UNIVERZA V LJUBLJANI
FAKLULTETA ZA DRUŽBENE VEDE

Matjaž Vidic

Ekstremizmi na internetu

Magistrsko delo

Ljubljana, 2011

UNIVERZA V LJUBLJANI
FAKLULTETA ZA DRUŽBENE VEDE

Matjaž Vidic

Mentor: doc. dr. Uroš Svete
Somentor: red. prof. dr. Vasja Vehovar

Ekstremizmi na internetu

Magistrsko delo

Ljubljana, *2011*

Zahvala

Mentorju dr. Urošu Svetetu in somentorju dr. Vasji Vehovarju za nenadomestljivo strokovno pomoč in vse ideje ter vzpodbude pri nastajanju magistrske naloge.

Sodelavcem, ki so me podpirali, pomagali in svetovali.

Posebna zahvala gre Ani, Vidi in Jolandi.

Ekstremizmi na internetu

V nalogi bom predstavil način delovanja domačih in tujih preiskovalnih organov, ki preiskujejo in preprečujejo kazniva dejanja, storjena s pomočjo interneta. Namen magistrskega dela je opisati metode in taktiko preiskovanja kaznivih dejanj različnih ekstremizmov, kot so terorizem, nacionalizem, rasizem, levi in desni politični ekstremizem in ne nazadnje sovražni govor, storjenih s pomočjo interneta. V magistrskem delu je predstavljeno področje računalniškega kriminala in pravna ureditev v Sloveniji ter zakonska podlaga za odkrivanje in preprečevanje ekstremizma na internetu. Obravnavane so oblike računalniškega kriminala, saj se tudi pri nas v vse večjem številu pojavljajo različne in nove oblike kaznivih dejanj, ki jih izvajajo ekstremistične skupine in so povezane s kibernetskim prostorom. Analiza problema v magistrskem delu je lahko zanimiva in uporabna tako v kriminalistični policiji kot tudi za zakonodajalca.

Težava pri odkrivanju kaznivih dejanj s pomočjo interneta je v tem, da se preiskovalci srečujejo z elektronskimi dokazi in morajo biti skrajno previdni pri zbiranju in varovanju, saj se lahko hitro poškodujejo ali uničijo. Internet ne pozna državnih mej, ne pozna družbenih razlik, ne pozna časovnih, jezikovnih ali geografskih razlik. Zaradi tega je pomembno mednarodno sodelovanje varnostnih organov. Prav tako je pomembno, da imajo države, kolikor je le možno, usklajeno zakonodajo, ki pokriva ekstremizme na internetu, in na ta način lahko učinkoviteje sodelujejo pri preiskavah. Bistven izziv pri preiskav kaznivih dejanj povezanih z internetom je vprašanje smiselnosti uporabe tradicionalnih oblik pridobivanja dokazov na eni strani in vprašanje pretirane uporabe sodobne tehnologije pri pridobivanju zanesljivih dokazov, kar pogsto pomeni pridobivanje tudi velike količine zasebnih podatkov.

Dejstvo je, da pripadniki ekstremističnih skupin potrebujejo internet, predvsem za širjenje svojih ciljev in prepričanj, širjenje groženj, novačenje novih članov in iskanje finančne podpore.

Nekateri uporabniki interneta so bili v preteklosti prepričani, da je internet zaradi svojih lastnosti že po svoji naravi odporen proti nadzorovanju države, danes različne zakonodaje čedalje bolj omejujejo prispevke na internetu, po drugi strani pa varnostni organi odkrivajo nove možnosti nadzorovanja uporabnikov interneta.

Ključne besede: internet, ekstremizem, kriminal, preiskovanje, kibernetski prostor, mednarodno sodelovanje.

