KIBERANGELČKI UMAZANEGA OBRAZA

Tvrtko M. Šercar
Institut informacijskih znanosti, Maribor

Kontaktni naslov:
tvrtko.sercar@izum.si

Izvleček
Povod za nastanek tega članka je kampanja, ki so jo anonimni posamezniki lani in predlani vodili preko interneta z namenom diskreditirati vodstvo IZUM-a. Nakazan je pravni in tehnološki vidik kibernadlegovanja. Prikazano je, kako so se s kiberkriminalom spoprijele zakonodaje ZDA in EU. Namen članka je prepoznati kibernadlegovanje kot resni družbeni problem, ki si kot posebna vrsta kiberkriminala zasluži pozornost nacionalne zakonodaje tudi v Sloveniji. Največji problem je potegniti črto ločnico med kibernadlegovanjem, ki je svojevrstna kontinuiteta verbalnega dejanja, in zakonsko zaščiteno svobodo govora, ki je ena največjih vrednot demokratične družbe zahodne civilizacije.

Ključne besede
kiberkriminal; kibernadlegovanje; pravni vidik; tehnološki vidik; ZDA; EU

Abstract
The impetus for this article was the campaign conducted on the Internet last year and the year before by anonymous individuals trying to discredit Izum's management. Some of the legal and technological aspects of cyberstalking are pointed out, and ways of dealing with the problem of cybercrime, based on US and EU legislation, are also presented. The objective of the article is to have cyberstalking recognised as a serious social problem which merits, as a special type of criminal offense, the attention of the Slovenian legislature. The biggest problem is actually drawing a boundary line between cyberstalking which is a unique continuity of speech activities, and freedom of speech which is one of the greatest values of a democratic society in Western civilisation and protected by law.

Keywords
cybercrime; cyberstalking; legal aspect; technological aspect; USA; EU

UVOD

Povod za ta članek je kampanja, ki so jo anonimni posamezniki lani in predlani vodili preko interneta z namenom diskreditirati vodstvo IZUM-a. Čeprav je videti, da so to kampanjo opustili, je kibernadlegovanje (*cyberstalking*) splošni problem sodobne informacijske družbe, razsežnost katerega vedno bolj narašča.

Informacijske prometnice kot infrastruktura informacijske družbe se vedno hitreje razvijajo. Internet in druge telekomunikacijske tehnologije omogočajo napredek slehernega vidika družbe na vseh koncih sveta: pospešujejo trgovino, izpopolnjujejo izobraževanje in zdravstveno skrb, participativno demokracijo, olajšujejo sporazumevanje v družini, med prijatelji in ljubimci bodisi čez cesto bodisi okrog sveta. Kiberprostor je zaradi svojih številnih prednosti, kot so nizki stroški, enostavna uporaba in anonimnost, postal plodno polje tudi za protizakonita kriminalna dejanja.[1] Računalniki in internet so danes globalno in drugače obvezni sestavni del informacijske civilizacije in kulture, kibernadlegovanje pa je ena temnih senc te kulture.

Gre za relativno nova kriminalna dejanja, kot so:

- hekerstvo (hacking), krekerstvo (crackering), vključno z izdelavo računalniških programov tipa virus, worm itd.
- virtualna otroška pornografija,
- kibernadlegovanje/preganjanje žrtev.

Izraz kibernadlegovanje je bil skovan, da označi zlorabo interneta, e-pošte ali drugih e-medijev za nadlegovanje ali

preganjanje drugih oseb. Kot pri fizičnem nadlegovanju in preganjanju sta bila v mnogih online primerih nadlegovalec in žrtev sprva v družbenem stiku, kibernadlegovanje pa se je začelo, ko je žrtev poskusila prekiniti odnos.

Dejstvo, da kibernadlegovanje ne sloni na fizičnem stiku, ustvarja napačno sliko, da je bolj nedolžno kot fizično nadlegovanje. To pa ni res, saj postaja internet vedno bolj sestavni del zasebnega in profesionalnega življenja slehernega posameznika. Poleg tega anonimnost, ki jo omogoča internet, otežuje identifikacijo storilca.

