hiperrealno tako sodi v področje simulacije (same) simulacije. Baudrillard loči tri redove simulakra: 1. naturalistične simulakre, osnovane na podobi, ki ciljajo na povrnitev ali na idealno stvaritev narave po podobi Boga; 2. produktivne simulakre, osnovane na energiji, moči, njeni materializaciji s pomočjo stroja; 3. simulakre simulacije, osnovane na informaciji, modelu, kibernetični igri z namero totalnega nadzora. Glej: Jean Baudrillard: *Simulaker in simulacija*, str. 143 in nasl.

tualno realnost tako označujeta fizična, geografska ločenost udeležencev in to, da namen njihovega sodelovanja ni nujno določen vnaprej, ampak je ta namen lahko povsem nov in se vzpostavi šele v virtualni realnosti.¹³ Specifična komunikacija, ki je bistvena za preučevanje kibernetičnega prostora (saj zato »informatijska revolucija«), podira zvezo med fizičnim kontekstom in družbeno situacijo; čas in prostor sta transcendirana, komunikacija označuje anonimnost »priklopljenec« ločenih od telesa, kar deinhirira, sproža občutja drznosti, osvobojenosti, nezmotljivosti. V tem smislu je kibernetična realnost podpornik narcisistične kulture (Christopher Lasch), patološke narcisoidnosti kot najbolj prilagojene osebnostne strukture v postmoderni družbi (Slavoj Žižek). Internet je performans, spektakl, kjer se predstavljamo in na novo izumljamo. Je ekran za projekcijo naše podobe, samokreacijo, prostor naracije o samem sebi, »a funclub to oneself« (Di Giovanna), zvezan s principom užitka in postmoderno potrošniško kulturo. Je torej postmoderna medij *par excellence*.

3.2. Kibernetična identiteta

Pomembna značilnost virtualne realnosti in komunikacije med njenimi udeleženci je njihova anonimnost. Ta pri uporabniku omogoča nastanek virtualne identitete. Internet je »laboratorij za konstrukcijo identitete« (Turkle), uporabniku je omogočeno, da pusti svojo identiteto, ki jo ima v vsakdanjem svetu, v sobi, kjer je računalnik, je prizorišče, kjer lahko »udejanji« (*act out*) svoj »resnični« jaz, želje in fantazije.

Preskok v drugo identiteto je zanimiv, ker nam razkriva naravo same identitete. Posamična »realna« identiteta je tako razgaljena kot nestalna, kontingentna. Očitno je, da identiteta ne obstaja kot ontološka kategorija, nekaj, kar je v »človekovi naravi« že v trenutku njegovega rojstva. Obstajajo le mehanizmi, ki posameznikom ponujajo različne identitete, in s tem povezani mehanizmi, ki subjektom ponujajo razloge za sprejemanje določenih identitet. Mehanizmi tvorbe identitet so zelo raznoliki, postopki produkcije identitet pa se nikoli ne »končajo«. Bistvo identitete je v njenem nenehnem revidiranju in samozanikovanju, identiteta ni zapisana v genih, ki bi jo imeli od rojstva do smrti in ni utemeljena v ničemer zunaj sebe. Gre za identitetno redefiniranje *ad infinitum*. Identiteta je proizvod interakcije, diskurza, komunikacije, zato vsaka diskurzivna situacija od nosilca zahteva, da vedno znova zavzame svojo identitetno pozicijo. Primer kibernetičnega prostora tako jasno prikaže, da je »petrifikacija« identitetne pozicije fikcija, saj je identiteta subjektu v bistvu tuja, nekaj, kar ni čisto njegovo.

Identiteta je tako nedvoumno družbeni proizvod, »skupinski projekt« (Crawford), projekt »biti specifična oseba« (Clarke). Vprašanje identitete je eno izmed glavnih tem postmoderne

¹³ Tadej Praprotnik: *Skupnost, identiteta in komunikacija v virtualnih skupnostih*, str. 6.

teorije, po kateri je subjekt razsrediščen, fragmentiran, brez fiksne in trdne identitete. Temeljna posebnost virtualnega, sintetičnega in tehnološkega kibernetičnega sveta pa je tudi v pojmu identitete.¹⁴ To ne pomeni, da v prejšnjih obdobjih identiteta ni bila problematizirana.¹⁵ Pomeni le to, da v tolikšni meri ni bila predmet dvoma, saj družbeni red ni dopuščal in omogočal radikalno drugačnih »preživetvenih strategij« posameznikov. V tem oziru pa je zlasti zanimivo proučevanje mehanizmov, ki si med seboj konkurirajo in posameznikom »vsiljujejo« posamične identitete. Eden izmed takih mehanizmov je tudi ideologija o osvobajajočem potencialu kibernetičnega prostora, v katerem lahko posameznik postane to »kar v resnici je«. Ideološkost tovrstnih sporočil je očitna. Sama narava identitete je namreč takšna, da nikoli ne more biti zares subjektova. Z identifikacijo z določenimi identitetami subjekt ne postaja vedno bolj »on sam«. Vendar, kdo potem je on sam, »kot takšen«? Na tem mestu se zdi naprimernejša razlaga, ki jo podaja lacanovska psihoanaliza. Po njej identiteta subjektu res ni lastna, ni njegov sestavni del, toda ravno ta neustreznost identitete s subjektivnim »resničnim bistvom« je konstitutivna za vznik samega subjekta. Ravno v kolikor subjekt ne pride do sebe, postaja subjekt. V tem je radikalna odtujitev subjekta od samega sebe, ki jo Lacan locira v fazo nastajanja jaza, v t. i. fazo zrcaljenja.¹⁶ To je razlog, da Lacan »jaz« pojmuje kot instanco samoprevar, samoodtujujočo instanco, preko katere si subjekt postaja tuj samemu sebi. Po Žižku, sam ta proces premikanja med mnogoterimi identifikacijami predpostavlja neke vrste prazno vez, ki omogoča preskok iz ene v drugo identiteto; in ta prazna vez je po njegovem subjekt sam.¹⁷ Lacanovsko rečeno, je identiteta, tako kot nezavedno, strukturirana kot govorica.

Identiteta je tako v kibernetičnem prostoru razgaljena. Ni trdna, temveč fluidna, amorfna in multidimenzionalna, zato so možne multiple identitete, identitetne manipulacije in spremembe. Konstrukcija identitete na netu je tako razpeta med igrivostjo in zlorabo.

3.2.1. Kraja identitete (*identity theft*)

Veliki pomen identitete v kibernetičnem prostoru se kaže tudi na kriminološko/viktimološkem polju. Kraja identitete

(*identity theft*) oziroma identitetna prevara (*identity fraud*) je tako značilna zlasti za prostor, ki ga označuje velika anonimnost. Pri kraji identitete gre za krajo osebnih identifikacijskih informacij in fraudolentno uporabo le-teh v (običajno) pridobitniške namene (npr. pridobitev zneska posojila, ki pa ga mora odplačati oškodovani). Za operacionalizacijo pojma identitete – kar pomeni uvajanje pojma kraje identitete – pa je potrebno diverzificirati njegove pomenske odtenke. V tem smislu je mogoče razlikovati več vrst identitet: individualno identiteto, družbeno identiteto in pravno identiteto.¹⁸ Individualna identiteta je subjektivna konstrukcija sebe, soustvarjena z refleksijami drugih in s posameznikovimi interakcijami z družbenim redom.¹⁹ Družbena identiteta je povezana z načinom, kako posameznik predstavlja sebe v družbi, kar jo loči od individualne identitete, ki je odvisna zlasti od načina, kako je posameznik dojet v družbi. Na ti dve identiteti lahko kraja identitete vpliva, čeprav teh dveh identitet v pravno-tehničnem smislu ni mogoče ukrasti. Ukrasti je mogoče le pravno identiteto. Ta je za razliko od prvih dveh precej trdna, saj gre pri njej za skupek karakteristik in znakov, ki omogočajo odgovor na dve vprašanji: »Kdo je ta oseba?« in »Ali je to ista oseba?«. ²⁰ Pri razliki med individualno identiteto in pravno identiteto gre tako lahko tudi za »krajo identitete«.

Glede na intenzivnost neujemanja med individualno identiteto in pravno identiteto v teoriji razlikujejo med več vrstami kraje identitete. Zlorabo informacij, ki so specifične za določeno osebo, z namenom prepričati druge, da gre za to osebo, je mogoče tipologizirati glede na tri spremenljivke:²¹ 1. trajanje, 2. stopnjo poglobljenosti oziroma intenzivnost posega v žrtvine osebne informacije in 3. motivacijo storilca. Pri trajanju kraje identitete gre lahko za enkratni dogodek ali za trajajoče celostno življenje v pravni identiteti drugega. Stopnja intenzivnosti posega je glede na množico podatkov, zbranih o posamezniku, v »informatizirani družbi« lahko vedno večja (npr. osebni podatki, bančni in finančni podatki, zdravstveni in socialni podatki itd.), tako da lahko ločimo med totalno krajo identitete, ki je običajno trajna, s katero subjekt začne novo (pravno) življenje, ubežniško krajo identitete (*escape identity theft*) ali delno, ki je običajno začasna in se nanaša le na nekatere vidike življenja (npr. nakup blaga s tujo kreditno kartico). Glede na motivacijo storilca pa lahko govorimo o kriminalni kraji identitete, če gre za uporabo tujih podatkov z vednostjo in namenom storiti nezakonito dejanje v imenu žrtve.

¹⁴ Glej še Richard Bartle: *Designing Virtual Worlds*, str. 159.

¹⁵ V kiberpankovskem romanu *Nevromant* Williama Gibsona je vprašanje identitete prikazano na naslednji način: »Prav nič ne pomeni, če gresta vidva z Gladkim še tako globoko s tistim kitajskim virusom, če tale zadeva ne sliši prave besede.« »In kakšna je ta beseda?« »Ne vem. Lahko bi rekel, da me to, da ne vem, prav določa, ker ne morem vedeti. Sem tisto, ki ne more vedeti besede. Tudi če bi ti vedel in bi mi povedal, jaz ne bi mogel vedeti. Tako imam vse zvezano. Nekdo drug jo mora zvedeti...« »Kaj se zgodi potem?« »Potem mene ni več. Neham obstajati.« Str. 189.

¹⁶ Bice Benvenuto, Roger Kennedy: *The Works of Jacques Lacan: An Introduction*, str. 145.

¹⁷ Slavoj Žižek: *Kiberprostor ali neznosna zaprtost bivanja*.

¹⁸ Tako Emily Finch: *What a tangled web we weave: identity theft and the Internet*. V: Yvonne Jewkes et al.: *Dot.cons: Crime, deviance and identity on the Internet*, str. 87.

¹⁹ Zanj velja vse, kar smo o pojmu identitete razčlenili zgoraj.

²⁰ Glej John Torpey: *The Invention of the Passport: Surveillance, Citizenship and the State*, str. 166.

²¹ Tako Emily Finch: *What a tangled web we weave: identity theft and the Internet*. V: Yvonne Jewkes et al.: *Dot.cons: Crime, deviance and identity on the Internet*, str. 90.