Extremisms on the internet

In my Master's degree I'm going to present the way the national and foreign authorities, that investigate and prevent criminal actions caused by means of the internet, operate. The purpose of this Master's degree is to describe the methods and tactics of investigating criminal actions of different extremisms, such as terrorism, nationalism, racism, left and right political extremism and, finally, hostile speech, all done by means of the internet. In this Master's degree the sphere of computer crime, the legal order in Slovenia and the legal basis for discovering and preventing extremism on the internet are presented. The computer crime forms are also dealt with since there have appeared more and more different and new forms of criminal actions in Slovenia, which are carried out by extremistic groups and are connected with cybernetic space. The analysis of the problem can be interesting to and can come in useful for the criminal police as well as for legislators.

The difficulty in uncovering criminal actions caused by means of the internet lies in investigators coming upon e-evidences. The investigators must be extremely careful when assembling and protecting these evidences since such evidences can be quickly damaged or destroyed. The internet knows no borders, social differences, it knows no time, language or geographical differences. That is why the international security authorities cooperation is important. It is also important for countries to have a coordinated legislation, which covers extremisms on the internet, and therefore take an effective part in investigations. The question of reasonability of using traditional ways of collecting evidence on one hand and on the other hand the question of excessive use of modern technology when acquiring reliable evidence represent a fundamental challenge when investigating criminal actions connected with the internet, which is often connected with acquiring a large amount of personal data.

The fact is that members of extremistic groups need the internet, mainly for spreading their goals, beliefs and threats, but also for recruiting new members and finding financial support.

In the past, some internet users were sure that the internet was in its nature immune against control. Today different legislations are limiting articles on the internet more and more and security authorities keep finding out new possibilities of controlling the internet users.

Key words: the internet, extremism, crime, investigation, cybernetic space, international cooperation

KAZALO

SEZNAM TABEL

SEZNAM KRATIC

BKA Bundeskriminalamts
Dos Denial of Service
DNS Domain Name System/Service/Server
ETA Euskadi Ta Askatasuma
EU Evropska unija
FBI Federal Bureau of Investigation
FTP File Transfer Protocol
HTTP Hypertext Transfer Protocol
IKT informacijsko-komunikacijska tehnologija
IP Internet Protocol
IRC Internet Relay Chat
IWS Internet World Stats
MIT Massachusetts institute of technology
NCB Nacionalni centralni biro
P2P Peer-to-peer
RSS Really Simple Syndication
SURS Statistični urad Republike Slovenije
TREVI Terrorism, Radicalism, Extremism and Violence – International
TWG Terrorism Working Group
UKP Uprava kriminalistične policije
URL Uniform Resource Locator
VOIP Voice over Internet Protocol
WWW World Wide Web
ZKP Zakon o kazenskem postopku

1 UVOD

1.1 OBRAZLOŽITEV TEME – OPREDELITEV PREDMETA RAZISKOVANJA

S prodiranjem informacijske tehnologije v skoraj vse pore življenja postaja ta infrastruktura vedno pogostejša in priljubljenejša tarča internetnih storilcev kaznivih dejanj in tudi ekstremistov. Internet ponuja takojšnjo svetovno razširjenost, možnost promoviranja njihovih organizacij in rekrutacijo novih somišljenikov.

Ne glede na vero, kulturo, etničnost ali družbeno-ekonomski status, je temelj vsakega ekstremizma dihotomija »mi proti njim« (Tankel 2007, 56, in Zeidan 2007, 68), kar je navsezadnje tudi temeljna značilnost fundamentalizma. Takšno dojemanje stvarnosti je privlačno, ker nudi poenostavljeno sliko kompleksnega sveta. Pogosto se ekstremisti zatečejo v svoj svet, se izolirajo v poizkusu, da bi izoblikovali samo majhen delček svojega idealnega življenjskega prostora. Ker njihove utopije nikoli ne postanejo realnost, se zatečejo k nasilju (Tankel 2007, 56).

Pripadniki ekstremističnih skupin informacijsko tehnologijo za svojo dejavnost uporabljajo predvsem za zlorabo informacijske tehnologije za podporo ali izvajanje teroristične dejavnosti. S pomočjo spletnih strani razširjajo ideološko propagando, novačijo nove pripadnike, pridobivajo finančna sredstva in varno komunicirajo med seboj in med skupinami. Prav tako je internet izjemen pripomoček za pridobivanje podatkov, ki so pomembni za teroristično in ekstremistično delovanje, pri tem pa nudi anonimnost v različnih operacijah (Weiman 2004).