Kibernadlegovanje omogoča:

- decentralizirana narava interneta,
- anonimnost kibernadlegovalcev,
- spletne strani z množico osebnih podatkov o nekem posamezniku,
- neustrezna zakonodaja, ki povečini ni dovolj specifična za ta problem in nima univerzalno veljavne definicije tega pojma.

Vse to istočasno otežuje odkrivanje in kazensko preganjanje storilca tovrstnega kriminalnega dejanja. Ob tem pa je treba vzeti v obzir tudi zakonodajo o verbalnih dejanjih. Znan je primer *Prvega amandmaja k ustavni listini ZDA,* ki ščiti pravico do svobode govora in izražanja.

Kot rečeno, prvi pogoji za legitimno kriminalizacijo posameznih vrst računalniških kriminalnih dejanj so predvsem jasne, nedvoumne in stroge zakonske definicije tovrstnih dejanj.

Vendar poleg pravnega vidika obstaja tudi tehnološki problem. Od tega, kje se je računalniško kriminalno dejanje zgodilo, je odvisno, katera oblast (država) je pristojna, da zakonsko ukrepa. V ameriški sodni praksi je znan primer 19-letnega mladeniča Kammersella, ki se je preko svojega domačega računalnika v Riverdalu (država Utah v ZDA) prijavil na ISP (Internet Services Provider) AOL (America Online) in odposlal grožnjo o podstavljeni bombi na računalnik Ogden Service Center, upajoč, da bo njegova zaposlena prijateljica zaradi grožnje prej zapustila službo in prišla na sestanek z njim. Ker je vsako sporočilo, odposlano preko AOL-a, avtomatsko posredovano iz države porekla na AOL-ov glavni strežnik v Virginiji, preden gre na končno destinacijo – v tem primeru nazaj v državo Utah, se zastavlja resno pravno vprašanje, ali je za dejanje Kammersella pristojno sodišče v državi Utah ali zvezno sodišče.

Globalna narava računalniškega kriminala terja mednarodni/meddržavni konsenz o teh vprašanjih, sicer se lahko čezmejna preiskovanja tolmačijo kot zelo očitna kršitev suverenosti določene države.

PRIMER ZDA

Države z najrazvitejšo informacijsko družbo in inovativno družbo znanja so nesporno Združene države Amerike. Poleg tega, da ZDA vodijo po participativni demokraciji, relativno nizkem koeficientu socialne neenakosti, državljanskih pravicah, znanosti in umetnosti, gospodarski in vojaški moči (skratka so vodilna država v sodobni informacijski civilizaciji kot centralni civilizaciji sedanjosti), [2] so se morale tudi kot prve spoprijeti s problemom kibernadlegovanja na najvišjem nivoju državne oblasti.

Po statističnih podatkih, ki še niso popolni in še ne zajemajo vseh držav, je bilo v ZDA do konca leta 2000 zabeleženih 10,2 mio žrtev nadlegovanja (8,2 mio žensk in 2 mio moških). Vse to se je zgodilo samo v zadnjih treh ali štirih letih. V tem času je v ZDA imelo dostop do interneta 80 mio odraslih oseb in 10 mio otrok. Neka raziskava je pokazala, da se 25 % primerov nadlegovanja lahko klasificira kot kibernadlegovanje. Podatki so že tedaj kazali, da je kibernadlegovanje resen in rastoč problem.[3]

Po drugem viru [4] je teroriziranih žensk v ZDA na leto približno 1 mio. Čeprav nadlegovanje ni spolno specifičen kriminal, prizadeva ženske 75–80 % tovrstnih kriminalnih dejanj. Zanimivo je, da so žrtve večinoma navadni ljudje, ne pa imenitne osebe. Od zgodnjih devetdesetih let je distribucija žrtev v ZDA bila s tega vidika naslednja: navadni državljani 51 %, imenitne osebe 17 %, preostalih 32 % pa so bile manj znane osebe iz zabavne dejavnosti.

Po podatkih neprofitne organizacije za pomoč žrtvam kiberkriminala CyberAngels [5] je bilo leta 1999 v svetovnem kiberprostoru približno 63.000 nadlegovalcev in 500.000 žrtev.

Da je temu tako, potrjujejo tudi podatki, ki jih zbirajo ponudniki internetnih storitev (ISP).

