Revija za kriminalistiko in kriminologijo | Ljubljana 48 | 1997 | 2, str. 179 - 188

Kriminaliteta v globalni komunikacijski mreži (internet)

Maja Zupančič *

Članek predstavlja internet, njegove zmogljivosti in uporabnike, posebej tudi slovenske uporabnike. Osrednja pozornost je namenjena kriminaliteti v kibernetskem prostoru, oblikam zlorab interneta, možnostim samovarovanja, nadzoru in cenzuri, metodam in poskusom cenzuriranja v nekaterih državah ter pravnim dilemam in problemom kazenskega pregona. V dodatku so navedene nekatere pomembnejše kriminološke in kazenskopravne raziskave, ki so jih med leti 1985 - 1995 izvedli v ZDA na temo računalniške kriminalitete.

Ključne besede: kriminaliteta, internet, računalniška kriminaliteta, kibernetski prostor, kazenski pregon.

UDK 343.3/.7:519.6

1. Kaj je internet in kaj omogoča

Internet (mednarodno omrežje mrež) omogoča uporabnikom računalnikov dostop do najrazličnejših storitev in neposredno komunikacijo. Gre za največje mednarodno računalniško omrežje, ki povezuje več milijonov računalniških uporabnikov. Povezuje okoli 70.000 manjših omrežij, 5 milijonov računalnikov in 50 milijonov uporabnikov.[1] Ker ni v lasti ali pod nadzorom nobene organizacije, ni mogoče natančno oceniti, za kako veliko omrežje v resnici gre. Znani so poskusi nekaterih organizacij, ki skušajo vendarle raziskati velikost tega omrežja. Ena izmed organizacij je npr. Network Wizards,[2] ki je januarja 1996 ugotovila, da je v internet vključenih okrog 240 tisoč ločenih računalniških omrežij v obliki imen področij (*domain names*) in več kot 9,4 milijona računalnikov gostiteljev (*host computers*).[3] Internet je tehnološki medij prihodnosti in omogoča uporabo najobsežnejšega vira informacij v današnjem času. Poznavalci sodijo, da gre za najhitreje rastoči medij sedanjosti in prihodnosti.

Internet se je razvil iz računalniškega sistema, ki ga je v sedemdesetih letih izdelalo ameriško obrambno ministrstvo. Namenjen je bil univerzitetnim in vojaškim raziskovalcem, omogočil pa naj bi jim neovirano delo, če bi del sistema (omrežja) postal neuporaben zaradi morebitnega jedrskega napada.[4] Zgrajen je bil kot informacijski sistem brez osrednjega upravljalca in lastnika, tako da nihče ne more nikogar izključiti iz omrežja. Kasneje so ga uporabljale ameriške univerze, ki so iskale možnosti za hitro izmenjavo informacij.

Internet omogoča izmenjavo neomejene količine informacij. Uporabniki se največkrat priključijo na oddaljen računalnik in imajo možnost žskočitiž v njegove podatkovne baze. Z možnostmi, ki jih nudi, prikličejo slike, zvok, video, prenašajo datoteke na osebni računalnik, nakupujejo izdelke z vtipkavanjem številk kreditnih kartic itd. Uporabniku so na voljo različne informacije in storitve, od strokovnih razprav z različnih področij, 'kiberpank subkulture',[5] do poljudnih tem in praktičnih nasvetov. Z njegovo pomočjo lahko prelistavamo revije, dobimo informa-

* Maja Zupančič, dipl. sociologinja, pripravnica v referatu za analitiko, Ministrstvo za notranje zadeve, Štefanova 2, 1000 Ljubljana.

[1] Unistar, 1996. Doswell, 1996.

[2] Network Wizard je ameriška organizacija, ki izdeluje, prodaja tehnične in programsker rešitve za računalniško in komunikacijsko industrijo. Vodi jo Mark K. Lottor, ki med drugim tudi skrbi za dvakrat letno izvedbo raziskave o številu uporabnikov interneta.

[3] Lowe, 1996.

[4] Weitemeier, 1996.

[5] Skupine, ki jih povezuje kibernetski prostor s posebnim kulturnim sistemom norm in načinov ravnanja.

cije za poslovneže, kuharske recepte, poiščemo najugodnejšo ponudbo o potovanjih in nakupih, preverimo vremenske napovedi, si ogledamo erotiko itd.6 Na internetu lahko dobimo informacije o različnih vladnih in nevladnih organizacijah. Od uradnih državnih predstavništev so že možni dostopi v baze ameriške vlade, OZN, EU in Nata. Prav tako je z njim omogočen vstop v velike svetovne knjižnice (Library of Congress, Bibliotheque de France, British Library itd.).

Mednarodno omrežje torej omogoča hiter dostop do informacij, prenose podatkov in datotek ter izredno hitro in razmeroma poceni komuniciranje med uporabniki. Nudi različne informacijske servise, med najbolj priljubljenimi pa so:[7]

Elektronska pošta (E-mail) - je zelo razširjena oblika komuniciranja in predstavlja enega glavnih servisov interneta. Omogoča pošiljanje pošte iz kateregakoli računalnika v omrežju na katerikoli elektronski naslov.

World Wide Web (WWW) oziroma 'svetovni splet' - omogoča uporabnikom omrežja, da si na različnih naslovih in straneh ogledujejo tekst, grafiko, zvok ali video. Postal je najbolj priljubljena storitev na internetu.

Gopher - je servis, ki omogoča preko enotnega vmesnika dostop do vseh vrst informacij. Organiziran je hierarhično v imenike, kjer posamezni element predstavlja zapis ali datoteko, iskanje podatkov po ključni besedi, novi imenik, iskanje osebe preko 'telefonskega imenika' ali priključitev na drugi računalnik. Podatke prikazuje v obliki imenikov ali datotek; večina strežnikov omogoča zanj tudi iskanje informacij.

Veronica - je storitev, ki po strežnikih Gopherja išče datoteke.