Internet je tudi instrument planiranja in podpore. Poleg funkcije instrumenta komunikacije je tudi pripravljalno orodje za napade tako v resničnem kot tudi digitalnem svetu. Informacije, kot so satelitske slike, ki so bile nedolgo nazaj dosegljive le strokovnjakom, so danes javno dobro. Te slike, ki jih ekstremisti že uporabljajo, je zelo lahko kombinirati z drugimi podatki, kot so seznami ulic v določenih mestih. Tako lahko na primer zelo natančno načrtujejo evakuacijske poti (poti pobega) celo brez dejanske prisotnosti oseb na kraju.

Te informacije se lahko združujejo tudi z drugimi, pogosto brezplačno dostopnimi informacijami na spletnih straneh podjetij, vladnih služb in medijev. Tako so na primer lahko zbrane in uporabljene informacije o varnostnih pomanjkljivostih na bankah, v denarnih ustanovah, na letališčih ali v transportnih podjetjih. Po podatkih priročnikov za teroriste lahko tako preko javnih virov pridobijo najmanj 80 % potrebnih informacij o nasprotniku. Najdbe na računalnikih ekstremistov potrjujejo, da so tovrstne informacije dejansko pridobljene in uporabljene za načrtovanje napadov. Še več, glede na navedbe nekaterih avtorjev, teroristične organizacije baze podatkov uporabljajo za zbiranje, razvrščanje in ocenjevanje podrobnosti potencialnih ciljev v Združenih državah Amerike. Ob takšnem ozadju je razumljivo, da vlade po svetu skrbnikom strani z digitalnimi zemljevidi in satelitskimi slikami svetujejo oziroma predpisujejo, da izvzamejo nekatere – varnostno pomembne – informacije (Brynjar 2007).

Informacijsko-komunikacijska tehnologija (IKT) je sorazmerno poceni in lahko dostopna, hkrati uporabnikom omogoča anonimnost in geografsko in prostorsko neomejenost. Tako kot IKT uporabljajo podjetja in zasebniki, ker jim omogoča učinkovito široko predstavljanje dejavnosti, tako IKT uporabljajo tudi ekstremistične skupine. Ekstremistične skupine računalnike, programsko opremo, telekomunikacijska sredstva in internet uporabljajo za organiziranje delovanja in usklajevanje dejavnosti.

V diplomski nalogi bom opisal načine, kako ekstremistične skupine, tako v svetu kot v Sloveniji, uporabljajo internet za širjenje svojih idej. Po svetu se varnostni organi ukvarjajo predvsem s kaznivimi dejanji, ki jih preko interneta širijo teroristične organizacije. Gre predvsem za spletne strani, na katerih objavljajo članke, s katerimi širijo svoje cilje in namene delovanja. Najaktivnejše so teroristične organizacije, ki širijo islamistične radikalne ideje. V Sloveniji se varnostni organi pri preiskovanju ekstremizma na internetu ukvarjajo predvsem s širjenjem sovražnega govora in idej nekaterih desničarskih skupin. Namen naloge je ugotoviti na kakšen način domači in tuji preiskovalni organi preiskujejo in preprečujejo kazniva dejanja, storjena s pomočjo interneta. Namen preučevanja v magistrskem delu so metode in taktika preiskovanja kaznivih dejanj različnih ekstremizmov, kot so terorizem, nacionalizem, rasizem, levi in desni ekstremizem in ne nazadnje sovražni govor, storjenih s pomočjo interneta.