Večina glavnih ponudnikov internetnih storitev v ZDA ima naslove za prijavo zlorabe ali kibernadlegovanja po e-pošti. Splošno se ta naslov glasi “abuse@[the ISP’s domain]”, npr. “abuse@aol.com”. Toda v praksi so predvsem osredotočeni na nezaželeno komercialno e-pošto (*spamming*, *mail-bombing*) po naročilu njihovih uporabnikov, ne pa na kibernadlegovanje, saj je taka zaščita, predvsem zbiranje podatkov, zaradi decentralizirane narave interneta po njihovi oceni draga in težka.

ZDA imajo že zelo pestro in razvito informacijsko, institucionalno in zakonsko infrastrukturo za boj proti kibernadlegovanju in kiberpreganjanju.

Pomemben del prizadevanj se nanaša na izobraževanje in zaščito potrošnikov. Znan je izobraževalni projekt Online

Public Education Network (OPEN) iz leta 1996, ki svetuje, kako ravnati ob prevarah, kako zmanjšati skrbi staršev in zaščititi zasebnost. Namen javnega servisa GetNetWise [6] je pomoč staršem in otrokom pri uporabi interneta in zaščita pred pornografi, hekerji, nadlegovalci in drugimi, ki zlorabljajo internet, na način, ki drži uporabnike na razdalji "en klik od" (One Click Away). Internetna industrija proizvaja tudi orodja v klepetalnicah za blokiranje sporočil tistih posameznikov, ki grozijo. Ponudniki internetnih storitev tudi filtrirajo vsebine na strežnikih (gated communities), ki je namenjena otrokom in drugim uporabnikom. Predvsem je zaželeno sodelovanje med online industrijo in policijo ter med ISP-ji in žrtvami kibernadlegovanja. ISP-ji tako priporočajo žrtvam, naj kopirajo vse e-maile, ki jih pošiljajo kibernadlegovalci; predlagajo jim, da pogosteje spreminjajo gesla in druge podatke za identifikacijo. V neki fokusni skupini žrtev kibernadlegovanja, ki jo je organiziralo Ministrstvo za pravosodje ZDA, so udeleženci poudarili pomembnost strokovne pomoči zdravnikov, delavcev za zaščito otrok, šolskega osebja in delodajalcev ...

Najstarejša in največja organizacija za varnost na internetu je že omenjena organizacija CyberAngels, ustanovljena leta 1995; je v pomoč tistim, ki sumijo, da bodo postali žrtve hekerjev, tistim, ki jih skrbijo virusi v računalniku, tistim, ki se želijo online naučiti več o zaščiti otrok, in tistim, ki so žrtve online nadlegovanja ali preganjanja. Pomoč zagotavljajo v angleškem, španskem, francoskem in nemškem jeziku.

GetNetWise je javni servis korporacij, ki se ukvarjajo z internetnimi dejavnostmi, in organizacij, ki opravljajo javno službo, njihov namen je, kot rečeno, držati uporabnike na razdalji "en klik od".

Institute for Security Technology Studies: A National Center For Cybersecurity and Counterterrorism Research, Development & Analysis (ISTS) [7] v ZDA je organizacija kiberpolicajev, strokovnjakov za računalniški kriminal. Pri ISTS deluje International Association of Computer Investigative Specialists (IACIS) [8], prostovoljna neprofitna korporacija strokovnjakov, ki so se posvetili izobraževanju na področju računalniške forenzične znanosti o sredstvih in načinih uničevanja bodisi dokazov bodisi računalniških sistemov ali obojega. Tam so leta 1991 skovali izraz računalniška forenzična znanost.

Z računalniško forenzično znanostjo in z izobraževanjem na tem področju se ukvarja tudi New Technology Inc. (NTI) v ZDA.[9] NTI naj bi imel največji laboratorij za računalniško forenzično znanost v svetu.