Usenet - je množično uporabljan servis interneta, ki organizira sporočila posameznikov po temah. Gre za skupine novic, ki imajo značilno zgradbo, uporabniki o njih izmenjujejo svoja mnenja, komentirajo prejšnja sporočila ali odpirajo nove razprave. Teme oziroma 'oglaševalske deske' so razporejene po poglavjih: znanost (sci), rekreacija (rec), družba (soc), računalništvo (copm), nedefinirana kategorija 'alternate' (alt) ipd.

Telnet - je servis, ki omogoča računalnikom, da delujejo kot terminali oziroma da drug računalnik uporabljajo tako, kot da bi bili nanj neposredno priključeni.

FTP (File Transfer Protocol) - so pravila za prenos datotek. Gre za program, ki prenaša datoteke med sistemi in posreduje uporabnikom zahtevane informacije. Uporablja se za povezovanje z 'gostiteljskimi' računalniki v internetu in za sprejemanje datotek iz njih. 'Gostiteljski' računalniki v internetu tako dovoljujejo vsakomur, da pregleduje njihove imenike in prebira ter prenaša zanj zanimive datoteke.

IRC (Internet Relay Chat) - omogoča pogovor, ki je podoben telefonskemu, le da je treba sporočilo vtipkati; komuniciranje samo poteka podobno kot preko CB radijskih postaj. Hkrati se lahko pogovarja več sogovornikov, ki se vključujejo po želji. Pogovor poteka tako, da vsi vse 'slišijo', čeprav se nahajajo na različnih delih sveta.

Internet Talk Radio - oddaja zvočne zapise (priljubljena oddaja z intervjuji je npr. 'Geek of the Week' [8]).

CUSeeMe - je videokonferenčni sistem uporabe interneta. Omogoča, da uporabniki vidijo in slišijo drug drugega na svojih računalniških zaslonih.

Danes so v internet povezani računalniki najrazličnejših operacijskih sistemov (UNIX, VMS, Windows, Windows NT, OS/2) in tipov (od osebnih računalnikov in zmogljivih delovnih postaj, do mini in super računalnikov). Računalniki so priključeni samostojno ali pa preko omrežja (lokalna mreža LAN ali globalno omrežje WAN). Vsa omrežja in vsi računalniki v internetu delujejo samostojno in neodvisno od drugih, za komunikacijski proces z internetom pa uporabljajo isti omrežni jezik TCP/IP.[9]

2. Uporabniki interneta

Internet danes omogoča dostop do najrazličnejših informacij ter je hitro in poceni komunikacijsko sredstvo. Zaradi njegove vse večje priljubljenosti se nenadzorovano širi tudi množica njegovih uporabnikov.

---

6 Cortese, 1996. Weitemeier, 1996

7 Več o tem v Lowe, 1996 in v revijah Moj mikro (1996), Kriminalistik (1996), idr.

8 'Geek of the Week' je tedenski intervju s pomembnimi posamezniki s področja tehničnih komunikacij (ugledni programerji, znani raziskovalci, inženirji), ki obravnavajo aktualne probleme in rešitve, ki se nanašajo na računalništvo, internet in ostala omrežja.

9 TCP/IP je standard, ki se v internetu uporablja za označevanje vsebine podatkovnih paketov in skrbi za točen prenos podatkov. TCP (Transmission Control Protocol) oziroma protokol za nadzor prenosa, se uporablja v povezavi s standardom IP (Internet Protocol).

Raziskave kažejo, da so tipični uporabniki omrežja stari okoli 30 let, moškega spola, izobraženi in imajo dobre dohodke. Prav ta skupina predstavlja idealno ciljno skupino za tržne strateg. Med rednimi uporabniki interneta je največ mladih, v glavnem študentov, narašča pa tudi število otrok in starejših. Leta 1995 so ugotovili 10 % mesečno rast uporabnikov interneta, v prvem polletju leta 1996 pa 40 % rast.[10]

Analizo o strukturi slovenskih uporabnikov interneta so pripravili na Fakulteti za družbene vede in jo predstavili v projektu RIS (Raba Interneta v Sloveniji, 1996). Povzemamo nekaj osnovnih ugotovitev raziskave:

- Tri četrtine uporabnikov (76 %) je moških, večinoma mlajših in bolje situiranih, le četrtina med njimi je žensk. Po ugotovitvah študij (tudi tujih) pa delež žensk med uporabniki narašča in strokovnjaki pričakujejo, da bodo v prihodnje internet enako pogosto uporabljali tako moški kot ženske.
- Skoraj polovica (44 %) uporabnikov interneta sodi v populacijo, ki se še izobražuje (osnovnošolci, dijaki, študenje). Drugo večjo skupino uporabnikov tvorijo zaposleni. Obe skupini se razlikujeta po dostopu do interneta in namenu uporabe. Dijaki in študentje imajo dostop do interneta predvsem preko šol in univerze, uporabljajo pa ga največkrat za izobraževanje. Zaposleni ga uporabljajo zlasti za iskanje poslovnih informacij, nanj pa so priključeni v svojih podjetjih.
- Tretjina uporablja internet dnevno.
- 17 % tistih, ki so v prejšnjih letih že uporabljali internet, ga v letu 1996 niso uporabljali. 83 % uporabnikov še naprej uporablja internet in možnosti, ki jih ponuja, oziroma je to vir informacij, ki se mu ne želijo odreči.
- 67 % uporabnikov meni, da je gmotno stanje njihovega gospodinjstva povprečno, 29 % nadpovprečno, 4 % pa podpovprečno. Slovenski uporabniki se glede na materialno stanje ne razlikujejo od uporabnikov drugod po svetu. Pričakujemo lahko, da bodo tudi slovenski uporabniki storitev interneta zanimiva in ciljna skupina za tržne načrtovalce in ponudnike.
- Tretjina uporabnikov ima dostop do interneta tudi od doma, tretjina to še načrtuje. Prevladuje dostop na podlagi skupnih gesel (35 %) in preko gesel sorodnikov in prijateljev (14 %).
- Slovenski uporabniki omrežja daleč največ uporabljajo storitve WWW (90 % uporabnikov), sledi elektronska pošta (82 % uporabnikov), pogosta pa je tudi uporaba FTP in Telneta.
- Najpogosteje uporabljajo internet za pridobivanje informacij, sledi raziskovalno delo, zabava in uporaba za poslovne namene.
- Po razširjenosti uporabe interneta med prebivalstvom sodi Slovenija med prvih 25 držav na svetu.