Kraja identitete je bila ob koncu 20. stoletja označena kot »najhitreje rastoča kriminalna dejavnost« (npr. zlasti pri *on-line* finančnem poslovanju). Glede na to oceno, dejstva, da informacije iz preteklosti danes »vztrajajo«, čeprav bi bile sicer pozabljene, in dejstva, da je informacija o žrtvi osnova kraje identitete, informacijska tehnologija s hitro obdelavo velike količine osebnih podatkov povečuje priložnosti za storitev tovrstnih kaznivih dejanj. »Informacijska revolucija« je tako proizvedla informacijske karceralne mreže, ki se zategujejo in generirajo strukturne pritiske k proizvodnji vedno novih osebnih podatkov. Povečane zahteve po identifikacijah so tako neposredni vzrok povečanja kaznivih dejanj kraje identitete, saj prevladuje skoraj obsesija po osebnih podatkih: (včasih) antropometrija (merjenje telesa), obvezna fotografiranja obraza, registracija rojstev, smrti, skupnega življenja, kraja bivanja in drugi podatki za »potrebe« socialne države, ki potrebuje vedno več evidenc.²² Gre za proces fiksiranja identitet posameznikom, »etos identifičnosti«. Danes pa so skušnjave po zbiranju podatkov še večje, zlasti biometrija (»znanost na pohodu«) omogoča merjenje prstnih odtisov, očesnih mrežnic, DNK, geometrijo roke (skeniranje dlani)²³ itd., kar vodi k privlačnosti in večji invazivnosti kraje identitete.

Večina pravnih ureditev ne pozna tatvine identitete kot samostojnega kaznivega dejanja, kar pomeni, da je eventualno tovrstno dejanje mogoče pravno kvalificirati kot goljufijo (seveda z izpolnjenimi ostalimi znaki za to kaznivo dejanje). V pravnih ureditvah, kjer je tatvina identitete samostojno kaznivo dejanje, pa je ta vezana na storilčev namen, da uporabi osebne identifikacijske podatke za storitev kaznivega dejanja (takšna je ureditev po *Theft and Assumption Deterrence Act* iz 1998 v ZDA) ali pa je osredotočena na premoženjske posledice, ki jih utрпи žrtev (takšna je ureditev po *Theft Act* iz leta 1968 v Veliki Britaniji).

3.2.2. Pravo o identiteti?

Danes najbolj pogosta oblika digitalne identitete je elektronski poštni naslov (*e-mail address*) in elektronska pošta postaja že običajen komunikacijski kanal. Zaznati je torej nek trend vedno večjega pomena *on-line* identitete, zato se postavlja vprašanje, ali potrebujemo »pravo o identiteti«? Zakonodajalčevo »centralno« pravo o identiteti ali »listina svoboščin« zaradi kontingentne narave identitete skoraj ni mogoča, možna pa so zasebna pravila, pravila uporabnikov, ki so odvisni od nemotnega upravljanja z *on-line* identiteto in zaščiteni pred posegi v njihove *on-line* identitete.

²² Glej John Torpey: *The Invention of the Passport: Surveillance, Citizenship and the State*, str. 19.

²³ V ZDA po tem principu deluje letalski sistem INPASS (*Immigration and Naturalisation Passenger Accelerated Service System*) za hitrejšo vkrčevanje, pri katerem potnik vstavi pametno kartico, v kateri je shranjena slika njegove dlani, svojo dlan pa položi na skener – če se podobajeta lahko potnik nadaljuje pot. Sistem je prostovoljen. Zaenkrat.

Že danes lahko rečemo, da imajo *on-line* identitete v lasti posredniki – podjetja, ki ustvarjajo kibernetične prostore. Zaenkrat so to podjetja, ki ustvarjajo prostore za igre,²⁴ kasneje pa je zaradi vedno večjega dojemanja javnega spleta (*www*) kot »divjega zahoda« pričakovati razvoj zasebnih spleto. Ti posredniki so vir pravil že danes in imajo vse pravice do izklopa posameznega uporabnika zaradi kršitve njihovih pravil. Ker so ti ponudniki zasebniki, gre za pogodbeno pravo,²⁵ kar pomeni, da je uporaba sile v kiberprostoru privatna zadeva. Tovrstno diverzifikacijo javnega in zasebnega pospešuje tudi vedno večja privatizacija interneta in privatno upravljanjih mrež, ki naj preprečijo vstop nezaželenim vsebinam (virusi, prekomerno pošiljanje poštnih sporočil,²⁶ nameščanjem vohunske programske opreme²⁷ ipd.). Tudi na področju kibernetičnega prostora se na ta način s »filtriranjem« nezaželenih vsebin in omogočanjem dostopa do željenih vsebin ustvarja enklave, ograjene vrtove s privatno upravo, ki med seboj tekmuje za klientelo.

Oblikovanje identitet v fizičnem svetu se od oblikovanja identitete v virtualnem svetu razlikuje v vlogi skupnosti. V fizičnem svetu je vloga skupnosti implicitna, skrita, medtem ko v virtualnem svetu to oblikovanje identitete s strani skupnosti v celoti postane eksplicitno. 'Bogovi' *online* sveta so tako ljudje, ki vodijo ta svet, ki oblikujejo kode, ki poganja ta svet, zato se v teoriji v glavnem zavzemajo za kolektivno lastništvo *on-line* prostora.²⁸

3.3. Kibernetične skupnosti

V kibernetični realnosti udeleženci oblikujejo kibernetične skupnosti. Te skupnosti naj bi bile družbeno dovršene možnosti bivanja, ki ponuja lažnejše in (skorajda) čudežno življenje, možnost, da decentralizirane mreže omogočijo posameznikom povezavo in izgradnjo transparentnega političnega sistema brez birokratske državne oblasti. Takšen je pogled zagovornikov osvobajajočega potenciala kibernetičnega prostora. Vendar vedno bolj postaja očitno, da tehnologija, ki naj bi nam v prvi vrsti izboljšala kakovost življenja, slabi naše socialne vezi, interakcijo z drugimi ljudmi. Atomiziranost postmoderne družbe pa zato tudi (in še zlasti) v kibernetičnem prostoru vzbuja željo po povezanosti. V tej smislu gre za »lakoto« po skupnosti, ki jo začne človek graditi takoj, ko se mu odpre nov prostor. Gre za strah pred praznim prostorom nepripadanja, za grozo pred

²⁴ Kot je npr.: <http://www.everquest.com>.

²⁵ V primeru *Noah v. AOL Time Warner, Inc.*, 261 F. Supp.2d 532 (E.D.Va. 2003) je tožnik trdil, da AOL (*America Online*) krši njegove pravice iz 1. amandmaja s tem, ko je zaprla njegov račun kot odgovor na njegova pro-islamska sporočila; sodišče je odločilo, da AOL ni državni organ in se zato nanj 1. amandma ne nanaša.

²⁶ T. i. *spamming* (pošiljanje nezaželenih reklamnih sporočil) in *flooding* (poštni napad ali zasutje poštnega predala s sporočili).

²⁷ *Spyware*.

²⁸ Glej Susan P. Crawford: *Who's in Charge of Who I am?: Identity and Law Online*.

padcem v Lacanovo Realno, Freudovo »grozljivo« (*Das Unheimliche*), ki je posameznikov motiv za sprejemanje posameznih idenitet v kibernetičnem prostoru in zunaj njega. Druga plat uporabe računalnikov,²⁹ ki je diametralno nasprotna ideji osvobajajočega potenciala kibernetičnega prostora, pa predstavlja dejstvo, da je zgolj za oblikovanje kibernetičnih skupnosti znotraj računalniške strojne opreme, kar zreducira posameznike na izolirane, osamljene v monitor boljšeče monade, ki na koncu koncev niti ne vedo s kom komunicirajo (»resnično« ali neresnično osebo, državnim agentom, ki združuje več »resničnih« oseb hkrati, morda računalniškim programom itd.).

Kibernetične skupnosti so s kriminološkega vidika zanimive zaradi relativizacije konvencionalnih moralnih imperativov, transformacije deviantnih ravnanj v nedevidentna, njihove normalizacije in destigmatizacije storilcev. Uporabniki, ki bi bili sicer v fizičnem življenju ogroženi, zlasti statusno ali identitetno, imajo v kibernetičnem prostoru možnost, da se povežejo in oblikujejo lastne skupnosti.³⁰ Na ta način se prakse običajno dojele kot transgresivne prelevijo v družbeno sprejemljive. Informacije krožijo v teh skupnostih brezplačno, zato so v tem smislu izvorno zveste internetni ideji o »darovalni ekonomiji« (*gift economy*, Rheingold), po kateri nobena programska rešitev ni bila namenjena materialnemu okoriščenju posameznega programerja, temveč programski (hekerski) skupnosti kamor je programer posredoval svoj izdelek v morebitne dopolnitve (ideja odprto kodnega sistema).

Nadaljnja posebnost kibernetičnih skupnosti je v tem, da si same oblikujejo minimalna etična pravila primerne obnašanja (*netiquette*). Regulativna funkcija v kibernetičnih skupnosti tako poteka prek več nivojev. Demokratičen potencial ima velika vloga uporabnikov (*netizens*), samoregulacija in na ta način oblikovani kolektivni etos. Teorija kibernetičnega prostora pripisuje pomembno regulativno vlogo tudi industriji (zlasti zaščitne programske opreme) in drugim interesnim skupinam (npr. *Internet Watch Foundation*, *Cyberangels* itd.). Vloga

državnih organov (»kiberpolicije«) je manjša, ti se ukvarjajo predvsem z enkripcijo, digitalnim »jemanje prstnih odtisov« za zaščito avtorskih pravic in patroljiranjem po internetu.

Kibernetične skupnosti so zaradi opisanih demokratičnih potencialov »preživetvene strategije« pripadnikov raznovrstnih manjšin. Zlasti feministke pa ugotavljajo, da se na internetu, kljub osvobajajočem potencialu, perpetuirajo ustaljene neenakosti. Poleg tega gre seveda pri participaciji v kibernetičnih skupnostih za vprašanje, kdo sploh ima dostop do tega prostora. Glede na družbeno-ekonomski položaj gre namreč večinoma za dobro stoječi, »normalni«, potrošniško naravnani srednji sloj, kateremu je bila komercializacija interneta v 90. letih prejšnjega stoletja tudi namenjena.

Ta hkratna demokratičnost interneta in njegova perversnost je dobro razpoznavna na primeru uporabe *on-line* pornografije³¹ in prostitucije.³² Slednja naj bi pomenila možnost drugačne razporeditve moči pri plačnem seksu, možnost za novo reprezentacijo in večjo kontrolo žensk pri samoreprezentaciji. Enakost pri dostopu do pornografskega gradiva *on-line* pa naj bi tudi ženskem omogočila dostop do vsebin, pri katerem se jim ni treba »razgaliti«, tvegati s stigmatizacijo in fizično ogroženostjo ter razvoj vsebin, ki predstavljajo ženske libidinalne interese. Anonimnost in možnost eksperimentiranja v varnem zavetju doma, zlasti tudi učinek breztelesnosti interneta in z njim povezanosti osvobojenosti od družbenih zapovedi telesnega videza, omogoča ženskam osvobajanje od patriarhalnih spon. Perversnost interneta na primeru uporabe *on-line* pornografije pa je v tem, da njegovi osvobajajoči učinki hkrati pomenijo nevarnosti, da imajo dostop do vsebin otroci, da se olajšuje otroška pornografija ipd. Tovrstne transgresije brez škode za identiteto in status, pohodi v seksualno »drugost«, tehnike komuniciranja v anonimnih klepetalnicah (*chat-rooms*), so tehnike, ki omogočajo »reševanje obraza« (*saving face*), so prostor za vajo družbenih vlog, ki jih bodo uporabniki morda kasneje odigrali v »resničnem« življenju. Dihotomija interneta (demokratičnost in perversnost) je dihotomija njegove rabe. Morda je preučevanje seksualnosti v kibernetičnih prostorih toliko bolj privlačno, ker je po eni strani to področje, ki ga je sicer izrazito težko empirično raziskovati zaradi nepripravljenosti udeležencev, po drugi strani pa je seksualnost bolj fluidna in je zato eksperimentiranje na seksualnem področju bolj pogosto; svoboda menjave vlog je draž kibernetičnega seksa – spremenljivke, kot so starost, spol, rasa, etnično poreklo, neverbalna komunikacija, glas, obleka, postava in tudi fizična nezmožnost, so namreč stvar izbire.