Z vidika ekstremizma je računalnik sredstvo za izvrševanje kaznivih dejanj, v določenih primerih je lahko celo objekt napada. Na žalost storilci kaznivih dejanj pogosto ostajajo nekaznovani. Temu botrujeta predvsem zaostajanje kazenske zakonodaje za tehnološkim razvojem ter večja ali manjša anonimnost vsakega udeleženca, kar je posledica vedno večjih možnosti uporabe interneta, ki omogoča objavo informacij z možnostjo odgovora vsakega posameznega poslušalca.

Danes poznamo mnogo ekstremizmov, nekateri obstajajo izključno za širjenje različnih radikalnih idej in temeljijo na javnem spodbujanju sovraštva, nasilja ali nestrpnosti in njihovi pripadniki zaradi širjenja tovrstnih idej izvršujejo kazniva dejanja. V magistrski nalogi se bom osredotočil na ekstremizme, s katerimi pripadniki ekstremističnih skupin izvršujejo kazniva dejanja.

2 METODOLOŠKO-HIPOTETIČNI OKVIR MAGISTRSKEGA DELA

Osrednje raziskovalno vprašanje magistrske naloge je raziskati vzroke in oblike razširjenosti ekstremizmov s pomočjo interneta ter ugotoviti, kakšen vpliv ima ta na varnost. Poskušal bom predstaviti razvoj interneta v kriminalne namene in vzroke za pojav radikalnih idej na internetu.

Namen magistrskega dela:

- **Predstaviti možnosti uporabe interneta v kriminalne dejavnosti.** Internet danes prestavlja enega najbolj množičnih medijev. Poleg veliko prednosti, kot je, denimo, hiter prenos informacij, omogoča tudi hitro širjenje radikalnih idej in izvrševanja kaznivih dejanj, s katerimi se pridobiva materialna sredstva.
- **Predstaviti ekstremistične skupine, ki uporabljajo internet za širjenje propagande.** Širitev in dostopnost interneta sta spodbudila tudi nekatere teroristične skupine, ki sicer zavračajo zahodno kulturo, da so presegle svoje poglede in uporabljajo internet, kot širitev svojih idej.
- **Ugotoviti in preučiti vzroke za pojav radikalnih idej na internetu**. Internet je predvsem orodje za informiranje o mnogih kršitvah človekovih pravic po svetu, ravno tako pa se uporablja za širjenje radikalnih idej.
- **Preučiti uporabo interneta na nekaterih področjih kriminalitete in ekstremizma.** Internet je povzročil pravo evolucijo širjenja vsebin, kar je kaznivo dejanje, ali radikalnih idej in načina, kako izvrševati kazniva dejanja.
- **Predstavitev domačih in tujih varnostnih organov, ki preiskujejo tovrstno kriminaliteto, in uporabe njihovih preiskovalnih metod.** Ravno zaradi široke uporabe interneta za kriminalne dejavnosti je bilo tako v Sloveniji kot po svetu ustanovljenih kar nekaj specializiranih služb znotraj varnostnih organov, ki skrbijo za preiskovanje tovrstnih kaznivih dejanj. Varnostni organi se neprestano prilagajajo novim načinom izvrševanja kaznivih dejanj s pomočjo interneta.
- **Opisati razloge, zakaj varnostni organi zelo omejeno posegajo po možnosti cenzuriranja ali zaprtja internetnih strani, ki širijo propagando.** Standardi demokracije in spoštovanja temeljnih človekovih pravic,

kamor sodi tudi pravica po informiranju, varnostnim organom preprečujejo množično zapiranje internetnih strani.

2.1 STRUKTURA MAGISTRSKEGA DELA

Magistrsko delo je razdeljeno na naslednje vsebinske sklope:

- V uvodu magistrskega dela je opredelitev predmeta raziskovanja.
- Opredeljen je metodološko-hipotetični okvir magistrskega dela, kjer so v vsebinsko smiselnih podpoglavjih najprej predstavljeni struktura dela, izhodišča (predpostavke) in omejitve magistrskega dela, sledijo jim cilji in namen dela, glede na cilje so v nadaljevanju določene smiselne trditve oz. hipoteze, ki bodo v delu preverjane, na koncu pa so predstavljene uporabljene metode raziskovanja ter pričakovane ugotovitve.
- S teoretičnega vidika so opredeljeni vsi ključni pojmi, ki so potrebni za razlago podatkov, stališč in mnenj v magistrskem delu. V tem poglavju gre predvsem za podroben izbor obstoječih definicij domačih in tujih avtorjev, ki se ujemajo s predmetom preučevanja.
- Predstavljen je razvoj interneta, predvsem v smislu zlorabe interneta v kriminalne namene.
- Predstavljene so ekstremistične ideje na internetu; na kakšen način različne teroristične, separatistične, rasistične in druge nasilne subkulture uporabljajo internet.
- Prikazana sta struktura in način dela varnostnih organov, tako domačih kot tujih. Pri tem so opisani mednarodni sporazumi med Republiko Slovenijo in drugimi državami in mednarodnimi ustanovami. Opisan je tudi pomen mednarodnega sodelovanja.

Relevantnost magistrskega dela je v predstavitvi načina preiskovanja tako domačih kot tujih varnostnih organov za preiskovanje in preprečevanje kaznivih dejanj ekstremizma s pomočjo interneta. Internet za širjenje idej in propagande uporabljajo različne ekstremistične skupine, denimo, protiglobalistična, separatistična, nacionalistična gibanja ali različne subkulture. Internet se uporablja predvsem kot medij za prenos informacij. Za ekstremistične skupine informacija pomeni moč. Mediji poročajo predvsem o

dramatičnih dogodkih. Dramatični dogodek je priložnost za javno predstavitev svojega obstoja ali pridobitev širše javne podpore.

Relevantnost teoretičnega raziskovanja predlagane teme magistrskega dela se je pokazala tudi v prikazu uporabe interneta v kriminalne in ekstremistične namene. Preučil sem razvoj interneta in njegovo uporabo v kriminalne namene, poskušal najti razloge, zakaj se kljub široki uporabi interneta v kriminalne namene države ne odločajo za množično cenzuro ali zaprtje dostopa do določenih spletnih strani. Za opis uporabe interneta v kriminalne in teroristične namene sem uporabil dostopno literaturo in raziskovanje z udeležbo z uporabo svojega znanja, ki sem ga pridobil z delom v različnih mednarodnih delovnih skupinah za preprečevanje terorizma. Preučil sem preiskovalne metode in taktike varnostnih organov za preprečevanje in zbiranje dokazov o storjenih kaznivih dejanjih na internetu.

Teoretična relevantnost magistrske naloge je v opisu nujnega sodelovanja med državami in njihovimi varnostnimi organi pri preiskovanju internetnega kriminala. Glavni cilj je preučitev zakonskih možnosti preiskovanja tovrstnih kaznivih dejanj in možnosti in načina sodelovanja domačih in tujih varnostnih organov.

Aplikativna relevantnost magistrskega dela je v oblikovanju izhodišč za izvajanje ustreznih ukrepov pri zagotavljanju varnosti pred grožnjami ali kaznivimi dejanji na internetu, kar je mogoče aplicirati tudi na Slovenijo in preiskovanje kaznivih dejanj kriminalistične policije.

Glavna omejitev v nalogi je samo preprečevanje in preiskovanje kaznivih dejanj ekstremizma na internetu. Preiskovanje poteka tako na nacionalni kot na mednarodni ravni. Ker bi bila podrobnejša analiza posameznih nacionalnih zakonodaj in s tem povezanih preiskav zaradi različnih metod in različnih operativnih ukrepov varnostnih organov ter zaradi različnih definicij, kaj je kaznivo, preobsežna, bom preučeval zgolj odzivanje mednarodne skupnosti.