3. Nasprotja in dileme, ki jih je prinesel internet

Za vsako novo komunikacijsko tehnologijo je značilno, da ima dolgoročne posledice. Z internetom nastajajo nove možnosti povezovanja, ki poleg pozitivnih prinašajo tudi negativne posledice.

a) Kriminaliteta v kibernetskem prostoru (kiberprostoru)

S hitrim razvojem informatike in računalništva se spreminja tudi družba (v socialno/sociološkem, političnem, ekonomskem in gospodarskem smislu). Nastajajo nove oblike informacijskih komunikacij. Te vplivajo na družbeni razvoj, saj omogočajo mednarodno izmenjavo podatkov na različnih področjih, predvsem na področju znanosti, kulture in gospodarstva. Informatika pa se seveda ne uporablja samo v družbeno koristne, poštene in humane namene, pač pa tudi za dejanja, ki so družbeno nesprejemljiva in pogosto kazensko preganjana.[11] Razvija se računalniška kriminaliteta, problemi pa nastajajo pri njenem odkrivanju in kazenskem pregonu.

Z nastankom interneta, ki komunikacijam ne postavlja ovir, se je razvil nov družbeni prostor, ki ga je nemogoče nadzorovati v celoti in ki omogoča tako stare kot tudi povsem nove oblike računalniške kriminalitete.[12] Nekatere, zlasti razvite države, so se že soočile z njimi, zato razmišljajo o zakonodajnih rešitvah, ki bi omogočile pregon tovrstnih kaznivih dejanj. Ugotavljajo, da naraščata tako obseg kot tudi raznovrstnost načinov in oblik izvajanja računalniškega kriminala.[13]

S tem pa raste tudi število možnih žrtev računalniške kriminalitete. Vsak uporabnik interneta

[10] glej Moj mikro, 1996. Doswell, 1996. Harbot, 1996.

[11] Harbot, 1996.

[12] Weitemeier, 1996.

[13] Blakey, 1996

(in računalnika) je možna žrtev. Spletne strani WWW, ki so v svetovni mreži najbolj priljubljene, se skoraj popolnoma izmikajo državnemu nadzoru. Po omrežju potuje 'digitalno orožje',[14] kodirana sporočila in navodila 'lovcev' na informacije. 'Hekerji' [15] se po telefonski napeljavi tihotapijo v tuje računalnike, kriminalci pa se dogovarjajo za kriminalne posle. Tudi tajne službe uporabljajo internet kot svoje orodje.[16] Posledice zlorabe tega medija utegnejo biti zelo neprijetne, še posebno v velikih in kompleksnih družbah. Izgube (ugleda koroporacije, finančne izgube itd.) so zaradi vdora v računalniški sistem lahko usodne za normalno delovanje in celo obstoj celih podjetij in družb (npr. heker, ki je bil zaposlen pri telefonski družbi MCI je družbe MCI, AT&T in druge oškodoval za 50 milijonov dolarjev: zapisoval si je kode telefonskih kartic, jih dekodiral in prodajal naprej). Veliko vdorov v sisteme ni prijavljenih, saj je neprijetno, če nekdo ukrade 'strogo varovane' podatke in jih posreduje v svet. T.i. hekerje zelo redko odkrijejo. Komuniciranje preko elektronskih medijev je zato manj varno, kot bi si želeli uporabniki, ki ob priključitvi na internet le redko pomislijo na neštete možnosti negativnih posledic.

Z internetom so se pojavile nove oblike zlorab, za katere bo treba šele ugotoviti, kolikšna je škoda, ki jo povzročajo in kakšne so pravne poti za njihovo zatiranje. Med nove oblike zlorab uvrščamo t. i. črne kopije (neupravičeno razmnoževanje računalniškega programa za lastno uporabo) in 'piratstvo' (okoriščanje z razširjanjem nezakonito razmnoženih računalniških programov). Predstavljata nezakonito izkoriščanje avtorskih del in sodita med nove oblike računalniškega piratstva[17] v omrežju, ki ima posebej škodljive posledice za založnike programske opreme ter končne uporabnike.[18] Nove možnosti zlorabe nudi elektronska pošta, po kateri si kriminalci že pošiljajo šifrirana sporočila.[19] Tako na primer trgovina z orožjem ali mamili ne poteka več le po telefonu, ampak tudi po svetovni računalniški mreži. Pri tem si 'trgovci' pomagajo s 'kriptozaščito' (programi za šifriranje in dešifriranje sporočil), ki sporočila spreminja v neprepoznavne informacije. Naslovnik razbere prvotno besedilo le v primeru, če dobi geslo za ustrezni program, ki šifrirano besedilo dešifrira. Poleg takšnih kriminalnih dejanj najdemo na internetu tudi različne vsebine sporne narave, kot npr. ideološko propagando, pornografijo, propagiranje nasilja in napeljevanje h kaznivim dejanjem (uživanju drog, izdelavi bomb, terorizmu ...).[20]

Poleg klasičnega kriminala se v zvezi z uporabo interneta pojavljajo tudi vprašanja 'elektronske etike'. Posojanje ali prodajanje naslovov uporabnikov različnih mednarodnih mrež npr. ni nezakonito, vendar pa pri takem 'posojanju' in 'prodajanju' ne gre toliko za krajo podatkov kot prav za problem elektronske etike. Med uporabniki interneta, predvsem tistimi, ki uporabljajo elektronsko pošto in 'IRC', obstaja elektronski bonton ali 'netika'.[21] Kršitve pravil bontona se urejajo med uporabniki

---

[14] Je orožje, ki nima klasične oblike, a ima zato toliko večjo moč (ponavadi vsebuje pomembne informacije, ki se prenašajo po digitalnih poteh omrežja).