²⁹ Tako Slavoj Žižek: *The Plague of Fantasies*, str. 138.

³⁰ Npr. spletna stran *Punternet*, ki povezuje uporabnike storitev prostitutk (glej Yvonne Jewkes et al: *Dot.cons: Crime, deviance and identity on the Internet*, str. 41–51.), ali skupnosti za sklepanje »paktov smrti« po internetu na Japonskem (t. i. *cyber suicides*). Pri slednjem gre za fenomen, ko se povežejo v skupine (2-7) ljudje, ki si niso blizu in prebivajo v različnih predelih države, z namenom skupno storiti samomor. V skupini predvsem zato, ker jim je tako lažje in je manj verjetnosti, da si bodo premislili v zadnjem trenutku. Gre za specifičnost japonske kulture, ki pretendira k hierarhični organiziranosti, tako da se oblikujejo šibke individualne identitete. Reakcije policije na Japonskem so panične, tako da zapirajo spletne strani, kar pa nima smisla, ker si uporabniki pomagajo s stranmi, odprtimi na serverjih v tujini. Paradoksalnost tovrstnih skupnosti je tudi v tem, da tovrstne strani postajajo forumi za pomoč ljudem v stiski, ki tako dobijo prostor, kjer lahko spregovorijo o svojih težavah. (Več v: Richard Lloyd Parry: *Suicide, the net and death with a stranger*.)

³¹ Po nekaterih ocenah so bile pornografske storitve »zagonsko go-rivo« komercialne rabe interneta.

³² Povzemam po Yvonne Jewkes et al: *Dot.cons: Crime, deviance and identity on the Internet*, str. 36 in nasl.

3.4. Čustvena inflacija

Pri obravnavi psihološke fenomenologije kibernetičnega prostora ne moremo mimo čustev. Čustvena inflacija (Jones) kibernetičnega prostora je fenomen, ko ima udeleženec kiberprostora veliko poznanstev, ki jih lahko sklepa z ostalimi udeleženci (npr. v klepetalnicah,³³ s sodelovanjem na forumih itd.), za katera je značilna čustveno ohlapna povezava. Možnost hitro najti novega znanca namreč udeleženca v kibernetičnem prostoru spodbuja k temu, da znanstva hitro sklepajo in prav tako hitro opuščajo. To udeležencem omogoča narava same skupnosti, ki je določena le z besedno ravno. Udeležencu, ki vstopa v skupnost, njegov položaj in njegova vloga nista predoločena. Tako se generira občutek, da posameznik ne pripada skupnosti, temveč, da skupnost pripada njim.³⁴ Po drugi strani pa ravno ta množičnost osebnih vezi onemogoča sklepanje pravih osebnih vezi. Temeljno za osebno vez je ravno njena izključevalna narava – ko smo z vsemi hkrati, v bistvu nismo z nikomer.

V kibernetičnem prostoru je zanimiv fenomen komercializacije emocionalnosti in intimnosti, ki se kaže pri storitvah, povezanih z iskanjem partnerja (*on-line dating* oziroma *cyberdating*) in tudi otrok. Problemi obstoječih družb (patriarhalnost, kolonializem) se tako prenašajo in perpetuirajo tudi v kibernetičnem prostoru.

3.5. Psihoanaliza in kiberprostor

Osvobojenost od telesnosti naj bi v kibernetičnem prostoru zagotavljala emancipacijske učinke. Tako naj bi npr. virtualne »zmenkarje« (*on-line dating* oziroma *cyberdating*) udeležence osvobajale od siceršnjih spon »telesnosti«, zaradi katerih se v kibernetičnem prostoru počutijo bolj sproščene. Raziskave³⁵ kažejo, da so zlasti dekleta »uporabnice« *on-line* »zmenkarij«, ker se v takem prostoru počutijo prijetneje. Na ta način lažje odpravijo strah, ki je povezan z zavrnitvijo, po drugi strani pa so lahko bolj agresivne in lahko bolje izražajo svoja čustva. Na prvi pogled to potrjuje tezo o osvobajajočem potencialu kibernetičnega prostora. Po drugi strani pa je očitno, da »pravi« problemi še vedno ostajajo nerešeni, potlačeni. Dekleta se s prikrivanjem »telesnosti« samega diktata estetskih zapovedi ne znebijo, temveč ga udeležajo na prikrit način. Gre za reprodukcijo seksizma, saj dekleta tudi v *on-line* zmenku pogosto reproducirajo izven-kibernetične hegemonске vzorce »lejšega spola«.

³³ Najbolj znan je IRC (*Internet Relay Chat*) komunikacijski program, ki ga je napisal Jarkko Oikarinen na univerzi v Ouluju na Finskem l. 1988. Bistveno zanj je, da omogoča komunikacijo med več sto »klepetalci« hkrati, ki z vzpostavitev svojega kanala sami ustvarjajo svoje skupnosti. Več o tovrstni komunikaciji: Tadej Praprotnik: *Skupnost, identiteta in komunikacija v virtualnih skupnostih*, str. 104.

³⁴ Steven G. Jones: *The Internet and its Social Landscape*.

³⁵ Glej npr. Lynn Schofield Clark: *Dating on the Net: Teens and the Rise of »Pure« Relationships*.

Kako je torej z zatrjevano večjo stopnjo osvobojenosti udeležencev, ki se gibljejo v kibernetičnem prostoru? Ključno vprašanje pri analizi kibernetične realnosti je torej: za kakšno novo realnost pravzaprav gre in kaj je pri njej tako novega? Že pri dosedanjem navajanju smo ugotovili, da gre v kibernetični realnosti za reprodukcijo vzorcev, vrednot, stereotipov, predsodkov v nov prostor, po drugi strani pa udeleženca kibernetičnega prostora npr. njegova »telesnost« ne predeterminira. Kljub temu pa mu to še ne zagotavlja večje stopnje osvobojenosti. Kje je potemtake osvobajajoč potencial kiberprostora? Vprašanje identitete kot eno izmed osrednjih tem postmodernega diskurza se tiče samega bistva konceptualizacije subjekta. V tradicionalni vrednostni optiki obstaja nek zamrznjen konglomerat ponotranjenih vzorcev, vlog, shem, stereotipov, vrednot, ideologije, ki jo subjekt dojema za svojo. V kibernetičnem prostoru pa subjekt spozna, da identiteta ni nekaj vnaprej določenega, kar pridobi z rojstvom, temveč je »nekaj« kar (vsakodnevno) v interakciji z drugimi vedno znova (re)definira. Kibernetični prostor tako odstira, seje dvom v prepričanje, da obstaja neka ontološko dana identiteta. V tem smislu Turkle³⁶ zoperstavlja dve možnosti ravnanja s težavami z »resničnega« sveta v kibernetičnem svetu: »udejanjanje« (*acting out*) in »pre-delava« (*working through*). V prvem primeru subjekt zgolj sledi ubežniški logiki in »udejani« (*act out*) težave »resničnega« življenja v kibernetični realnosti. V drugem primeru pa uporablja kibernetični prostor, da si ozavešči nekonsistentnosti v lastnih identifikacijah in jih predela. V tem primeru tako lahko računalniški zaslon (kibernetična realnost) deluje kot psihoanalitik, saj preko njega suspendiramo simbolna pravila, ki regulirajo naše aktivnosti v »resničnem« življenju in tako eksternaliziramo potlačene vsebine, s katerimi se sicer nismo zmožni soočiti.

Na podlagi navedenega lahko razločimo vsaj tri poglede na kibernetično realnost. V psihoanalitičnem pogledu je zanimiv pogled na kibernetični prostor, po katerem se imaginarno prekrije z realnim, kar je zaznati pri Baudrillardu.³⁷ Po tem pogledu subjekti v kibernetičnem prostoru nazadujejo v pred-simbolno psihotično stanje stopljenosti z materinsko Stvarjo. Kibernetični prostor je tako mesto psihične regresije v simbiotično stanje, ki ga ponazarja lacanovsko imaginarno, ki je mesto uživanja, domišljije in fantazije.

Drug pogled poudarja osvobajajoči potencial kiberprostora. Njegova temeljna ideja je, da lahko v kibernetičnem prostoru zavzemamo različne spolne in družbene identitete, kar nas osvobaja prijema patriarhalnega zakona in bioloških okovov. Na ta način kiberprostor spodbuja ideologijo ustvarjanja samega sebe in iskanja odgovora na subjektivno dilemo o lastni identiteti. Gre za prehod od strukturne simbolne kastracije k

³⁶ V. Sherry Turkle: *Life on Screen: Identity in the Age of the Internet*. Povzemam po Slavoj Žižek: *The Plague of Fantasies*, str. 138.

³⁷ Glej še: Paul Virilio: *Hitrost osvoboditve*.

novi post-ojdipski libidinalni ekonomiji. V to skupino lahko uvrstimo tudi tehnične navdušence in druge zagovornike kibernetičnega prostora, ki jih družijo mistično/religiozna vizija o boljši prihodnosti v kibernetičnem prostoru. V tem smislu je mogoče govoriti o sublimaciji in investiranju naših pričakovanj v tehnologijo in z njo povezanim nastankom kiberprostora. Kibernetični prostor je s tem utelešenje pričakovanj in mitov našega časa.^{38, 39}

Po tretjem pogledu na kiberprostor, ki ga podaja Žižek,⁴⁰ oba navedena pogleda na kibernetični prostor zgrešita poanto, ker danes v nekem smislu »Drugi ne obstaja več«. Ta odsotnost Drugega se kaže v pojavu vznikanja etičnih komisij, ki naj kot »mali veliki Drugi« razrešijo etične zagate na raznih novih področjih, kot npr. v medicini in biogenetiki, nadalje v pojavu »kulture pritožb«, ko subjekt s tožbo histerično od Drugega zahteva utemeljitev svoje lastne eksistence, v vznikanju verskih fundamentalizmov itd. Kot protiutež umiku velikega Drugega se tako pojavljajo različne oblike velikega Drugega, ki obstaja v Realnem. Vero v velikega Drugega v Realnem pa Žižek označi kot definicijo paranoje. Gre za nezaupanje v red simbolnih funkcij, združeno z vero, da obstaja neki »Drugi (od) Drugega«, ki vleče niti našega dogajanja.