2.2 CILJI IN NAMEN MAGISTRSKEGA DELA

Glavni cilj magistrskega dela je analizirati prepletanje uporabe interneta in izvrševanje kaznivih dejanj, povezanih z ekstremizmom. Magistrska naloga sledi naslednjim vsebinskim ciljem:

- predstavitev teoretičnega okvirja za razumevanje pojava kibernetskega ekstremizma,
- predstavitev definicij izrazov, uporabljenih v magistrskem delu, opredelitev temeljnih pojmov, kot so terorizem, separatizem, rasizem, subkulture, nacionalizem, varnost, in opis značilnosti in razvoja internetnega terorizma,
- opis razsežnosti kibernetskega prostora, načina njegove uporabe za izvajanje računalniške kriminalitete,
- prikaz načina uporabe interneta v kriminalne namene,
- pregled uporabe različnih orodij za izvrševanje kaznivih dejanj preko interneta,
- pregled razvoja interneta in razvoja izvrševanja kaznivih dejanj s pomočjo interneta,
- preučitev vzrokov za uporabo interneta za izvrševanje kaznivih dejanj,
- preučitev vzrokov za uporabo interneta v ekstremistične namene,
- preučitev razširitve uporabe interneta za izvrševanje kaznivih dejanj,
- predstavitev zakonskih možnosti preprečevanja kaznivih dejanj prek interneta.
- predstavitev dela varnostnih organov v tujini in Republiki Sloveniji, ki se ukvarjajo s preprečevanjem internetnega kriminala.

2.3 TRDITVE (TEZE, HIPOTEZE)

V magistrskem delu postavljam naslednje hipoteze:

Hipoteza 1 **Internet vpliva na razvoj ekstremističnih idej pri posameznikih, ki s pomočjo interneta iščejo somišljenike. Ekstremistične skupine internet uporabljajo predvsem za predstavitev svojih ciljev, financiranje in pridobivanje novega članstva, in ne za napade na internetno infrastrukturo.**

Hipoteza 2 **Slovenska zakonodaja zagotavlja pogoje, ki omogočajo preiskovanje kaznivih dejanj, storjenih s pomočjo interneta. Pretekle izkušnje so pripomogle k nadgradnji izvajanja preiskav, preiskovalci so pridobili nova tehnična znanja in začeli uporabljati nova tehnična sredstva. Slovenska zakonodaja se ustrezno prilagaja novim trendom izvrševanja kaznivih dejanj preko interneta.**

2.4 UPORABLJENA METODOLOGIJA – RAZISKOVALNE METODE IN TEHNIKE

Prva metoda bo zbiranje informacij, virov in relevantne literature za oblikovanje postavljenih hipotez pri preučevanju internetnega terorizma. Za pregled izbrane tematike bom uporabil tako primarne vire (dokumenti, poročila, zapisniki) kot sekundarne (dostopne v akademskem okolju, in sicer monografske publikacije, znanstvene in strokovne članke)[1].

Magistrsko delo se opira na dostopno tujo in domačo literaturo ter vse dostopne vire, ki teoretično in praktično obravnavajo omenjeno tematiko. Pri preučevanju in izdelavi magistrskega dela bo uporabljenih več vrst virov in različne raziskovalne metode.

Za predstavitev tematike in verifikacijo trditev sem uporabil dva temeljna pristopa: teoretičnega in empiričnega. S pomočjo prvega sem podrobneje opredelil teoretične in

[1] Članki pomembnejših teoretikov, tako domačih kot tujih, ki se ukvarjajo s problematiko ekstremizma.

metodološke vidike preučevanja. V empiričnem delu (študija primera) pa sem predstavil, kako se preiskovalni organi lotevajo posameznih primerov.