[15] Razlikovati je potrebno med *hekerji* (hackers) in *krekerji* (crackers) in telefonskimi *friki* (phone freaks). Splošno se uporablja izraz heker. *Hekerji*: heker je posameznik, ki uživa v raziskovanju programov, sam navdušeno, obsedeno programira in spoštuje lastna etična pravila, ki pravijo, da naj bo dostop do računalnikov vsakomur mogoč, informacije morajo biti svobodno dostopne, računalniki nam izboljšujejo življenje, oblast (politiki, vojski in pravosodju) pa ne gre zaupati. *Krekerji*: vdirajo in razbijajo zavarovane računalniške sisteme. *Friki*: umetniki vdiranja v telefonska omrežja.

[16] Zgonik, 1996.

[17] Organizacija BSA (Business Software Alliance - interesno združenje proizvajalcev in prodajalcev računalniške strojne in programske opreme) loči pet osnovnih oblik programskega piratsva (BSA, 1996): *ponarejanje* ('Counterfeiting': neavtorizirano reproduciranje in distribuiranje zavarovanih programov na disketah ali CD-ROM-ih v opremi, ki je po navadi tudi ponarejena), *nalaganje na trdi disk* ('Hard Disc Loading'; proizvajalci ali prodajalci pri prodaji računalnikov brezplačno opremijo računalnik z neavtoriziranimi programi), *mehko piratstvo* ('Softlifting'; podjetje ali večji uporabnik nabavi samo eno legalno kopijo programa in jo neavtorizirano reproducira na vse svoje računalnike), dajanje v najem ('Sofware Rental'; predstavlja novo absolutno avtorsko pravico in se kaže kot dajanje v najem primerkov avtorskega dela), *piratstvo elektronskih oglasnih desk* ('Bulletin Board Piracy'; neavtorizirana naložitev računalniškega programa na elektronsko oglasno desko).

[18] Geary, 1995.

[19] Icove, 1995.

[20] Quain, 1996. The Netly News, 1996.

[21] Pravila *netike* med drugimi tudi opredeljujejo, da naj bodo sporočila kratka in jedrnata, naj se po elektronski pošti ne pošilja nezaželenih oglasov, naj se nikoli brez dovoljenja ne objavlja zasebne elektronske pošte...

in upravljalci lokalnih omrežij v internetu. Uporabnik se lahko pritoži lokalnemu upravljalcu omrežja ali ponudniku dostopa do interneta, ki nato kršiteljem lahko celo odvzame dostop do omrežja.[22] Med hujše kršitve sodi potvarjanje osebnih podatkov pri pisanju pošte ali zlorabe pri naročanju blaga preko omrežja.

b) Oblike zlorab interneta

Razvoj informacijsko-telekomunikacijske industrije je ponudil nove možnosti za razmah kriminalitete, med trenutno najbolj aktivne pa uvrščamo zlorabo interneta. Po navedbah različnih avtorjev,[23] sodijo med najbolj razširjene in do sedaj znane naslednje oblike zlorabe interneta:

- **Neupravičeno prilaščanje avtorskega dela oziroma intelektualne lastnine**

Veliko informacij na mreži je namenjenih javni rabi. Besedila, slike, zvok, video lahko prenesemo na svoj računalnik in jih poljubno uporabljamo. Kopija elektronskega teksta se v ničemer ne razlikuje od izvirnika. Gre za novo obliko zlorabe intelektualne lastnine.

- **Pornografija**

Na internetu je dostopna dokaj široka ponudba pornografije. Raziskovalci z ameriške univerze Carnegie Mellon so ugotovili, da omrežje omogoča razširjanje ogromne količine pornografskega gradiva, da so uporabniki teh storitev predvsem moški in da je največje povpraševanje po gradivu za pedofile. Strokovnjaki in uporabniki pa vendarle ugotavljajo, da dostop do pornografije ni tako enostaven in da je ni v tako ogromnih količinah, kot so to poudarjali mediji, ki so javnost večinoma seznanjali le s tovrstno zlorabo interneta.

- **Elektronska trgovina**

Vsak nakup ali uporaba drugih komercialnih storitev v mreži pusti za seboj digitalne sledi. Pravilno povezane sledi podatkov se lahko uporabljajo za komercialne storitve, tržniki pa pri tem ostajajo neodkriti. Pri poslovanju s kreditnimi karticami obstaja veliko možnosti za njihovo zlorabo. Prav zaradi tega pa strokovnjaki razvijajo in za potrebe elektronske trgovine uvajajo elektronski denar, ki bo ščitil uporabnika omrežja pred zlorabo kreditnih kartic.

- **Banke podatkov o državljanih**

Z vdori v baze podatkov različnih ustanov (npr. zdravstvo, gospodarstvo, državna uprava) hekerji kršijo tajnost podatkov.

- **Politična propaganda skrajnežev**

Po internetu neonacisti širijo svojo propagando. 'Anarhistična kuhinja' spodbuja in napeljuje uporabnike k stanju družbenega kaosa ter posreduje navodila za izdelovanje nevarnih stvari in snovi. V tej skupini je dejavno tudi gibanje satanistov.

- **Terorizem**

Gre za spodbujanje k mednarodnemu terorizmu in terorističnim akcijam. V prihodnosti teroristi v svojih napadih ne bodo uporabljali le klasičnih metod nasilja, temveč bodo svoje teroristične akcije izvajali tudi v svetovnem omrežju z načrtnim uničevanjem informacijskih sistemov in baz podatkov. Pri tem sicer ne bo prihajalo do človeških žrtev, ampak do oškodovanja posameznih institucij. Poznavalci menijo, da bi se terorizem utegnil z ulic preseliti na žinformacijsko avtocestož.

- **Verski obračuni**

Preko interneta posamezniki in skupine pošiljajo žaljiva mnenja o posameznih verskih skupnostih. V omrežju že zasledimo prave verske obračune med verniki in oporečniki. Na eni strani uporniki (t. i. heretiki) žnapadajož cerkvenega poglavarja, na drugi strani pa najbolj zvesti verniki napadajo kritike.

- **Rasne nestrpnosti**

Ekstremistične skupine širijo po internetu sovraštvo, antisemitistične ideje, rasizem in druge za uporabnike žaljive ideologije. Ku Klux Klan ipd. zlorabljajo omrežje za širjenje svojih rasističnih prepričanj.