Women Halting Online Abuse (WHOA) se ukvarja z izobraževanjem internetne skupnosti o online nadlegovanju, usposabljanjem žrtev nadlegovanja in oblikovanjem politik, po katerih se sistemi lahko prilagajajo z namenom ustvariti okolja brez nadlegovanja. WHOA podpira pravico do svobode govora online in drugače, vendar meni, da svobodni govor, ki vključuje grožnje emocionalnemu in fizičnemu varstvu, ni zakonsko zaščiten. Naloga WHOA je ščititi ljudi pred nadlegovanjem, ki temelji na spolni, rasni, etnični in starostni neenakosti. Predvsem je organizacija žensk, ki s statističnimi podatki predstavljajo večino žrtev.[10]

Search [11] je konzorcij pravosodnih uradnikov iz vseh držav v ZDA, ki skrbi za boljše pravno informiranje in učinkovito uporabo informacijske tehnologije v institucijah pravosodnega sistema.

Privacy Rights Clearinghouse (PRC) [12] je neprofitni program za izobraževanje, raziskave in zastopanje potrošnikov. Publikacije PRC-a so v pomoč pri zaščiti osebnih podatkov in zasebnosti.

Stalking resource center je del National Center for Victims of Crime (NCVC) za različne informacije, dokumentacijo in publikacije o nadlegovanju.[13]

V februarju leta 1999 je Al Gore, tedanji podpredsednik ZDA, zaprosil državnega odvetnika (Attorney General), da razišče naraščajoči problem kibernadlegovanja, avgusta istega leta pa je predsedniku ZDA posredoval poročilo [14], v katerem je:

- obravnaval naravo in razsežnost kibernadlegovanja kot družbenega pojava,
- opisal odziv zakonodaje, industrije in skupin žrtev na ta problem,
- analiziral adekvatnost zveznih zakonov in zakonov posameznih ameriških držav v zvezi s kibernadlegovanjem,
- podal priporočila, kako se boriti proti temu naraščajočemu družbenem problemu.

Ker univerzalna sprejeta definicija kibernadlegovanja ni obstajala, je bil v poročilu izraz definiran kot uporaba interneta, e-pošte in drugih e-oblik sporazumevanja z namenom anonimnega nadlegovanja drugih oseb.

Večina zakonov ameriških držav obravnava nadlegovanje žrtve kot ponavljanje groženj z nasiljem, nekateri zakoni vključujejo tudi grožnje žrtvini ožji družini, nekateri pa kot nadlegovanje kvalificirajo tudi dejanja, ki samo implicirajo grožnjo. Praviloma se nadlegovanje in nasilje začne kot anonimno zaplotništvo in ga je treba takoj vzeti zelo resno.

Borbo proti otroški pornografiji na internetu in seksualnemu izrabljanju otrok je začel Federal Bureau

of Investigation (FBI) v letu 1995. Za tovrstna dejanja, ki se začnejo z online stikom z otrokom, je že do konca decembra 1998 bilo obsojenih 232 oseb. V pomoč staršem je FBI pripravil tudi online Parent's Guide to Internet Safety.[15]

Drugi najpogostejši objekt seksualnega kibernadlegovanja moških so ženske.

Čeprav gre za stari problem, je nadlegovanje, vključno s kibernadlegovanjem, pritegnilo pozornost zakonodajalcev šele v zadnjem desetletju prejšnjega stoletja.

Prvi zakon o tradicionalnem nadlegovanju je bil sprejet v državi Kalifornija leta 1990, kibernadlegovanju pa se še vedno ne posveča toliko pozornosti, kot si je ta problem zaradi svoje razsežnosti zasluži. Ker kibernadlegovanje zelo pogosto vključuje tudi grožnje z umorom in ugrabitvijo, žalitve druge osebe, njenega ugleda in lastnosti, se lahko obravnava tudi po zakonu o tradicionalnem nadlegovanju.

Danes imajo podobne zakone v vseh 50 državah in Washingtonu D.C. Leta 1999 je približno 1/3 držav imela zakon proti nadlegovanju, ki je izrecno zajemal kibernadlegovanje preko interneta, e-pošte, pozivnikov (pagerjev) ali drugih e-medijev.

Po zveznem zakonu je prenos katerega koli sporočila v meddržavni in zunanji trgovini, ki vsebuje poskus žaljenja druge osebe, zločin, za katerega je predvidenih do 5 let zapora in 250.000 USD kazni. Leta 1998 je Clinton podpisal zakon, ki ščiti otroke pred online nadlegovanjem.