Glede kibernetične identitete pa Žižek⁴¹ meni, da internet kljub vlogam, ki jih igramo na njemu, omogoča obdržati »resnično« samopodobo. Virtualna podoba, ki jo gradimo, je zunanja in ločena od »resničnega« mene, na internetu pa lahko vsaj za kratek čas pozabimo nase, se odpočijemo od nenehnega »stika s samim seboj«, spočijemo od tega, da smo polno odgovorni za svoja dejanja. Po drugi strani pa smo lahko v

virtualni podobi, ki jo izgradimo na internetu, bolj »mi sami« kot smo v fizičnem svetu, saj odkrivamo vidike naše identitete, ki si jih v »resničnem« življenju nikoli ne bi upali niti priznati, saj bi sprejem tovrstnih vidikov identitete vodil v dezintegracijo naše biti. Na ta način je mogoče sprožiti »deinhibi-cijski efekt« (Suler), ki omogoča sprožiti mojo »temno stran in povnanjiti ves moj libidinalen potencial«,⁴² s čimer moj »elektronski id dobi krila.«⁴³

3.6. Posebnosti razmerja subjekt-subjekt in subjekt-stroj

V kibernetični realnosti prihaja v komunikaciji do transformacije jezikovne rabe, ki je posledek omejenosti komunikacije na pisano besedo. V običajni neposredni komunikaciji namreč sogovornik spremlja še kopico drugih – neverbalnih sporočil, ki mu jih sporočevalec hote ali (pogostejše) nehote sporoča. V kibernetičnem prostoru se tako razvijajo dopolnitve besedilne komunikacije. V jeziku zaradi potrebe po hitrosti sporočanja idej in misli zlasti v sinhroni komunikaciji (*real-time chat*) prihaja do skrajševanja besed in pisanje inicialk (npr. BTW (*by the way*) – mimogrede, C U (*see you*) – se vidimo, R (*are*) – si/ste). Besedam se pogosto dodajajo reprezentacije psihičnih stanj (npr. *smileys* – smeški, kot so: ☺ ali :-)) (nasmech), ☹ ali ;-((žalost), @}---- (roža) itd.). Zaradi večje učinkovitosti komunikacije pa se tudi v kibernetičnem prostoru razvija sistem socialnih sankcij za udeležence, ki motijo sožitje in normalen potek komunikacije (*netiquette*). Zaradi najpogostejše uporabe angleščine med »nativnimi« in »nenativnimi« govorniki pa se tudi sama angleščina razvija v t. i. *net-work* angleščino.

Interakcija uporabnikov s tehnologijo ni zanemarljiva. Kljub temu, da ne moremo govoriti o odnosu subjekt-subjekt, raziskovalci ugotavljajo nekatere značilnosti človeškega odzivanja na tehnologijo, kot da bi šlo za prave ljudi. Z računalniki se tako pogovarjamo, jih rotimo, malikujemo itd. V tem smislu gre za preučevanje, ki združuje različna področja, kot so družbene vede in tehnologija, oblikovanje in psihologija.⁴⁴

³⁸ Vincent Mosco meni, da je eden izmed pglavitnih mitov računalniške komunikacije mit, da bo ta pomenila epohalno transformacijo subjektive izkušnje. Subjekt bo lahko transcendiral čas, kar se odraža v »koncu zgodovine« (Fukuyama), transcendiral bo prostor, kar se odraža v koncu geografije in moč, kar se odraža v koncu politike in ekonomije (nastanek t. i. »mrežne ekonomije«). Ugotavlja, da so bila tovrstna pričakovanja investirana že pred vznikom računalniške revolucije v telegrafsko revolucijo, v revolucijo elektrike, telefona, radija in televizije. Vse te »revolucije« so nekoč inspirirale velike vizije družbene transformacije, danes pa vsi ti tehnični dosežki niso več sublimni. To pa po njegovem ne pomeni, da nimajo družbene in ekonomske moči. Šele takrat, ko tehnologije prenehajo biti sublimne mitološke ikone in vstopijo v prozaičen svet banalnosti, postanejo pomembne sile za družbene in ekonomske spremembe. (Vincent Mosco: *The Digital Sublime: Myth, Power, and Cyberspace*.)

³⁹ Privlačnost kiberprostora nazorno prikaže kiberpankovski prvenec *Nevromant*: »Caseu je bilo štiriindvajset let. Pri dvaindvajsetih je bil eden najboljših kavbojev v Sprawl. ... Zaradi mladosti in sposobnosti je bil skoraj ves čas v stanju adrenalinskega vzburjenja, priključen na predelan kiber-stolp, ki je projiciral njegovo breztelesno zavest v skupno halucinacijo, matriko.« William Gibson: *Nevromant*, str. 9, poudarke dodal A.Z.

⁴⁰ Glej Slavoj Žižek: *Kiberprostor ali možnost prekoračiti fantazmo*.

⁴¹ Slavoj Žižek: *The Plague of Fantasies*, str. 127 in nasl.

⁴² Supra op., str. 137.

⁴³ Sherry Turkle: *Life on Screen: Identity in the Age of the Internet*. Povzemam po Slavoj Žižek: *The Plague of Fantasies*, str. 137, op 15.

⁴⁴ Primer tovrstnega preučevanja je delo avtorja Clifforda Nassa in Scotta Braveja, *Wired for Speech: How Voice Activates and Advances the Human-Computer Relationship*, v katerem prepričljivo demonstrirata, da se ljudje aktiviramo z glasom (*voice-activated*), da se odzivamo na glasove, ki jih spuščajo nove tehnologije tako, kot bi se odzivali na resnične ljudi in se obnašamo tako kot v vsaki družbeni situaciji. Tako se npr. sprašujeta, ali se odzivamo na ženski glas v e-trgovini enako kot na moški, ali je odzivanje tehnologije s »človeškim« glasom vedno primerno in zaželeno ipd. Čeprav je knjiga prvenstveno namenjena oblikovalcem in (zlasti!) prodajalcem, nazorno prikaže odnos oziroma libidinalno investicijo subjekta v tehnologijo.

4. Posebnosti viktimizacij in žrtev kibernetične kriminalitete

Računalniške povezave v mednarodno telekomunikacijsko omrežje so omogočile napade na računalnike iz okolja zunaj dosega neposredne žrtve. Prvi *on-line* napadi so se zgodili v ZDA v 70. letih prejšnjega stoletja, torej v času nastajanja med-mrežnega sistema.

Temeljna značilnost viktimizacij kibernetične kriminalitete je množičnost žrtev.⁴⁵ V informacijski družbi poleg korporacij (pravnih oseb in državnih organov) uporabljajo medmrežne povezave tudi posamezniki, ki nimajo toliko tehničnega znanja in časa, da bi se ukvarjali s posodobitvami programske opreme, ki jih v korporacijah opravljajo za to usposobljeni sistemski administratorji. Najpogostejša žrtev je po podatkih Euro-pola⁴⁶ kljub temu gospodarstvo, sledijo mu državne institucije in na zadnjem mestu zasebni uporabniki. Najbolj pod »udarom« je torej gospodarstvo, kar je veliki meri pripisati tudi oceni, da je 70 odstotkov dnevne povprečne vrednosti posamezne delovne organizacije shranjene v obliki informacij, te pa so večinoma v elektronski obliki. Razlogi, da so najpogostejše žrtve ravno gospodarski subjekti in državne institucije pa so tudi strukturne narave. Sama internetna kultura, kultura hekerstva, ki je v samem osrčju ideje o medmrežju in je bila »pogonsko gorivo« njegovega razmaha, je namreč v veliki meri vrednostno diametralno nasprotna »kulturi« okoriščanja, maksimiranja dobičkov, monopoliziranja koristi izvirajočih iz intelektualnih stvaritev najpogostejših žrtev kibernetične kriminalitete.⁴⁷

Naslednja specifičnost viktimizacij kibernetične kriminalitete je nizka stopnja zaznavanja viktimizacij. Vdore v uporabnikov računalniški sistem prek računalniškega omrežja je težko opaziti brez posebne programske zaščitne opreme in s tem povezanega tehničnega znanja. »Logična bomba« ali virus se lahko sprožita šele po preteku določenega časa in na drugem koncu sveta. V prikrito pojavno obliko kibernetične kriminalitete uvrščamo npr. *data travellers*, vohunske programe, ki pregledujejo računalnik in obveščajo o njegovi konfiguraciji in vsebini tretje osebe. Prikrita tehnika napada je tudi tehnika *war dialer*, ustvarjanje stranski vrat v programu in prisluškovanje računalnikom. Za slednje je zanimivo to, da gre za prisluškovanje, ki se ne razlikuje od drugih oblik prisluškovanja, le da gre za prisluškovanje računalniški strojni opremi (*hardware*), ki pri delovanju spušča komaj slišne zvoke, te pa posebne naprave prestrezajo in »dešifrirajo«.

Zanimiva psihološka posebnost kibernetične viktimite je prikrivanje in/ali zanikanje statusa žrtve.⁴⁸ Kot omenjeno, je večina žrtev kibernetične kriminalitete gospodarskih subjektov, še posebej iz bančnega ali zavarovalniškega sektorja in državnih institucij. Največkrat gre za sabotaže (*cyber-sabotage*), ki so po nekaterih ocenah najpogostejša dejanja kibernetične kriminalitete, saj naj bi bilo kar 80 odstotkov kaznivih dejanj storjenih znotraj podjetij.⁴⁹ Ti najpogostejše viktimizirani subjekti pa niso naklonjeni razkrivanju lastne viktimizacije, saj ranljivost pomeni tveganje za nadaljnje poslovanje, povečanje nezaupanja ali izgubo zaupanja javnosti, ki je *sine qua non* za njihovo delovanje.⁵⁰ To pomeni, da je sekundarna viktimizacija teh subjektov večja od primarne viktimizacije in da je t. i. temno polje kiberkriminalitete oziroma kiberviktimite zelo veliko. Vsa ta dejstva so seveda vzpodbudna za kriminalno delovanje, prav tako pa otežujejo odkrivanje in preučevanje tovrstnih ravnanj zaradi nepoznavanja celega spektra s tem povezanih okoliščin (npr. poznavanja subkulture, dimanike, motivov storilcev, specifičnega *modus operandi* itd.).

V teoriji se pojavljajo različni predlogi zakonodajno-tehnične ureditve, s katerimi naj se prepreči prikrivanje viktimizacij, in sicer:

- a) obligatornost prijave kršitev organom pregona: stališče je problematično, zaradi obligatornega poseganja represivnih organov. Žrtev naj bo tista, ki odloča o tem, ali želi vpletenost tretjih strank (države) v razmerja, ki jih ima z drugimi. Načelo *volenti non fit injuria* v odškodninskem pravu in načelo *ultima ratio* kazenskopravnega poseganja v družbeno razmerja sta temeljni merili, ki morata veljati tudi v kibernetičnem prostoru. Po drugi strani je treba varovati interese žrtev, dasiravno to pomeni z državno neintervencijo, sicer bi žrtev utrpela dvojno viktimizacijo – s strani storilca in države;
- b) dolžnost prijave/razkritja kršitev obstaja le nasproti specializiranim strokovnim službam, ki bi v naslednji fazi posredovale kot mediator med žrtvijo in organi pregona;
- c) ustanovitev »platform« za diskusijo brez razkrivanja imen žrtev, na katerih dejanske/potencialne žrtve lahko sodelujejo in izmenjajo zaščitne ukrepe v sodelovanju z organi pregona. »Platforme« bi lahko bile tudi kot zbirni prostor za razkrite primere, svetovanje ipd. Rešitev se zdi še zlasti primerna

⁴⁸ Po nekaterih ocenah naj bi bilo prijavljenih le 10 odstotkov kaznivih dejanj, povezanih z računalniki. Vir: URL: www.intergov.org.

⁴⁹ Tako McGibbon: *Beware the security enemy within*.

⁵⁰ V Sloveniji je bil npr. odmeven domnevni vdor v računalniški sistem Nove Ljubljanske banke d.d. v letu 2003. NLB d.d. je ves čas zanikala, da je v njeno *on-line* bančništvo (spletno poslovalnico *Klik NLB*) vdrl heker, in zatrjevala, da je njihov sistem popolnoma varen. Osnovni problem, ki se je pokazal tudi v tem slovenskem primeru, je v tem, da je velika večina uporabnikov tovrstnih *on-line* storitev tehnično usposobljena toliko, da uporablja te storitve, tehnično ozadje pa jim še zdaleč ni doumljivo, tako da so prepuščeni retoriki PR predstavnikov domnevnih žrtev.