- **Žalitve in obrekovanja**

Žalitvam in obrekovanju so izpostavljene različne javne osebnosti, državniki in drugi funkcionarji.

- **Napeljevanja k nasilnim dejanjem**

Tovrstna napeljevanja so lahko uperjena zoper posameznika, manjšine ali skupine. Napeljevanje poteka z namernim razširjanjem napačnih informacij in zavajanjem ljudi.

- **Komunikacijsko sredstvo za organizirani kriminal**

Internet omogoča pranje denarja v 'kibernetski pralnici', ki nima geografskih meja, zlasti pa nudi možnosti za zlorabo elektronske pošte za načrtovanje, pripravo in izvedbo raznovrstnih kaznivih dejanj mednarodno organiziranih kriminalnih skupin.

- **Vdori v sisteme**

Vdori v različne finančne sisteme omogočajo med drugim denarni prenos (ob vdoru v bančni sistem), nadzor nad računalniškimi sistemi korporacij ipd.

---

22 glej Moj mikro, 1996.

23 Dibbell, 1995. Elmert-Dewitt, 1995. Harbot, 1996. Quain, 1996. Blakey, 1996. Icove idr., 1995.

- **Napeljevanje h kaznivim dejanjem in navodila za izvajanje le-teh**

Možno je napeljevanje uporabnikov interneta k uživanju drog, izdelovanju bomb in k drugim nesprejemljivim dejavnostim. Na internetu je mogoče najti celo navodila, kako izdelati bombo, izvesti samomorilsko dejanje, napotke za gojenje marihuane doma itd.

- **Zloraba elektronske pošte**

Gre za možnosti izsiljevanja, grožnje in žalitve lastnikov naslova elektronske pošte. Prav tako je mogoče namenoma preobremeniti elektronski naslov, ko nekdo želi drugemu onemogočiti komuniciranje preko elektronske pošte.

- **Računalniški virusi**

Po omrežju internet je možno pošiljati računalniške viruse z namenom, da se onemogoči delovanje informacijskih sistemov oz. računalniških naprav.

c) Možnosti samovarovanja

Zaradi pretoka velikih količin informacij preko omrežja internet se pojavlja vprašanje varstva podatkov. Uporabniki se največkrat ne zavedajo, da z dostopom do informacij, ki ga imajo sami, omogočajo tudi drugim uporabnikom dostop do lastnega informacijskega sistema in podatkov v osebnem računalniku ali v lokalnem omrežju.

K preprečevanju najhujših zlorab bo pripomoglo boljše softversko orodje. Najbolj enostavna zaščita pred vdorom iz zunanjih sistemov je npr. geslo in uporabniško ime[24]. Z razvojem tehnologije so na voljo vedno bolj zapletene metode varovanja. Najboljše do sedaj znano varstvo je t. i. 'požarni zid'.[25] Dodatno zaščito dosežemo s kodiranjem (enkripcijo) podatkov. Tudi vključitev MNZ-ja RS v omrežje internet je realizirana ob upoštevanju zahtevnih varnostnih vidikov in stališč (fizična ločitev ITSONZ-a od drugih omrežij, preprečevanje vstopov iz zunanjih sistemov, popoln nadzor ustreznih služb nad priključnimi točkami v zunanje sisteme, ločen sistem priključkov na zunanja omrežja, zavarovan z varnostno zaporo, ki ustreza strogim merilom glede varnosti pred računalniškimi vdori). Večji problem je varstvo pred zlorabo osebnih podatkov. Proti takšnim zlorabam se poleg navedene zaščite v nekaterih državah borijo z zakonodajo in kaznovanjem ter ozaveščanjem uporabnikov o spoštovanju elektronske etike.

Kljub temu pa nikoli ne bo varovala, ki bi zlorabe interneta popolnoma preprečilo, a pri tem ne bi omejevalo svobode izražanja. Prav ta je med najpomembnejšimi prednostmi interneta.

d) Nadzor in cenzura

Okvirje življenja in delovanja v sodobni družbi opredeljujejo zakonska določila, ki se razlikujejo od države do države. Internet je s svojo širino zbližal uporabnike iz različnih držav z različno zakonodajo.

Zaradi svoje globalnosti in vseprisotnosti informacij, do katerih omogoča dostop vsakomur, je internet in njegovo strukturo težko nadzorovati. Tako kot ni mogoče imeti celovitega pregleda nad vsebino, tudi ni institucije, ki bi bila organizacijski, finančni, politični in operativni nosilec njegovega delovanja. Internet ni v lasti ali pod nadzorstvom nekega organa ali posameznika, temveč je last vseh, ki ga uporabljajo.[26] Med uporabniki pa se seveda najdejo tudi taki, ki njegove možnosti izrabljajo za protizakonito delovanje.

Pravniki poskušajo ugotoviti, v katero vrsto medijev bi sploh lahko uvrstili internet; sprašujejo se, ali je internet mogoče prištevati k medijem, kot sta radio in televizija, ki ju lahko vlada lažje tehnično nadzoruje kot tiskane medije.[27] Trenutno interneta ni mogoče cenzurirati iz povsem tehničnih razlogov, kajti zasnovan je tako, da se cenzuri izogiba. Omrežje deluje tako, da podatki na svoji informacijski poti lahko potujejo po različnih poteh. Ponavadi informacije potujejo po najkrajši poti, če pa ob tem 'trčijo' na blokado, se njihova pot preusmeri. Omrežje zato pojmuje cenzuro kot 'motnjo'. Hkrati pa tudi v samem omrežju obstaja strah pred anarhijo, ki omogoča, da lahko vsakdo govori o čemerkoli, nihče pa ne odloča o ničemer.

Popolnega nadzora nad omrežjem seveda ni mogoče pričakovati. Cenzura potrebuje naslovnika, v internetu pa je ta neoprijemljiv. Mreža prav tako nima lastnika, ki bi ga bilo mogoče nadzorovati. Avtokratske vlade skušajo omrežje cenzurirati, ne vedo pa kako. Zagovorniki interneta pa želijo sami

---

[24] Icove idr., 1995.