Izhajajoč iz pomanjkljivosti obstoječih zakonov (zveznega in državnih) je zvezni javni tožilec v svojem poročilu za predsednika iz leta 1999 [16] predlagal sprejetje zakona o zatiranju kibernadlegovanja v vseh državah. Na zvezni ravni naj bi bil zakon dopolnjen, dopolnitve pa bi morale biti tehnološko nevtralne, to pomeni, da ne bi smele biti v nasprotju z zakoni posameznih držav in lokalnih skupnosti ter s Prvim amandmajem, ki ščiti svobodo govora, in interneta kot tehnologije, ki svobodo govora omogoča. Kibernadlegovanje namreč lahko vključuje pomembne elemente svobodnega govora, kar pa ne zmanjšuje javne potrebe po zakonski ureditvi in še ne pomeni, da bi sprejetje zakonskih predpisov na kateri koli način smelo preprečevati svobodo govora, ki jo jamči Prvi amandma k ustavni listini ZDA.Vrhovno sodišče ZDA je že leta 1969 potrdilo, da vlade posameznih držav lahko kriminalizirajo resne grožnje, ne da bi pri tem kršile Prvi amandma. Vendar je treba biti posebej pozoren pri pripravi zakonov o kibernadlegovanju, da ne bodo v nasprotju z ustavo zajamčeno svobodo govora, kot so npr. politični protesti in druge oblike legitimnega ravnanja.

Zakonsko ukrepanje otežuje več dejavnikov:

- Žrtve kibernadlegovanja po večini nočejo poročati o tovrstnih dejanjih bodisi zaradi tega, ker ne vedo, da predstavljajo kriminalno dejanje, bodisi ker ne pričakujejo, da jih bodo policija in drugi organi pravnega reda resno vzeli.
- Večina državnih organov za uresničevanje zakona se zaenkrat ne zaveda, kako resen družbeni problem je kibernadlegovanje, niti niso usposobljeni za preiskovanje kiberkriminala.
- Zakoni za zaščito zasebnosti pogosto omejujejo možnost policije, da preiskuje kriminalce v kiberprostoru.
- Pri kibernadlegovanju gre za dejanja preko komercialnih online servisov, zaradi česar je problem še težji. Servisi zagotavljajo anonimno sporočanje preko interneta, in sicer v obliki prostih elektronskih poštnih predalov na spletni strani. Druga oblika vključuje poštne strežnike, ki po naročilu brišejo identifikacijske podatke iz e-pošte; s pošiljanjem e-pošte skozi več takih servisov kibernadlegovalec skoraj popolnoma doseže anonimnost sporočila, kljub temu pa lahko pusti svoje elektronske sledi na spletu kot vlomilec prstne odtise na kraju zločina.

Velemesti, kot sta Los Angeles in New York, sta ustanovili posebne time za preiskovanje kibernadlegovanja. FBI ima po vsej Ameriki oddelke za računalniški kriminal kot tudi National Infrastructure Protection Center v Washingtonu. Ministrstvo pravosodja je znotraj oddelka za kriminal leta 1996 ustanovilo sekcijo za računalniški kriminal in intelektualno lastnino. Vsak urad javnega tožilca na lokalni in državni ravni v ZDA ima tudi prosekutorje z izkušnjami za računalniški kriminal. Toda za borbo proti kibernadlegovanju je najpomembnejše splošno razumevanje kiberpojava.

V prvem uspešnem sodnem postopku po novem zakonu o kibernadlegovanju v državi Kaliforniji je bil leta 1999 neki moški zaradi spolnega kibernadlegovanja obsojen na 6 let zapora.

Za predsednika ZDA je podobno poročilo o protizakonitih dejanjih na internetu v marcu leta 2000 izdelala posebna delovna skupina pod naslovom *Elektronska meja: izziv zakonsko nedovoljenih dejanj, ki vključujejo uporabo interneta*.[17] Skupina je obdelala naslednje vrste kriminalnih dejanj:

- prevare preko interneta,
- online otroško pornografijo, zvabitev otrok in sorodne aktivnosti,

- prodajo prepovedanih drog in kontroliranih substanc preko interneta,
- prodajo orožja preko interneta,
- kockanje preko interneta,
- prodajo alkohola preko interneta,
- online prevare varnostnih služb,
- piratstvo programske opreme in kraja intelektualne lastnine.