Trditve sem preverjal s kombinacijo naslednjih kvalitativnih in kvantitativnih metod in tehnik:

1. s pomočjo analize primarnih, sekundarnih in terciarnih virov:
    - pri sekundarnih virih se bom opiral na pisne vire – ustrezna strokovna literatura, časopisni članki, obstoječe statistike, analize policy, prispevki iz konferenc ipd. Kot primarne vire bom uporabil različne kodekse, deklaracije, sporazume in pogodbe. Izkoristil bom tudi terciarne vire, pri čemer mi bo v pomoč predvsem internet;
    - z metodo analize in sinteze: uporabil bom kvalitativno analizo besedila, v študijah primerov bom delno uporabil tudi kvantitativno metodo raziskovanja. V empiričnem delu naloge bom zajel objave z elementi ekstremizma, objavljene na internetu, ki so bile objavljene na različnih spletnih straneh. Pri tem se bom opiral na predpostavko, da ekstremisti internet potrebujejo in uporabljajo za dosego svojih ciljev;
    - metodo deskripcije oz. deskriptivno metodo (za opisovanje dejstev, procesov oziroma za opis delovanja obravnavanega področja);
2. s pomočjo strukturiranega intervjuja, opravljenega s strokovnjaki za preiskovanje kaznivih dejanj, povezanih z internetom;
3. s pregledom rešenih primerov izvajanja internetnega kriminala po svetu.

Pri pisanju magistrske naloge, predvsem pri pregledu podatkov ter študijah primerov, mi bodo pomagale tudi večletne izkušnje pri preiskovanju kaznivih dejanj s pomočjo interneta v Upravi kriminalistične policije ter sodelovanje v domačih in tujih delovnih skupinah na to temo.

Z uporabljeno metodologijo magistrsko delo poskuša zavreči ali potrditi postavljene trditve.

3 OPREDELITEV TEMELJNIH POJMOV

3.1 INTERNET

Internet je računalniško podprto komunikacijsko omrežje, sestavljeno iz neskončnega števila povezanih računalnikov, ki med seboj komunicirajo in si izmenjujejo podatke. Internet ni le svetovno omrežje, preko katerega s celega sveta pridobivamo kakršnekoli podatke ali informacije, temveč je tudi tako imenovana virtualna skupnost, ki odkriva nove razsežnosti te družbe.

3.1.1 ZGODOVINA INTERNETA

Za rojstni dan interneta velja 29. oktober 1969, ko so ob 21.00 s kalifornijske univerze (UCLA) na stanfordsko univerzo poslali prve podatke prek računalniške mreže, tedaj imenovane ARPANET[2]. Uspelo jim je povezati dva fizično ločena računalnika. Leta 1983 na ARPANET uvedejo protokol TCP/IP, kar je dejansko prvi internet. Leta 1986 so se prva v internet povezala prva komercialna omrežja in leta 1992 je internet začel prodirati praktično v vse stroke (Laudon 2006).

V Sloveniji se je internet začel hitreje razvijati v 90. letih. V Sloveniji narašča delež gospodinjstev z dostopom do interneta in delež gospodinjstev s širokopasovno internetno povezavo. V prvem četrtletju leta 2004 je imelo dostop do interneta 47 % gospodinjstev, v prvem četrtletju 2010 pa je bilo takih gospodinjstev že 68 %. Vedno več gospodinjstev v Sloveniji dostopa do interneta prek širokopasovne povezave, v prvem četrtletju 2010 je bilo takih gospodinjstev 62 %, v enakem obdobju leta 2004 pa 10 %. Slovenija je na ravni Evropske Unije po opremljenosti gospodinjstev z IKT med srednje razvitimi državami. V EU-27 je imelo v prvem četrtletju 2009 dostop do interneta nekoliko več gospodinjstev kot v Sloveniji (65 %), širokopasovno internetno povezavo pa je, tako kot v Sloveniji, uporabljalo 56 % gospodinjstev (SURS[3]).

---

[2] Ime ARPANET (Advanced Research Projects Agency) sicer izhaja iz kratice za agencijo ameriškega obrambnega ministrstva za napredne raziskave (Advanced Research Projects Agency - ARPA), celoten sistem pa je postavil znanstvenik iz »Massachusetts Institute Technology« Lincoln laboratorija Larry Roberts, ki je poskus pred 40 leti opazoval v pisarni v Washingtonu. Zdaj, štiri desetletja kasneje, je za BBC razložil, da ideja o ARPANETU pri obrambnem ministrstvu nikakor ni bila dobro sprejeta: *"Prepričani so bili, da je ideja grozna."*