⁴⁵ Za trend rasti števila uporabnikov medmrežja glej op. 2.

⁴⁶ Europol: *Computer-related crime within the EU: Old crimes new tools; new crimes new tools*, str. 61.

⁴⁷ Glej poglavje o strukturnem nasilju v kibernetičnem prostoru.

zaradi ohranjanja minimalne vloge države pri poseganju v kibernetični prostor in prepuščanju regulacije samim uporabnikom.

Teza pozitivistične kriminologije, ki je storilca dojemala kot žrtev socialnih okoliščin (sociološki pozitivizem), se presenetljivo odraža na področju kibernetične kriminalitete. Presenetljivo zato, ker statistični podatki⁵¹ kažejo, da so bili napadi na računalniško omrežje v 2/3 primerov motivirani zgolj z radovednostjo napadalcev. Raziskovalci sicer poudarjajo, da se ta trend spreminja in da so vedno pogostejši napadi, ki so skrbno premišljeni in dovršeni, tako da je njihova posledica tudi večja gospodarska škoda. Kljub temu pa ni mogoče spregledati dejstva, da je medmrežno okolje kriminogeno, zlasti zaradi nejasno postavljenih mej dovoljenega in nedovoljenega, ki pa jih je zaradi hitre rasti medrežja in vedno novih tehnologij nemogoče pravočasno, primerno, legitimno določati. Poleg tovrstnih »storilcev iz radovednosti«, je zanimivo tudi dejstvo, ki potrjuje znano kriminološko zakonitost, da so si storilci in žrtve zelo podobni (imajo podoben življenjski slog itd.). Na sicer ožjem področju kibernetične deviantnosti, tj. pri pošiljanju neželjenih sporočil (*spamming*) in s tem preobremenjevanju omrežja, so ravno žrtve tiste, ki najpogosteje viktimizirajo, saj kar 70 odstotkov tovrstne pošte prihaja s strani samih žrtev, ki imajo okužene računalnike.⁵²

Virtualna narava kibernetičnega prostora je lahko sama po sebi viktimizator. Zaradi svoje virtualne narave vpliva na subjektivno zmožnost ločevanja notranjega (npr. fantazij) in zunanjega sveta, na vzpostavitev koherentnih in kompleksnih povezav med mentalnim (notranjim) svetom in izkušnjami iz zunanjega sveta. Na ta način združuje v enem obe domeni človekove izkušnje – notranjo in zunanjo. Ljudje pred pretirano spremenljivostjo sveta razvijamo obrambe, pomemben pa je način, kako se tovrstni obrambni mehanizmi oblikujejo. Gre za odnos in zmožnost ločevanja med notranjim doživljanjem in zunanjim svetom, ki je temeljni pokazatelj psihoze. Posamezni primeri, ki jih je mogoče zaslediti v literaturi kažejo, da narava kibernetičnega prostora povzroča ali okrepi raznovrstne psihične motnje. Če sledimo uveljavljeni psihiatrični terminologiji, ne moremo govoriti npr. o bolezni odvisnosti od interneta, temveč le o morebitni patološki navezanosti. Zaradi združevanja obeh domen človekove izkušnje, notranje in zunanje, lahko subjekt postane patološko navezan, ko svoje glasove

in notranje življenje projicira v zunanost prek računalnika.⁵³ Primer vpliva narave kibernetičnega prostora na duševnost uporabnika je tudi diagnoza »priklop-izklop« pri otroku (*on-off child*). Ta se nanaša na učinek neinhibirane rabe najrazličnejših tipk in gumbov, ki vplivajo na način otrokovega mišljenja. Računalnik ima namreč velik vpliv na prilagoditev mentalnih mehanizmov, še posebej pa na razvoj posameznikovih zmožnosti simbolizacije.

5. Posebnosti storilcev kibernetične kriminalitete

Za storilce kibernetične kriminalitete se je pogovorno in v družboslovnih refleksijah uveljavila oznaka računalniški hekerji.⁵⁴ Ta termin so iznašli študentje na Inštitutu MIT (*Massachusetts Institute of Technology*), kjer so zgradili prvi moderni računalniški sistem.⁵⁵ Hekerstvo sprva ni imelo pejorativnega ali kriminalnega prizvoka in tudi ni bilo uničevalno ali vandalско samo po sebi. Sprva je bilo normalni, želeni pristop dela skupin, ki so se ukvarjale s programiranjem. Šele kasneje je prišlo do ločitve med programerji in »pravimi« hekerji, ki manipulirajo s celotnim tehničnim sistemom, ne le z določenim sistemom z namenom izboljšave programa. Pojem hekanje sprva tudi ni obsegal le računalniških manipulacij, temveč manipulacije kakršnekoli tehnologije za nekonvencionalne namene, pri čemer je bila s hekerstvom označena dejavnost, za katero je bila potrebna tehnična spretnost, katere namen je bil pridobiti oblast in gospostvo na račun velikega sistema. Sprva tako ni bilo distinkcije med zakonito in nezakonito dejavnostjo; zadoščala je zgolj manipulacija s tehnologijo.

Družboslovni analitiki⁵⁶ kibernetičnega prostora večinoma menijo, da se hekerska kultura nanaša na vrednote in prepričanja, ki so izšle iz omrežij računalniških programerjev v interakciji *on-line* pri sodelovanju pri samodoločenih projektih kreativnega programiranja. Konstitutivni lastnosti te kulture sta bili avtonomija pri projektih in institucionalna avtonomija. Turkle⁵⁷ definira hekanje kot prepovedano in impresivno dejavnost, ki vključuje sofisticirano tehnično znanje.

⁵³ Williams opisuje primer tovrstnega pacienta, ki mu je svet med človeških odnosov kalopsiral in je bila pretirana uporaba računalnika glavni simptom njegove bolezni. Tako je računalnik odigral pomebno vlogo pri poslabšanju njegove bolezni. Glej Paul Williams: *Information Technology*.

⁵⁴ V kiberpankovski literaturi kot anticipaciji internetnega sveta so kibernetični devianti poimenovani digitalni ali konzolni kavboji (William Gibson). Kibernetičen prostor je potemtakem v njej implicitno še vedno percipiran kot divji zahod, brezpravni prostor. Slednjemu pa je blizu »osvajalska« maskulinizirana logika.

⁵⁵ Tako Steve Levy: *Hackers: Heroes of the Computer Revolution*.

⁵⁶ Npr. Manuel Castells: *The Internet Galaxy*, Steve Levy: *Hackers: Heroes of the Computer Revolution*, Sherry Turkle: *Life on the Screen: Identity in the Age of the Internet*.

⁵⁷ Sherry Turkle: *The Second Self: Computers and the Human Spirit*. Povzemam po: Manuel Castells: *The Internet Galaxy*.

⁵¹ Deloitte Touche Tohmatsu & Victoria police, 1999: *Computer crime and security survey*. Navajam po: Europol: *Computer-related crime within the EU: Old crimes new tools; new crimes new tools*, str. 64, op. 117.

⁵² Po podatkih *Spamhaus Project*, neprofitne organizacije, ki sledi pošiljalcem neželjene pošte (*spammers*) in objavlja njihove internetne naslove, tako da lahko ponudniki internetnih storitev blokirajo njihova sporočila. Glej David Rowan: *Britain is flooding the world with spam*.

Znotraj hekerske kulture so se oblikovale različne subkulture, med njimi pa so s kriminološkega vidika najbolj pomembni krekerji. To so hekerji, ki svoje znanje uporabljajo za dejanja brezcilnega vandalizma in tudi v sami hekerski kulturi veljajo za »ne-prave« hekerje. Pri kršitvah pravic intelektualne lastnine pa je zaslediti tudi razlikovanje med »črnimi uporabniki« in pirati. Prvi kršijo pravice intelektualne lastnine zgolj z namenom, da bi si produkt pridobili za svojo uporabo, drugi pa jih kršijo z motivom pridobivanja dobička z nadaljnjim razpečevanjem proizvoda. Glede na veliko tehnično znanje, ki je potrebno za storitev kibernetičnega kriminalnega dejanja, in tudi po statističnih podatkih o (formalni) izobrazbi hekerjev, pa lahko hekanje v skladu z obstoječimi kriminološkimi klasifikacijami uvrstimo med kriminal »belih ovratnikov«. Stratifikacija hekerskih subkultur⁵⁸ poteka načeloma po tehnični plati in ne po osebni ali ideološki plati. Po politični plati gre za zagovornike načela prosto dostopne programske opreme kot sestavine temeljne človekove pravice do svobode izražanja⁵⁹ in pravice do zasebnosti; po osebni plati pa gre za hekerje, ki se dojemajo kot junaki kiberpunk literarne produkcije, uporniki zoper korporacijske prevzeme njihovih ponudnikov internetnih storitev. Skupnost hekerjev je globalna, neformalna in virtualna, čeprav se občasno tudi fizično srečujejo na kongresih. Združuje jih vera v moč računalniškega mrežnega povezovanja in težnja po obdržanju te tehnološke moči v lasti vseh.

Splošne značilnosti kibernetičnega prostora, ki pomembno vplivajo na dinamiko storilcev, so anonimnost, ki daje občutek podzemlja in skrivnostnosti, manjša fizična in čustvena rizičnost in manjša stopnja zaznavanja viktimite. Čas in kraj storitve željenega dejanja sta v kibernetičnem prostoru rekonceptualizirana in poljubna: posledice je mogoče sprožiti iz kateregakoli mesta na katerokoli drugo (dovolj nezavarovano) mesto, posledice pa lahko poljubno nastopijo po volji napadalca takoj ali točno določen čas v prihodnosti. Vse to daje hekerjem, ki jih spremlja minimalen občutek ogroženosti, občutek nepremagljivosti in vsemogočnosti, občutek breztelesnosti in pobega iz telesne kompleksnosti realnega sveta (*disembodiment of self*).⁶⁰ Motivi hekerjev so podobni motivom drugih storilcev kaznivih dejanj (pohlep, maščevanje, radovednost), najpogostejši

motiv pa je intelektualni izziv, ki ga hekerju predstavlja njegov podvig.⁶¹

Socialna konstrukcija hekanja je bila od 80. let prejšnjega stoletja dalje izrazito negativno konotirana in zajema naslednje elemente: pojem hekanja je omejen na računalniško tehnologijo, na nezakonito dejavnost, ki je namenjena pridobivanju dobička. Prav tako so običajne predstave o hekerjih izrazito pejorativne. Arhetipska predstava hekerja je predstava o adolescentnem fantu, ki izživilja svoje seksualne fantazije ali kavbojske sanje, je neurejenega videza, živi za in skozi svoj računalnik, kompulziven, distanciran od ostale mainstreamovske družbe, socialno neprilagojen in brez družbenih veščin, obsesiven, napihnjen, sebičen, solipsističen, a tehnološko izobražen. Njegov cilj je zrušiti vlado/e in onesposobiti obveščevalno/e službo/e. Heker je po teh reprezentacijah psihološko marginalen ali vsaj čudak (*freak*), do ostalih članov skupnosti (ne-hekerjev) goji občutek superiornosti, prekinja vezi s skupnostjo in beži v svet formalne strukture računalništva. Čeprav povečini vodi »normalno« življenje, gleda skupne kulturne filme (npr. *Enemy of the State*, *The Matrix*) in živi kot heker le *on-line*.