[25] 'Požarni zid' (Firewall) so računalniki, ki na vhodu v sistem preprečujejo milijonom uporabnikov interneta dostop do internega računalniškega sistema s pomembnimi podatki. Požarni zid navadno uporablja gesla, ključe, alarmne naprave in druge ovire proti vsiljivcem. S tem programskim paketom je mogoče nadzorovati pretok podatkov v določene mreže in iz njih, je torej nekakšen varnostni ščit pred okolico.

[26] Diamond in Bates, 1995.

[27] Dibbell, 1995.

izumiti orodje, ki bi omogočalo (samo)cenzuro. Kljub temu, da se zavedajo možnosti zlorabe takega orodja (nekatere vlade bi ga lahko uporabljale za žfiltriranjež informacij) menijo, da je ta način primernejši kot pa sodno preganjanje tistih, ki pošiljajo ali sprejemajo sporne vsebine. Ne nazadnje je vsebino informacije le težko nadzorovati in cenzurirati, še posebej, ko se pojavi na zaslonu zunaj države, od koder je bila informacija poslana.[28] Tehnolog računalniške družbe Sun Mycrosystems Eric Schmidt meni, da bodo uporabniki omrežja tisti, ki bodo morali v prihodnosti spoštovati krajevne zakone; za uresničitev posameznih konkretnih cenzurnih predpisov pa bo na voljo primerna programska oprema (ki bo pregledovala sezname in po merilih lastnika PC-ja izločala nezaželena mesta; iskala nezaželene besede in izločala neprimerna besedila). Že danes pa lahko podjetja, ki omogočajo dostop do interneta, sama izločajo določene informacije iz omrežja.

e) Metode in poskusi cenzuriranja v nekaterih državah

Ameriška vlada je zasnovala sistem Clipper Chip, ki šifrira in dešifrira telefonske klice in elektronsko pošto na način, da so uporabniki varni pred vdorom kogarkoli razen vlade same. Vladni uradniki so trdili, da potrebujejo Clipper, da bodo z njim prestrezali in dešifrirali sporočila kriminalcev, tihotapcev mamil in teroristov. Nasprotniki prizadevanj vlade so v Clipperju videli le službo za nadzor nad svobodnim pretokom storitev po internetu.[29]

Ameriški zakonodajalci oblikujejo novo zakonodajo, ki naj bi prepovedovala predvajanje nespodobnih vsebin, čeprav se zavedajo, da je lahko sprememba neučinkovita ali celo protiustavna. Predlagajo spremembo že obstoječega zakona o spodobnosti sredstev komuniciranja. Veljavnost tega zakona naj bi razširili še na računalniška omrežja. Predlog dopolnila zakona prepoveduje širjenje nespodobnih gradiv po omrežju. Za vsakogar, ki priskrbi takšna gradiva mladini do 18 let, predvideva kazen 100.000 dolarjev in zaporno kazen do dveh let. Glede na način delovanja omrežja, bi tak zakon inkriminiral tudi vse operaterje [30] omrežja, ki bi bili odgovorni za vsako obliko nespodobnosti, ki bi jo kdo poslal na internet. S tem bi postalo vprašljivo delovanje celotnega interneta. Zagovorniki državljanskih pravic menijo, da bi zakon kršil pravico do svobode govora in pravico do komuniciranja. Opozarjajo tudi, da s takim posegom utegne omrežje nadzorovati najbolj stroga in najmanj strpna skupnost v državi.[31]

Tudi azijske vlade pripravljajo protipornografsko zakonodajo. Kitajska vlada uresničuje politiko popolne cenzure interneta. Vsi uporabniki interneta so se morali prijaviti na policiji, zveze s tujino potekajo le preko ministrstva za telekomunikacije. Vse računalnike, priključene na internet, bodo opremili s filtri, ki bodo poleg pornografije nadzorovali tudi vse informacije, ki naj bi žškodovale javnemu redu.

V **Singapurju** odloča o cenzuri političnih stališč in pornografije ministrstvo za informacije in umetnost.

Pravoverne islamske države, kakršna je npr. **Saudska Arabija**, strogo nadzorujejo dostop do interneta. Konservativni politiki se bojijo, da bo internet idealen medij za kriminalce, primeren za trgovino z mamili, teroristična dejanja ali vohunjenje, nad katerim ne bo imela država nobenega nadzora.

V **Franciji** razmišljajo o uvedbi sistema PICS (Platform for Internet Content Selection). Gre za sistem, ki deluje na podlagi samoocenjevanja.[32] Odgovorni za omrežje (državna in privatna podjetja ter posamezniki, ki ponujajo dostop do interneta) naj bi sami ocenjevali vsebino, poseben program na uporabnikovem računalniku pa bi izločil tiste skupine informacij, ki jih naročnik ne mara sprejemati. Prednost sistema PICS je, da ne omejuje pisanja na internetu, temveč omejuje samo tisto, kar uporabniki (pre)berejo. S samocenzuro je tako zagotovljena svoboda govora.

Nemški politiki razmišljajo o zakonu o multimedijih. V iskanju možnih rešitev skušajo razširiti določila obstoječe zakonodaje še na svetovno informacijsko mrežo.

Med 25 ukrepi **sedmih najbolj razvitih držav (G-7)** in **Rusije** je posebna pozornost namenjena nadzoru nad telematskimi sistemi, da bi skrajnežem preprečili pošiljanje navodil, ki bi napeljevala k izdelavi nevarnih predmetov.[33]

Evropska unija je napovedala, da se bo odločno

---

28 Quittner, 1996.

29 Alkalaj, 1996.

30 Operaterji so tehnični 'oskrbniki' omrežja, ki predvsem skrbijo, da izmenjava in pretok informacij po tistem delu omrežja, ki ga nadzorujejo, pravilno poteka. Skrbijo, da se na vozliščih mreže podatki usmerjajo na pravilno pot.