PRIMER EU

Svet Evrope je leta 2001 sprejel *Convention on Cybercrime* [18] – prvi mednarodni sporazum o kiberkriminalu. Konvencija je rezultat štiriletnega dela ekspertov iz Evrope pa tudi iz ZDA, Kanade, Japonske in nekaterih drugih držav, ki niso članice Sveta Evrope. V preambuli dokumenta so za glavni cilj postavili zagotavljanje pomoči kriminalni policiji pri zaščiti družbe pred kiberkriminalom, posebej še z ustrezno zakonodajo in izboljšanim mednarodnim sodelovanjem.

Kiberkriminalna dejanja po tej konvenciji so:

- Napadi na zaupnost, integriteto in dostopnost računalniških podatkov in sistemov:
  - nedovoljen dostop do računalniških sistemov,
  - nedovoljeno preprečevanje prenosa privatnih računalniških podatkov,
  - nedovoljeno poškodovanje, brisanje, popačevanje, zamenjava ali skrivanje računalniških podatkov,
  - nedovoljeno vmešavanje v delovanje računalniških sistemov z vnosom, prenosom, poškodovanjem, brisanjem, popačevanjem, zamenjavo ali skrivanjem računalniških podatkov,
  - nedovoljena izdelava, prodaja, uvoz, distribucija ali drugačno dejanje (sredstev, vključno z računalniškimi programi, projektiranimi ali prilagojenimi za namene kriminalnih dejanj, navedenih v prejšnjih alinejah, razen za potrebe testiranja ali zaščite računalniških sistemov; računalniškega gesla, kode za dostop ali podobnega podatka za dostop do računalniških sistemov za namene kriminalnih dejanj, navedenih v prejšnjih alinejah, razen za potrebe testiranja ali zaščite računalniških sistemov).
- Napadi na računalnike:
  - računalniški ponaredki,
  - računalniške prevare.
- Kriminalna dejanja v zvezi z vsebino:
  - otroška pornografija.
- Kršenje avtorske pravice in sorodnih pravic.

Jurisdikcija posamezne države se lahko nanaša samo na njen teritorij, ladje in letala ter njene državljane.

Konvencija ureja tudi mednarodno sodelovanje med državami, saj se računalniške mreže vedno bolj globalizirajo.

Glavna načela v zvezi z mednarodnim sodelovanjem se nanašajo na:

- izročitev (ekstradicijo),
- medsebojno pomoč pri preiskovanjih, sodnih postopkih in zbiranju e-dokazov o kriminalnih dejanjih.

SKLEPNE MISLI

1. Kibernadlegovanje je danes pereč problem informacijske družbe.
   V tem hipu samo ZDA, najbolj razvita informacijska družba v sedanjem svetu, prepoznava – sociološko in zakonsko – kibernadlegovanje kot posebno vrsto kriminalnega dejanja in kot splošni družbeni problem. Po statističnih podatkih [19] je prevalencija kibernadlegovanja v razvitih informacijskih družbah v hitrem porastu.
   Kot skorajšnjo članico Evropske unije obvezuje *Konvencija o kiberkriminalu* Sveta Evrope tudi Slovenijo. Vendar, kot je pokazano, v *Konvenciji* kibernadlegovanje ni prepoznan pojav.
   Če je bila povod za ta članek kampanja preko interneta z namenom moralne in intelektualne difamacije (blatenja, sramotenja) vodstva IZUM-a, ki je imela nekatera obeležja kibernadlegovanja (anonimnost, repetitivnost, žaljenje, napadalnost), je namen članka prepoznati kibernadlegovanje kot resni družbeni problem, ki si kot posebna vrsta kiberkriminala zasluži tudi pozornost nacionalne zakonodaje.
2. Razlikovanje med svobodo govora in kibernadlegovanjem je delikatna (predvsem sodniška) naloga. Največji problem v zvezi s kibernadlegovanjem je namreč ugotoviti, kdaj gre za zakonsko zaščiteno svobodo govora, ki je ena največjih vrednot demokratične družbe zahodnega tipa, in kdaj za kibernadlegovanje in kiberpreganjanje izbrane žrtve, saj gre v obeh primerih za verbalno dejanje, ki predstavlja svojevrstni kontinuum. Da bi lahko med njimi v konkretnem primeru povlekli črto ločnico, minimalno potrebujemo:
   - univerzalno veljavno in natančno definicijo kibernadlegovanja, ki je obenem tudi zakonsko uveljavljena;
   - pripravljenost žrtve, da prijavi kriminalno dejanje, ki se nad njo vrši, in sodeluje z organi pravnega reda, vključno s policijo, na nacionalni in mednarodni ravni;
   - enote preiskovalnih služb in policije, ki obvladajo računalništvo (kiberdetektivi in kiberpolicaji);
   - nacionalno sodstvo, ki problem pozna teoretično in ima praktične izkušnje z ločevanjem zakonsko