Tovrstna socialna konstrukcija dejavnosti in njenih akterjev pa nosi ideološka sporočila, ki ustrezajo določenim skupinam. V ozadju tovrstnega etiketiranja se kažejo obrisi ideološkega boja med zagovorniki odprtokodnega sistema (*open source code*) programske opreme in med veliki korporacijami, proizvajalkami programske opreme, ki se zavzemajo za široko avtorskopravno zaščito svojih izdelkov.⁶² Bistveno za zagovornike odprtokodnega sistema pa je ravno sodelovanje, svoboda, kultura darovanja (*gift-culture*). Zaradi nedvoumno pozitivnih elementov hekerstva se zato uveljavlja distinkcija med hekerji in krekerji. Medijske reprezentacije, ki se nanašajo na razbijanje kod, ilegalne vdore, opustošenje »informatijske avtoceste«, se nanašajo na krekerje.⁶³ Hekerje na splošno tako kot ostale »zločince« obdaja avreola svetniškosti, reprezentirani so kot

⁵⁸ V zgodovinskih prikazih razvoja interneta se navaja za različna obdobja različne subkulture: v začetku 80. let so bile tri računalniške kulture (glede na tipe strojne opreme in programskega jezika): *Arpanet* (Lisp programski jezik), *Unix* (C programski jezik) in PC kultura (Basic programski jezik). Več v: Manuel Castells, 2001: *The Internet Galaxy* in John Naughton: *A Brief History of the Future: The Origins of the Internet*.

⁵⁹ Tako Richard Stallman, ustanovitelj *Free Software Foundation*, iz katerega se je kasneje razvilo *Free Software Movement*.

⁶⁰ Za fenomenološke opise hekanja glej Ellen Ullman: *Close to the Machine: Technophilia and its Discontents* ali Claudia Springer: *Electronic Eros: Bodies and Desire in the Postindustrial Age*.

⁶¹ Najbolj značilne deviantne aktivnosti hekerjev: nadlegovanje po elektronski pošti (*e-mail stalking*); pošiljanje neželenega (*spama*), sovražnega, obscenega, grozilnega materiala in »poštne bomb«; okužbe s programi (virusi), ki onemogočajo delovanje nameščenih programov; nadlegovanje v klepetalnicah (*chat stalking*), vključevanje v pogovor in žaljenje, sramotenje, opsovanje žrtev (*flaming*); pošiljanje žaljivih sporočil na BBS (*bulletin board system*), podpisanih z imenom žrtve, sprožanje govorice; škodoželjno obveščanje v novičarskih skupinah (*newsgroups*); pridobivanje nadzora nad operacijskim sistemom, nadzorovanje računalniškega namizja in beleženje opravil na računalniku (npr. branje teksta v realnem času).

⁶² Več o boju za prevlado nad (!) kibernetičnim prostorom v naslednjem poglavju.

⁶³ Ker pa nas na tem mestu ne zanimajo toliko pojavne oblike deviantnih ravnanj v kibernetičnem prostoru kot hekerska subkultura in psihična dinamika hekerjev, bomo v nadaljevanju uporabljali izraz hekanje kot nadpomenko, ki združuje vse tehnične manipulacije v kibernetičnem prostoru, tam kjer bo razlikovanje med različnimi hekerji bistvena, pa bomo na to posebej opozorili.

zadnji borci za svobodo v kibernetičnem prostoru, kot tudi etike-
ta zlih demonov kibernetičnega prostora, ki vznemirjajo dobro
hotečo moralno večino.

Taylor,⁶⁴ ki je opravil obsežne raziskave o hekerski kulturi z
intervjuji s posameznimi hekerji, tehničnim-varstvenim
osebjem in z analizami posamičnih primerov, meni, da je skupna
lastnost vseh hekerjev predvsem iskanje užitka, ki ga heker
dobi z identificiranjem artefakta znotraj velikega sistema, zato
da bi lahko upravljali s tem artefaktom učinkoviteje; bistrost in
premetenost sta cilj sama na sebi. To naj bi bistveno opredeljeva-
lo tudi spolno (*gender*) konstrukcijo hekerstva kot izrazito moš-
ke oziroma deške kulture. V splošnih predstavah o hekerjih,
njihovih medijskih reprezentacijah in statističnih podatkih je
namreč vedno v ospredju figura hekerja moškega spola. Vpra-
šanje spolne konstrukcije hekerstva kot tipično moške dejav-
nosti zato poleg »klasičnega« kriminalološkega vprašanja, »zakaj
so moški pogostejši storilci kaznivih dejanj«, odpira tudi vpra-
šanje o sami naravi in konceptualizaciji kibernetičnega prosto-
ra in o psihodinamiki hekerjev. Psihoseksualne teorije razla-
gajo to neudeležnost žensk v hekerski kulturi z domnevo, da
tovrstna tehnologija nudi katarzičen izhod predvsem frustrira-
nim mladim fantom, ki iščejo kanale za uveljavljanje svojih
teženj po dominaciji. Hekanje je v teh teorijah predstavljeno
kot substitut spolne aktivnosti ali nezrele seksualnosti (pri ka-
teri je računalnik hekerjev partner, virus pa skupni otrok).⁶⁵
Tehnologija je v teh primerih nesporno objekt libidinalne in-
vesticije, a po tem se ta dejavnost ne razlikuje od drugih človeških
(npr. kulturnih, znanstvenih, športnih idr.) prizadevanj. Tovrst-
ne razlage nekonstruktivnega hekerstva niso povsem neuter-
meljene, a so v celoti gledano enostranske, saj hekerje reduci-
rajo na dečke s preveč testosterona, premeščeno libidinalno
energijo, mačiste in Freudovo (po njihovem maskulinizirno)
teorijo o zavisti po penisu obračajo v »*kiborg envy*«. Spet dru-
ge razlage so bolj praktično orientirane. Ženske po teh razla-
gah ne programirajo, ker je to okolje prežeto z vrednotami nedo-
raslosti, nerodnosti, nezrelosti in ezoterike. Brezciljna destruk-
cija in tehnična dovršenost sama po sebi ženskam ni zanimiva,
saj si želijo tehnike, ki ima cilje zunaj sebe.⁶⁶

Konceptualizacija dežele mladih fantov in večnega študent-
skega življenja je moško orientirana predvsem zaradi prežeto-
sti zgodnjega hekerskega okolja z moškimi družbenimi atribu-
ti in z objektivni koncepti, ki jih lahko ti zavojujejo. Taylor
meni, da gre za »pionirsko mentaliteto«, po kateri se kibernetič-
ni prostor primerja z divjim zahodom, safarijem, osvajanjem,
zavojevanjem.⁶⁷ V tem smislu ni torej kibernetični prostor nič

novega, saj gre v civilizacijskem smislu za tipično zahodno,
židovsko-krščansko etiko, kjer štejejo vrednote, kot so prodor-
nost, inovativnost, drznost, moč, pogum, prestopanje mej itd.

Kljub temu pa je zgodnje hekerstvo, vsebovalo kvalitativno
predrugečene (protikulturne) vrednote, ki jih je izgubilo šele
kasneje s komercializacijo interneta v 90. letih prejšnjega sto-
letja. Kulturo hekerjev lahko danes po vrhuncu komercializa-
cije interneta razumemo kot kulturo vrednot, ki bi se morala
prebiti iz okvirov kibernetičnega prostora v »resnični« prostor.
Hekerstvo je (lahko) čuvaj pri uporabi nadzorstvenih tehnolo-
gij, pri zbiranju podatkov s strani oblasti in omejevanju komu-
nikacijske moči gigantskih korporacij, kulturni odpor in zalo-
ga opozicijskega znanja proti tehnološko-fašistični prihodnosti.⁶⁸
Komercializacija informacijske tehnologije je »naplavila«
krekerje, ki so kriminalno orientirani, profesionalizirani, vred-
notno pa v celoti pogreznjeni v prevladujočo »kulturo« kapita-
listične gonje za dobičkom. Hekerji so zaradi teh ožjih skupin
percipirani kot nevarni anarhisti in zločinci, ki se jih bojijo
vlade, računalniška in varnostna industrija, ki jim tovrstna nega-
tivna konceptualizacija hekerstva ustreza pri uresničevanju
njihovih teženj po dominaciji nad in v kibernetičnem prostoru.
Gre torej za strukturne kriminogene dejavnike kibernetične
kriminalitete, za zmožnost uveljavljanja simbolizacij in repre-
zentacij posameznih aktivnosti v kibernetičnem prostoru, ki
so odvisni od konstalacije moči med varnostno industrijo in
računalniškim »podzemljem«.

6. Strukturno nasilje in kibernetični prostor

Internet je tehnološki sistem, ki je družbeno ustvarjen ali
drugače, kultura proizvajalcev interneta je oblikovala internet
kot medij. Castells⁶⁹ deli internetno kulturo na štiri dele, ki jim
je skupna ideologija svobode. V začetni fazi je internetu kot
tehnologiji gospodovala tehnološko-meritokratska kultura z vero v
inherenten napredek znanstvenega in tehnološkega razvoja in
hekerska kultura. Slednja izvira iz akademske kulture, kjer so
glavne odlike odličnost, odprta komunikacija in kontrola med
seboj enakih. Hekerska kultura in njena etika je že v samem
začetku zaznamovala informatizacijo in predstavljala most med
znanjem tehnološko-meritokratske kulture in podjetništvom (tretji
del),⁷⁰ ki je tehnologijo posredovalo množicam v komercialno

⁶⁸ Tako Andrew Ross: *Strange Weather*, str. 82. Citiram po Paul A.
Taylor: *Hackers: Crime in the digital sublime*, str. 43.

⁶⁹ Manuel Castells, 2001: *The Internet Galaxy*, str. 36 in nasl.

⁷⁰ Ta podjetniška kultura je internet spremenila v poslovanje, v »novo
ekonomijo«. Podjetniška inovativnost in ne kapital naj bi bila gonilna
sila internetne ekonomije; ideje, ki se transformirajo v podjetja, glavni
vodili, ki naj omogočita uspeh in neodvisnost od tradicionalnega kor-
porativnega kapitala, pa sta pričakovana količina in hitrost pridobi-
vanja dobička. Internetni podjetnik združuje lik inovatorja, tehnologa
in venture kapitalista, je individualist z ekscenčno potrošnjo, nizko socia-
lizacijo in bolj umetnik kot poslovnež.

⁶⁴ Paul A. Taylor: *Hackers: Crime in the digital sublime*.

⁶⁵ Paul A. Taylor: *Maestros or misogynists? Gender and the social construction of hacking*, str. 135.

⁶⁶ Tako Paul A. Taylor: *Maestros or misogynists? Gender and the social construction of hacking*, str. 131.

⁶⁷ Tako je kibernetični prostor konceptualiziran tudi v kiberpanko-
vski literaturi, kjer so hekerji »konzolni kavbojji«.

uporabo. Četrty del internetne kulture po Castellsu je »virtualna skupnost« (Rheingold), t.j. skupek vrednot uporabnikov, ki krojijo vedenje in socialno organizacijo v kiberprostoru, oblikujejo družbene procese in uporabo tehnologije.

Bistvene kulturne in vrednostne elemente internetnih skupnosti kaže iskati v prevratnih 60. letih in protikulturnem gibanju. Zgodovinski pregledi interneta prikazujejo zgodnje *online* konference kot poskuse oblikovanja skupnosti po neuspehu protikulturnega gibanja v »resničnem« svetu. Hekersko kulturo tako v bistvu prežemajo vrednotna izhodišča, ki so bila izgnana iz »resničnega« sveta s »kontrarevolucijo« kapitala. Tovrstne vrednote protikulturnega gibanja so združene s tehnološkim znanjem tehnokratne kulture dobile ugodno okolje za razvoj hekerske kulture. Ta je združila visoko tehnološko znanje s svobodo, z užitki kreativnosti, ugledom in spoštovanjem med seboj enakih, vpeljala neformalno organizacijo,⁷¹ kulturo darovanja, vzajemnost, načelo sodelovanja, komercializacijo pa le pod pogojem, da so vse informacije o programih (prosto) dostopne in je program dovoljeno spreminjati, izpopolnjevanje. Te vrednote so nasprotje logiki privatizacije, dobička, formalnopравnih pravic in institucionalne moči. Po tej vrednotni optiki je primerna le delna komercializacija, priposestevanje in lastninjenje. Gre torej za povsem postmodernistično vrednotno optiko enakosti, svobode, proste komunikacije in ustvarjanja odprtega prostora, ki naj omogoči prostor za nove ideje.