31 Diamond in Bates, 1995.

32 Alkalaj, 1996.

33 Weitemeiner, 1996; The Netly News, 1996.

lotila varstva človekovega dostojanstva in mladoletnikov pred nelegalno in še posebej pred pedofilsko vsebino. Komisija je o tem sprejela zeleno knjigo in napovedala številne dejavnosti, pri čemer se bolj kot za urejanje z direktivami zavzema za medvladno sodelovanje. Komisar za tehnologijo in informatiko Martin Bangemann poudarja, da je treba v tisto, kar nacionalne zakonodaje preganjajo kot kriminalno in nelegalno, zajeti tudi internet. Poglavitna odgovornost za posredovanje vsebine pri tem odpade na operaterje dostopa do interneta.

Poleg tega so nekatere države z namenom, da bi preprečile šifriranje kriminalnih informacij, omejile kriptografijo. V Franciji je šifriranje zasebnih sporočil prepovedano.[34] Nemci razmišljajo o zakonu, ki predpisuje uporabo kriptografije (z njim bi policiji in tajni službi olajšali branje zasebne elektronske pošte).

f) Pravne dileme in problemi kazenskega pregona

Internet spreminja definicijo skupnosti, briše zemljepisne meje, spodkopava navade, pravila in zakone obnašanja ter ravnanja. S pravnega, zakonodajnega in policijskega vidika so nevarne ravno tiste lastnosti interneta, po katerih se ta razlikuje od drugih medijev. To pa je njegova globalnost in univerzalnost, ki se lahko v 'nepravih' rokah sprevrže v sredstvo nasilja in omejenosti. Geografsko internet presega meje posameznih držav ter ne ločuje različnih vrednostnih sistemov in prepričanj. Iz tega izhajajo nekatere pravne dileme in problemi:

- **'Nepravosodnost' interneta**

Internet, kot tudi druga omrežja, ne predstavlja otipljivega fizičnega objekta, ampak je skupek omrežnih protokolov, ki omogoča prenos informacij po številnih posameznih mrežah. Z internetom se zato srečujejo mnoge sodne oblasti, saj neko sporočilo lahko potuje kjerkoli v globalni mreži in je na vpogled kateremukoli uporabniku, ki je nanjo priključen v katerikoli državi. Internet tako obstaja v okviru 'več-pravosodnega' sistema, vendar pa je funkcionalno 'ne-pravosoden', saj ga ni mogoče fizično locirati in omejiti.

- **'Neoprijemljivost' interneta**

Posledica elektronskega značaja izmenjave informacij in decentralizirane strukture interneta je, da ne pozna osrednjega nadzornega mehanizma ali določene centralne lokacije, skozi katero bi potekal informacijski promet na omrežju. Tako neoprijemljiv prostor je težko nadzorovati in še težje izvajati sankcije za kršitelje. Komuniciranje v omrežju lahko nadzoruje uporabnik sam (samocenzura), lahko je za to odgovoren pošiljatelj ali prejemnik informacij. Odgovorne pa so lahko tudi družbene institucije, morda nevladne organizacije ali kar vlada. Svobodno posameznikovo presojanje o tem, kaj naj javnosti posreduje preko interneta zato presega možnosti različnih organizacij ali celo vlad, da bi minimalizirale nepravilnosti pri njegovi uporabi in omejile možnosti zlorabe. Merila o tem, kaj pošiljati po kibernetskem prostoru, določa posameznik sam. Na njegove odločitve lahko vplivajo predvsem splošne družbene norme, posameznikova osebna etika, manj pa zakonski predpisi. Strokovnjaki in uporabniki pesimistično ugotavljajo, da je zakone težko postavljati v prostoru, ki je "povsod in nikjer", in da je težko varovati lastnino, ki nima fizične oblike in jo je mogoče množično kopirati in poljubno reproducirati. Vendarle pa bodo države morale sprejeti ustrezno zakonodajo, ki bo vsebovala elektronsko komunikacijsko pravo, upoštevala mednarodno pravo in nacionalne varnostne vidike.[35]

- **Relativnost vrednot v globalnem (kiber) prostoru**

Katera merila in pravila naj bi veljala v kibernetskem prostoru? Če sprejmemo stališče, da lahko moralna načela (ali predsodki) neke politične, etične ali verske skupnosti omejujejo vsebino informacij, potem je o tem vprašanju utopično pričakovati vse-splošni mednarodni dogovor - v prostoru brez meja je vsaka problematika za nekoga sporna.[36] Potreba po zakonodaji, ki bo na globalni ravni (ravni celega planeta) opredelila kibernetski prostor in njegove zakone in ki bo pri tem vendarle usklajena z že obstoječimi pravnimi sistemi, je zato velika. Treba bo definirati kazniva dejanja, njihove pojavne oblike, načine izvršitve, ugotoviti možnosti in načine za njihovo odkrivanje, spremeniti kazensko zakonodajo itd.

- **Odgovornost sistemskih operaterjev**

Na vprašanje ali je dobavitelj dostopa do interneta odgovoren tudi za vsebino, ki jo je mogoče priklicati po svetovnem omrežju, do danes še nimamo odgovora. Sistemski, mrežni operaterji so v dilemi, kajti z zakonom niso pooblaščeni za nadzor in čiščenje vsebine, ki se posreduje po omrežju oziroma nimajo pooblastil za to, da razsojajo o vsebini sporočil na internetu. Odločitev o tem prepustijo pošiljatelju oziroma sprejemniku.

34 Alkalaj, 1996.

35 Greenspoon, 1995.

36 Alkalaj, 1996.

- **'Računalniški policisti'**

Ker se zloraba interneta in druge oblike računalniške kriminalitete hitro širijo in spreminjajo, vanj pa so vpleteni izjemno izobraženi posamezniki, se bodo morali organi kazenskega pregona spopadati z njimi v sodelovanju z računalniškimi strokovnjaki. Zaradi tehnične narave te kriminalitete bo treba ustanoviti posebne policijske enote, specializirane za odkrivanje tovrstnih zlorab.