zaščitene svobode govora od kibernadlegovanja, ki je po zakonu kriminalno dejanje.

Zakonodaja, sodišča in policija bi se morali zavedati eskalacije kibernadlegovanja in zastaviti strategije za reševanje teh problemov znotraj državnih kazenskih sistemov.

3. Kljub napredku veljavna zakonodaja ne more slediti tehnološkemu razvoju, prav tako pa ne more v korak s kriminalom, vključno s kiberkriminalom.

Reference

[1] Cyberstalking: A New Challenge for Law Enforcement and Industry. A Report from the Attorney General to the Vice President, August 1999. Pridobljeno 17. 4. 2000 s svetovnega spleta: http://www.cybercrime.gov/cyberstalking.htm.

[2] Cyberstalking: A New Challenge for Law Enforcement and Industry. A Report from the Attorney General to the Vice President, August 1999.

[3] Wilkinson, D. (1995). Central Civilization. Sanderson CWS. Citirano po: Makarovič, J. (1997). Nova prostorno-časovna obzorja v družbenih znanostih. *Nova revija* april-maj 1997, 16, 180–181, 173–183.

[4] Radosevich, A. C. (2000) Thwarting the stalker: Are anti-stalking measures keeping pace with today's stalker? University of Illinois law review, 4, 1371-1395. Pridobljeno 12. 1. 2004 s svetovnega spleta: http://home.law.uinc.edu/lrev/publications/2000s/2000/2000_4/radosevich.html.

[5] Pridobljeno 12. 1. 2004 s svetovnega spleta: http://www.cyberangels.org.

[6] Pridobljeno 12. 1. 2004 s svetovnega spleta: http://www.getnetwise.org.

[7] Pridobljeno 12. 1. 2004 s svetovnega spleta: http://www.ists.dartmouth.edu/text/ISTS/press-releases/july15_03.php.

[8] Pridobljeno 12. 1. 2004 s svetovnega spleta: http://www.ists.dartmouth.edu/IRIA/projects/wlwl/iacis.htm.

[9] Pridobljeno 12. 1. 2004 s svetovnega spleta: http://www.forensics-intl.com/def4.html .

[10] Pridobljeno 12. 1. 2004 s svetovnega spleta: http://www.feminista.com/archives/vlnl/whoa.html.

[11] Pridobljeno 12. 1. 2004 s svetovnega spleta: http://www.search.org/aboutus-contact/default.asp.

[12] Pridobljeno 12. 1. 2004 s svetovnega spleta: http://www.privacyrights.org.

[13] Pridobljeno 12. 1. 2004 s svetovnega spleta: http://www.ncvc.org.

[14] Cyberstalking: A New Challenge for Law Enforcement and Industry. A Report from the Attorney General to the Vice President, August 1999.

[15] Pridobljeno 17. 4. 2000 s svetovnega spleta: www.fbi.gov.

[16] Cyberstalking: A New Challenge for Law Enforcement and Industry. A Report from the Attorney General to the Vice President, August 1999.

[17] Pridobljeno 12. 1. 2004 s svetovnega spleta: http://www.usdoj.gov/criminal/cybercrime/unlawful

[18] Pridobljeno 12. 1. 2004 s svetovnega spleta: http://wwwconventions.coe.int/Treaty/en/Treaties/Html/185.htm.

[19] Cyberstalking: A New Challenge for Law Enforcement and Industry. A Report from the Attorney General to the Vice President, August 1999.