Na specifičnem področju internetnega razvoja je postmodernistična kulturna optika našla svoj izraz v odprtokodnem gibanju (*open source movement*), ki je postalo strukturna fizionomija interneta in temelj za razumevanje hekerske kulture. Odprtokodno gibanje je podaljšek izvornega gibanja za prosto programsko opremo (*free software movement*), temeljna ideja tega gibanja pa je obdržati kolektivne stvaritve zunaj vladnega dosega in dosega korporacij. Zgodovina gibanja za prosto programsko opremo sega v čas internetnih začetkov, ko so želeli programerji za operacijski sistem UNIX pridobiti avtorske pravice in so v MIT (*Massachusetts Institute of Technology*) ustanovili *Free Software Foundation* (iz katerega se je kasneje razvilo *free software movement*) in predlagali, da avtorsko pravico – *copyright* zamenjajo s »*copyleft*«. Slednja je pomenila, da vsak, ki uporablja prosto dostopno programsko opremo, v zameno distribuira na internet njeno izboljšano kodo. Fundacija je (pravno) izpeljevala to pravico iz temeljne človekove pravice do svobode govora in s tem do komunikacije in uporabe programske opreme. Po zgledu UNIX-a so razvili nov sistem GNU/Linux,⁷² ga posredovali v prosto uporabo na in-

ternet, pozvali uporabnike k njegovi izboljšavi in k posredovanju izboljšane verzije nazaj na internet. Tako so Linux ves čas izboljševali hekerji in drugi uporabniki. UNIX-ov lastniški sistem je med tem zavrl razvoj programske opreme, kasneje pa je bila Berkeley UNIX Group razpuščena in na trgu je kljub slabši tehnologiji ostal *Microsoft*, ki si je prilastil trg operacijske programske opreme. Alternativa je tako ostal GNU/Linux sistem.⁷³

Kapitalistična logika je ob komercializaciji informatijske tehnologije odprla vprašanje vdiranja v zasebnost, širjenja nadzorovalnih tehnologij in zaostila vprašanje kdo bo varoval varuhe (*quis custodiet custodes*) v zvezi z uporabo vrhunskih tehnologij. Rezultat nesorazmerja moči med hekersko postmodernistično kulturo in »digitalnim kapitalizmom« (Virilio) oziroma »digitalnim darvinizmom« (Taylor) je generiranje strukturnega nasilja v kibernetičnem prostoru. Prevlada vrednotne optike »digitalnih kapitalistov« se kaže v več primerih. V javnosti je zlasti znan projekt *Echelon*,⁷⁴ globalni elektronski vohunski sistem, namenjen kontroli komunikacijskega prometa, zlasti interneta in komunikacij po mobilnem telefonskem omrežju, pri katerem so sodelovale ZDA, Velika Britanija, Kanada, Avstralija in Nova Zelandija. Sofisticirana »prisluškovalna« naprava je izrabljala tedanje elektronske tehnologije za zbiranje podatkov, navedene države pa so ves čas zanikale njen obstoj. Kot vse kaže, pa naj bi ravno ta »neobstoječa« mreža zagotovila tehtne podatke (kot so bančni transferji, telefonski pogovori), ki so razkrili tvorce terorističnega napada na ZDA. Drug primer strukturnega nasilja v kibernetičnem prostoru je primer ameriškega velikana programske opreme *Microsoft*. Ta igra pomembno vlogo s programi, ki poganjajo različne sisteme, njihove izdelke pa poleg posameznikov (za »domačo« rabo), uporabljajo državne uprave na različnih delih sveta.⁷⁵ Tako velik tržni delež tega programskega velikana in množice njegovih nameščenih programskih sistemov pomenijo potencialno nevarnost vstopa »nepovabljenih gostov« prek »odprtih vrat« v programih, zaradi česar ni presenetljiva odločitev indijske državne uprave (v l. 2002) in mestne uprave mesta München (v l. 2003) – po velikosti primerljive s slovensko državno upravo – da bo uporabljala odprtokodne programske rešitve. Nadaljnji domnevni primer zlorabe, vtikane v oblikovanje kibernetičnega

⁷¹ Neformalne organizacije sestavljajo plemenske starešine, ki so vzdrževalci sistema (*tribal elders*, kot je npr. v Linux sistemu njegov začetnik Linus Torvalds) ali kolektivne avtoritete z menjajočimi vzdrževalci, ko-vzdrževalci za podsisteme itd.

⁷² Po 22-letnem študentu Linusu Torvaldsu, ki je izdelal operacijski sistem LINUX na podlagi avtorskopравno zavarovanega UNIX-a.

⁷³ Linux je l. 2001 uporabljalo okrog 30 milijonov uporabnikov, razlog njegove manjše uporabe pa je dejstvo, da je zapleten za uporabo, saj pri njegovi zasnovi ni bila v ospredju usmerjenost k uporabniku. Druga odprtokodna programska oprema so še npr.: *TCP/IP protokol*, na katerem je temeljil prvi mrežni sistem *ARPA-INTERNET*, *UNIX* operativni sistem v 70. letih, modemski protokoli v razvoju mrež za PC-je, *WWW server* in *browser*, *Mosaic Browser* in delno prvi komercialni browser – *Netscape Navigator*; tudi programska jezika *Java* in *Jini* (*Microsystems*), serverski program *Apache* itd.

⁷⁴ Glej tudi Doug Barney: *Say good-bye to privacy*, Denis Trček: *Lastniki vseh tvojih informacij*.

⁷⁵ Gre za t. i. *enterprise agreements*, s katerimi *Microsoft* kot »najemodajalec« opremlja državne uprave s programsko opremo.

prostora, je IBM-ova programska rešitev za skupinsko delo *Lotus Notes*. Glavna odlika tega programa je, da so vsi dokumenti uporabnikov (npr. javnih uslužbencev) arhivirani v elektronski obliki, za zaščito podatkov pa ima program vgrajeno ustrezno kriptografsko tehnologijo, katere moč je izražena v dolžini uporabljenih ključev za kriptiranje. Po nekaterih podatkih pa naj bi bil del tega ključa evropske različice (tovrsten program uporablja tudi slovenska državna uprava) dostopen ameriški NSA (*National Security Agency*), kar naj bi jim omogočalo vpogled v poslovanje uporabnikov, njihovo komunikacijo in (tudi) zaupno gradivo.

Mahinacije in malverzacije »digitalnega kapitalizma« (Virilio) s kibernetičnim prostorom so torej neizmerne. Ohrabruječe je, da kljub občutni prevladi podjetniške logike prisvajanja in izključevanja v kibernetičnem prostoru, ta v političnem smislu še vedno ostaja prostor za uveljavljanje in krepitev alternativnih vrednotnih optik. Hekerski vrednotni optiki je ta tehnologija »pisana na kožo«, antiglobalističnim gibanjem z mrežno strukturo pa prav mrežni sistem tehnologije ustreza kot sredstvo povezovanja in boja za prerazdelitve moči in virov.⁷⁶ Hektivizem, kot oblika fuzije političnega aktivizma in tehnologije, tako paradoksalno postaja oblika elektronske državljanske neposlušnosti, ki vpleta več realnih problemov družb, povezuje objektivni, abstrakten kibernetični prostor z »resničnim« svetom in skuša obrniti tehnolibertarizem in vrniti kibernetično družbo k izvorni ideji hekanja.

7. Sklep

Kibernetična realnost je s kriminološkega vidika nadvse paradoksalna. Deviantnost, transgresija običajnih, »normalnih«, utečenih praks in vrednot je nekaj, kar je vtakano v sam razvoj kibernetičnega sveta in hekerske kulture. Tehnološka odličnost kot prvenstveni cilj hekerskega delovanja je bila mogoča le zaradi transcendiranja pojmov, kot je lastninska in avtorska

pravica, ki temeljita na izključevanju, prisvajanju in privatizaciji. Odprtost kibernetičnega prostora je kulturno determinirana in vtakana v sam nastanek internetne kulture. Tudi upravljanje interneta je v veliki meri skupno; skupen razvoj protokolov, soglasja o standardnih in dodelitve imen in naslovov so potekali s koordinacijo uporabnikov. Komunitaren pristop h tehnologiji, srečanje meritokratske kulture in utopistične protikulture, samoocenjevanje in oblikovanje interneta z njegovo uporabo, so omogočili nesluten razvoj. Predružačeno kulturno in vrednotno ozadje kibernetičnega prostora pa ima ob poskusih »polaganja« kibernetičnega sveta na prokrustovo posteljo kapitalizma (tokrat pač »digitalnega«) paradoksalne učinke. Kibernetični prostor nudi možnost za osvoboditev subjekta od družbeno vsiljenih identitetnih obrazcev in njegovega identitetnega redefiniranja, po drugi strani pa prostor izolacije in pacifikacije subjekta; je prostor razdiranja obstoječih skupnosti in »čustvene inflacije«, a tudi prostor oblikovanja novih skupnosti; je prostor perpetuacije patriarhalnih, kolonialnih in seskističnih vzrocev, a tudi prostor, ki nudi možnost za njihovo preseganje; je prostor stigmatizacije, marginalizacije družbenih manjšin (še) v novem polju »resničnega« in hkrati prostor normalizacije, destigmatizacije »deviantnih« oblik ravnanja itd.

Virtualna narava kibernetičnega prostora je tisti *differentia specifica*, ki ima psihološke reperkusije in nas je vodila pri analizi kibernetičnega prostora. Pri tem smo analizirali pojem in mehanizme nastanka identitete, ki jih kibernetični prostor razgali, obravnavali kibernetične skupnosti in druge posebnosti psihološke fenomenologije kibernetičnega prostora. Posebnosti psihološke fenomenologije kibernetičnega prostora so logičen nasledek dejstva, da gre za »informacijsko revolucijo«, informacije pa kot element komunikacije povratno vedno vplivajo na subjekt. Še pred analizo posebnosti viktimizacij in storilcev v kibernetičnem prostoru smo skušali osvetliti tudi (proti)kulturne vidike kibernetičnega prostora in tako prikazali širše koordinate sicer v pretežni meri skomercializiranega kibernetičnega prostora. Kljub uspešnim poskusom vrednostnega zasuka iz protikulturne v »kulturno« kapitalistično vrednotno opcijo, pa duh uporniškega panka ni zamrl. Protiglobalistična gibanja uporabljajo internet kot medij postmoderne dobe *par excellence* za napade na simbole samega globaliziranega potrošniškega »digitalnega« kapitalizma; za napade na banke in vojaške baze (npr. Pentagon),⁷⁷ mašinerijo, ki je v začetku s financiranjem in prepustitvijo relativno velike avtonomije sploh omogočila razcvet »informacijske avtoceste«. Tako kibernetični prostor po izgubi mitičnega čara tehnologije in moči sublimirati libidinalno energijo ostaja pomembna alternativa vrednotnih življenjskih opcij in potencial družbenih sprememb.