- **Kazenski pregon**

V zvezi z varstvom podatkov bo treba iskati pravne rešitve na vprašanja, katere podatke lahko policija ali javno tožilstvo zahtevata od naslovnikov elektronske pošte, v katerih primerih lahko oba mehanizma ukrepata ipd.[37] Računalniški kriminal ima lahko negativne posledice za posamezne uporabnike informacijskih orodij, lahko pa ogroža tudi nacionalno varnost (npr. računalniški hekerji vdrejo v državne vojaške sisteme in razkrijejo javnosti zaupne podatke, si prilastijo nadzor nad bančnim sistemom in po želji opravljajo prenos vrednostnih papirjev in denarja itd.). Ker so zlorabe zelo različne, je treba nenehno prilagajati metode odkrivanja, preiskovanja in načine dokazovanja. Gre za mnogo bolj kompleksne in zahtevne postopke kot jih poznamo v primeru odkrivanja drugih kaznivih dejanj.[38] V kibernetskem prostoru je zelo težko slediti namenom kriminalcev in še težje zbirati dokazno gradivo. Izkazalo se je, da so pri iskanju elektronskega dokaznega gradiva lahko v pomoč telefonski računi, tiskane informacije, računalniška oprema (hardver in softver), odkritje odtujenih baz podatkov, zaznave sprememb v računalniškem sistemu itd. Za uspešno policijsko in kriminalistično delo bi bilo treba čim hitreje natančno opredeliti pravilnik postopkov, ki bi vseboval analize pojavov, metode in napotke za odkrivanje, preiskovanje in dokazovanje. Policija in zavarovalnice bi morale delovati preventivno in informirati podjetja in posameznike, ki so uporabniki interneta, da zavarujejo svoje sisteme pred vdori in možnimi zlorabami, jih usposobiti za prepoznavanje zlorab, ter jih obvestiti o tem, komu lahko zlorabe prijavijo.[39]

Članek napisan decembra 1996.

Dodatek: Nekaj pomembnejših kriminoloških in kazensko-pravnih raziskav, ki so jih med leti 1985-1995 izvedli v ZDA na temo računalniške kriminalitete.

Parker, D.B., Smith, D.C., Turner, G.W., Sherizan, S. Računalniški kriminal: Priročnik o kazenskem pravosodju; Problemi in praksa. (Computer Crime: Criminal Justice Resource Manual; Issues and Practices.) 1989. 222 st. NCJ 118214.

McEwen, J.T. Enote za računalniško kriminaliteto; Problemi in praksa. (Dedicated Computer Crime Units; Issues and Practices.) 1989. 130 st. NCJ 118215.

Conly, C. Organiziranje za preiskovanje in kazenski pregon računalniške kriminalitete; Problemi in praksa. (Organizing for Computer Crime Investigation and Prosecution; Issues and Practices.) 1989. 126 st. NCJ 118216.

Nugent, H. Državni zakoni s področja računalniške kriminalitete. (State Computer Crime Statutes. RIA.) 1991. 12 st. NCJ 128780.

---

37 Icove idr. 1995.

38 prav tam

39 V svetu deluje organizacija CERT ('Computer Emergency Response Team'), ki koordinira pri reševanju incidentov, obvešča o novih varnostnih problemih, posreduje informacije in svetuje. Vendar pa CERT ne predpisuje varnostne politike, ne sproža pravnih postopkov in ne vzdržuje računalniških omrežij strank. Obveščanje in reševanje varnostnih problemov v računalniških omrežjih v Sloveniji spremlja organizacija SI-CERT, kateri vdore v sistem lahko sporočimo tudi na elektronski naslov (si-cert@arnes.si).

LITERATURA:

1. Alkalaj M.: Ko se začno z medijem ukvarjati politiki. **Delo** 9. novembra 1996, s. 39.
2. Blakey D.: Policing Cyberspace. **Policing Today** 1996, št. 1, str. 18-21.
3. Cortese A.: Here comes the Intranet. **Business Week** 26. februarja 1996, str. 46-49.
4. Diamond E., Bates S.: Law and Order Comes to Cyberspace. **Technology Review Magazine 1995**. oktober.
5. Dbbelln, J.: Muzzling the Internet. **Time**, 18. decembra 1995, str. 56.
6. Doswell B.: Internet under attack. Intersec, 1996, št. 6, str. 174-176.
7. Elmert-Dewitt, P.: Snuff Porn on the Net. **Time**, 20. februarja 1995, str. 69.
8. Geary J.: Piracy And Profit. Time, 27. novembra 1995, str. 70-71.
9. Greeenspoon R: U.S. Government Control Over Export of Scientific Research and Other Tehnical Data. **Michigan Internet Law**, 1995, Winter.
10. Harbot S.: Verbrechen im Cyberspace, **Kriminalistik**, 1996, št. 3, str. 194-198.
11. Icove D., Seger K., VonStorch W.: **Computer Crime**. OžReilly & Associates, Sebastopol 1995.
12. Internet v Sloveniji. Posebna izdaja revije **Moj mikro**, 1996.
13. Lowe D.: **Omrežja za telebane**. Pasadena, Ljubljana 1996.
14. Quain J. R.: Counter Terrorism sites. **Quianžs Web Review**, Daily Internet Site Reviews, 29. julija 1996.
15. Quittner J.: Free Speech for the Net. **Time Magazine**, 1996, št. 26.
16. Terrifying Anti-Terrorism. **The Netly News**, 1996.
17. UNISTAR-jev vodič do kiberprostora. Ljubljana, Tiskarna Kurir 1996.
18. Weitemeier I.: Internet - Medium der Zukunft. **Kriminalistik**, 1996, št. 6, str. 401-405.
19. Zgonik A.: Internet, planetarna računalniška mreža. **Delo**, (Sobotna priloga), 24. avgusta 1996, s. 31.

Crime in a global communication network (Internet)

Maja Zupančič, Graduate Sociologist, Section for Analysis, Ministry of Interior of the Republic of Slovenia, Štefanova 2, 1000 Ljubljana, Slovenia

The paper presents Internet, its capacities and users, particularly Slovenian users. Central attention is devoted to crime in cyber space, to various forms of Internet abuse, to possibilities of self-protection, to control and censure, to methods and attempts at censure in some states and to legal dillemas and problems of criminal prosecution. In the appendix are listed some of the important criminological and criminal law research studies on computer crime whitch were conducted in the United States in the period 1985-1995.

Key words: crime, Internet, cyberspace, computer crime, criminal prosecution

UDC 343.3/.7:519.6