⁷⁶ Prvi primer politične rabe interneta in prve kibernetične vojne (*cyberwar*) so domorodni boji Zapatistov v državi *Chiapas* (Mehika) proti okupaciji, ki se je začela 1.1.1994. Z uporabo interneta so namreč ti pridobili svetovno publiciteto in podporo; po internetu učijo svoje jezike, običaje, zgodovino in na ta način slabijo siceršnjo cenzuro mehiške vlade. Tako gradijo svojo skupnost prek prostorskih meja *Chiapasa*. Mehika vlada jim je vrnila udarec po internetu z nadzorovanjem in obtožbami o hekerstvu (zato prva kibernetična vojna). Ta upor je tako postal primer (prve) uspešne uporabe omrežne komunikacije s strani ljudskega gibanja, iskanja mednarodne podpore, vrednosti elektronske podpore političnim gibanjem proti globalnem kapitalizmu in neoliberalizmu (upor Zapatistov po okupaciji 1.1.1994 šteje tudi za prvo protiglobalistično zborovanje), primer boja za pravice žensk, kmetov in domorodcev za zemljo. Glej Rinella Cere: *Digital counter-cultures and the nature of electronic social and political movements*. V: Yvonne Jewkes (ed.): *Dot.cons: Crime, deviance and identity on the Internet*, str. 153–161.

⁷⁷ Npr.: BBC, 1999: *Nato under »cyber attack«*.

Literatura

- Abelson, H.; Lessing, L. (1998). **Digital Identity in Cyberspace**. URL: <http://www.swiss.ai.mit.edu/6095/student-papers/fall98-papers/identity/white-paper.ht ml>.
- Abramson, B. (2005). **Digital Phoenix: Why the Information Economy Collapsed and How It Will Rise Again**. Cambridge: The MIT Press.
- Bartle, R. (2003). **Designing Virtual Worlds**. Indiana: Prentice Hall PTR.
- BBC (1999). **Nato under »cyber attack«**. URL: <http://www.flora.org/flora.mai-not/ 10498>.
- Barney, D. (2001). **Say good-bye to privacy**. URL: <http://www.networkcomputing .com/1222/1222colbarney.html>.
- Baudrillard, J. (1999). **Simulaker in simulacija**. Ljubljana: Študentska založba (Koda).
- Benvenuto, B. ; Kennedy, R. (1986). **The Works of Jacques Lacan: An Introduction**. London: Free Association Books.
- Brvar, B. (1982). Pojavne oblike zlorabe računalnika. *Revija za kriminalistiko in kriminologijo*, let. 33, št. 2. 92–104.
- Butler, J.; Laclau, E.; Žižek, S. (2000). **Contingency, Hegemony, Universality**. London & New York: Verso.
- Castells, M. (2001). **The Internet Galaxy**. Oxford: Oxford University Press.
- Clark, Schofield, L. (1998). Dating on the Net: Teens and the Rise of »Pure« Relationships. V: Steven G. Jones (ur.), **Cybersociety 2.0: Revisiting Computer-Mediated Communication and Technology**. London, Thousand Oaks, New Delhi: Sage Publications.
- Clarke, R.V. (2004). Technology, Criminology and Crime Science. *European Journal on Criminal Policy and Research*, Volume 10, No. 1. 55–63.
- Council of Europe (2001). **Convention on Cybercrime**. URL: <http://conventions.coe. int/Treaty/EN/cadreprincipal.htm>.
- Council of Europe (2003). **Additional Protocol to the Convention on Cybercrime, Concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed Through Computer Systems**. URL: <http://conventions.coe.int/Treaty/ EN/cadreprincipal .htm>.
- Crawford, S.P. **Who's in Charge of Who I am?: Identity and Law Online**. URL: <http://www.scrawford.net/page.php?display =writings>.
- Davies, S.D. (1994). Touching Big Brother: how biometric technology will fuse flesh and machine. *Information Technology and People* 7(4). URL: www.privacy.org/pi/reports/biometric.html.
- Europol, 2003. **Computer-related crime within the EU: Old crimes new tools; new crimes new tools**. Luxembourg: Office for Official Publications of the European Communities.
- Gibson, W. (1984). **Neuromancer**. New York: Ace Science Fiction.
- Gibson, W. (2004). **Virtualna svetloba**. Ljubljana: Založniški atelje Blodnjak (Knjižna zbirka Blodnjak).
- Gibson, W.; Sterling, B. (2003). **Spremenljivostni stroj** (I. in II. del). Ljubljana: Založniški atelje Blodnjak (Knjižna zbirka Blodnjak).
- Grabosky, P. (2001). Computer crime: a criminological overview. V: **Forum on Crime and Society**, volume 1, number 1. New York: United Nations Publications. 35–53.
- Himanen, P. (2001). **The Hacker Ethic and the Spirit of the Information Age**. New York: Random House.
- Huey, L. ; Rosenberg, R.S. (2004). Thoughts on Expanding Police Surveillance Opportunities under the Cyber-Crime Convention. V: **Canadian Journal of Criminology and Criminal Justice**, Volume 46, no. 5. 597–606.
- Jakulin, V. (1996). **Kazenskopravni vidiki računalniškega piratstva**. Vir: URL: <http://www.ius-software.si>.
- Jewkes, Y. (ed.) (2003). **Dot.cons: Crime, deviance and identity on the Internet**. Devon: Willan Publishing.
- Jones, S.G. (1997). The Internet and its Social Landscape. V: Steven G. Jones (ur.): **Virtual Culture; Identity & Communication in Cybersociety**. London, Thousand Oaks, New Delhi: SAGE Publications.
- Levy, S. (1984). **Hackers: Heroes of the Computer Revolution**. New York: Penguin.
- Longan, M. W. (1997). **Geography, Community and Cyberspace**. Paper presented at the 1997 Annual Meeting of the Association of American Geographers. URL: <http://ucsu.colorado.edu/olongan/geogcommcyber.htm>.
- Magnin, C. J. (2001). **The 2001 Council of Europe Convention on cyber-crime: an efficient tool to fight crime in cyber-space?** URL: <http://www.magnin.org/Publications/2001.06.SCULLM DisertationPrHammondCOEConvention.Cyber-crime.pdf>.
- McGibbon, A. (2001) **Beware the security enemy within**. Network News 13 June. URL: www.vnu.com.
- Mitnick, K.D. (2002). **The Art of Deception: Controlling the Human Element of Security**. Indianapolis: John Wiley & Sons Inc.
- Mosco, V. (2004). **The Digital Sublime: Myth, Power, and Cyberspace**. Cambridge: The MIT Press.
- Clifford Nass in Scott Brave, 2005: **Wired for Speech: How Voice Activates and Advances the Human-Computer Relationship**. Cambridge: The MIT Press.
- Naughton, J. (1999). **A Brief History of the Future: The Origins of the Internet**. London: Phoenix.
- Pahor, D. *et al* (2002). **Leksikon računalništva in informatike**. Ljubljana: Pasadena.
- Parry Lloyd, R. **Suicide, the net and death with a stranger**. URL: <http://www.timesonline.co.uk>.
- Pocar, F. (2004). New Challenges for International Rules against Cyber-Crime. *European Journal on Criminal Policy and Research*, Volume 10, No. 1. 27–37.
- Praprotnik, T. (2003). **Skupnost, identiteta in komunikacija v virtualnih skupnostih**. Ljubljana: ISH – Fakulteta za podiplomski humanistični študij (Knjižna zbirka Documenta).
- Ross, A. (1991). **Strange Weather: Culture, Science and Technology in the Age of Limits**. London: Verso.
- Rowan, D. **Britain is flooding the world with spam**. URL: <http://www.timesonline.co.uk>.
- Savona, E.U.; Mignone, M. (2004). The Fox and the Hunters: How IC Technologies Change the Crime Race. *European Journal on Criminal Policy and Research*, Volume 10, No. 1. 3–26.
- Springer, C. (1996). **Electronic Eros: Bodies and Desire in the Postindustrial Age**. Austin: University of Texas Press.
- Strehovec, J. (1999). Teorija posebnih učinkov. V: Jean Baudrillard: **Simulaker in simulacija**. Ljubljana: ŠOU Študentska založba (Knjižna zbirka Koda).
- Suler, J. (1996). **The Psychology of Cyberspace**. URL: <http://www.rider.edu/~csuler/psycyber/psycyber.html>.
- Taylor, P.A. (1999). **Hackers: Crime in the digital sublime**. London & New York: Routledge.
- Torpey, J. (2000). **The Invention of the Passport: Surveillance, Citizenship and the State**. Cambridge: Cambridge University Press.
- Trček, D. (2003). **Lastniki vseh tvojih informacij**. Vir: URL: www.delo.si.

48. Ullman, E. (1997). **Close to the Machine: Technophilia and its Discontents**. San Francisco: City Lights Books.
49. Turkle, S. (1997). **Life on the Screen: Identity in the Age of the Internet**. New York: Simon & Schuster.
50. Virilio, P. (1996). **Hitrost osvoboditve**. Ljubljana: Študentska organizacija Univerze (Koda).
51. Vogrinc, J. (1998). Zamišljene skupnosti danes (spremna beseda). V: B. Anderson: **Zamišljene skupnosti; O izvoru in širjenju nacionalizma**. Ljubljana: Studia humanitatis.
52. Warschauer, M. (2003). **Technology and Social Inclusion**. Cambridge: The MIT Press.
53. Williams, P. **Information Technology**. URL: <http://www.pschoanalysis.org.uk/paper.htm#s>.
54. Žižek, S. (1997). Kiberprostor ali možnost prekoračiti fantazmo. V: **Problemi**, let. 35, št. 7/8. 21–39.
55. Žižek, S. (1996). Kiberprostor ali neznosna zaprtost bivanja. V: **Problemi**, let. 34, št. 7/8. 101–132.
56. Žižek, S. (1999). Realno kiberprostora. V: **Problemi**, let. 37, št. 3/4. 5–16.
57. Žižek, S. (1999). **The Plague of Fantasies**. London: Verso.

Cybercrime: (cyber)criminological and (cyber)victimological particularities of the »information superhighway«

Aleš Završnik, LL.B., Institute of Criminology at the Faculty of Law, Poljanski nasip 2, 1000 Ljubljana, Slovenia

Cybercrime as an accompanying phenomenon of the »information revolution« and its most famous »service«, i.e. the internet »information highway«, is a very vague notion. Besides dilemmas inherent in crime in general, cybercrime is characterised by a specific nature of a crime scene. There is a question of virtual space that has an impact on the phenomenology of crime and its victimisation. In analysing cybercrime, the paper rests on sociological reflections of cyberspace and cyber (contra) culture, which are important for the understanding of criminological/victimological pair: offenders and a hacker culture on the one hand, and victims and victimological characteristics on the other. (Contra) cultural background of cyberspace belongs to ideological currents of post-modern theories, to which are common the questions of the individual's identity and mobiles for looking for communities and people in internet space. The paper therefore deals with the issues of »law of identity« in the internet »laboratory for the construction of identity« as well as with a identity theft or the identity fraud. The paper also gives an overview of cybercommunities, which are on the one hand the result of the liberating potentials of cyberspace, and on the other, the pacification and isolation of lonesome in screen goggling individuals. The central part of the paper is devoted to the specifics of victimisation by cybercrime and to cyberdeviants (console cowboys or hackers). After analyzing a social construction of hacker activities and its perpetrators, the paper presents the ideological struggle for primacy in cyberspace: a struggle between contra-cultural values, interwoven in the very creation of internet space, and the values of post-modern digital capitalism; a struggle for the primacy fought between a computer »underground« and security industry.

Key words: cybercrime, criminology, victimology, offenders, victims

UDC: 343.3/7:681.324