[3] Statistični urad Republike Slovenije je vladna ustanova, ki izvaja dela na področju državne statistike, usklajuje statistični sistem, določa metodološke standarde ter zbira in izkazuje podatke

Narašča tudi delež rednih uporabnikov interneta – tj. oseb, ki so internet uporabljale v zadnjih treh mesecih: v prvem četrtletju 2004 je bilo v Sloveniji v starosti od 16 do 74 let 37 % rednih uporabnikov interneta, v prvem četrtletju 2010 pa 72 %. Podobna je tudi slika o številu rednih uporabnikov računalnika: v prvem četrtletju 2004 je bilo med osebami v starosti od 16 do 74 let 48 % rednih uporabnikov računalnika (osebe, ki so računalnik uporabljale v zadnjih treh mesecih), do prvega četrtletja 2010 pa se je ta delež povečal na 72 % (SURS).

Spletna stran Internet World Stats (IWS[4]) redno objavlja število internetnih uporabnikov na svetu. Glede na podatke z dne 4. 9. 2010 je bilo takrat na svetu približno 1.966.514.816 uporabnikov interneta, kar je več kot četrtina vse svetovne populacije.

3.1.2 STORITVE, KI JIH OMOGOČA INTERNET

Internet nudi vrsto storitev. Vzpostavitev WEB 2.0 je omogočila, da spletni projekti predstavljajo ne le statično informacijo, temveč življenjski slog. WEB 2.0 je naslednja generacija spleta. Nudi nam spletna orodja, ki uporabnikom omogočajo, da komunicirajo, sodelujejo in si izmenjujejo informacije na način, kot ga prej nismo poznali. Do zdaj je vse temeljilo še na povezovanju informacij, WEB 2.0 pa povezuje ljudi. Orodja postajajo bolj fleksibilna, uporabnost pa raste z domišljijo razvijalcev in uporabnikov (Križanič 2010).

WEB 2.0 je splet, namenjen socializaciji, in uporablja nove spletne aplikacije, kot so blogi, podcasti, video sharingi, RSS, Ajax, Wiki, peer-to-peer, tagging, feeds in še polno zapletenih pojmov, ki pomenijo več interaktivnosti, dinamičnih vsebin in prilagodljivosti. WEB 2.0 olajša odkrivanje novega znanja in poseganje po relevantnih informacijah. Med tem ko WEB 2.0 še vedno zori, z njegovo pomočjo vezi med ljudmi postajajo tesnejše, poslovneži lahko pridobivajo novo znanje in se zaradi tega bolje odločajo, realno-

oziroma je glavni izvajalec in povezovalec dela na področju državne statistike. Na svoji spletni strani www.stat.si vse te podatke tudi redno objavlja.

[4] Spletna stran Internet World Stats (IWS) je mednarodna spletna stran na naslovu www.internetworldstats.com, ki ažurno zbira podatke o uporabi interneta na svetu in podatke o statistikah svetovne populacije ter izvaja marketinške raziskave na internetu za več kot 223 držav in svetovnih regij.

časovno sodelovanje pa postaja enostavnejše kot kdajkoli prej. WEB 2.0 omogoča, da postanejo uporabniki aktivni člen vsake spletne strani, s tem pa se gradi zavest pripadnosti, kar je koristno za vsako podjetje s pozitivnimi referencami (Križanič 2010). Uporabniki so čedalje bolj informirani, bolj povezani, bolj komunikativni in imajo več stvari pod nadzorom kot kdajkoli prej. Analitiki podjetja Jupiter Research so spoznali ključne učinke tehnologije na družbo (Ryan in Jones 2009, 14–17):

- *Interpovezanost*: Mrežna digitalna tehnologija uporabnikom omogoča hitrejše povezovanje med seboj. Prek e-pošte, instantnega sporočanja (angleško IM), mobilnega sporočanja, spletnih socialnih omrežij, kot so Facebook, MySpace, Linkedln, ali še globlje, s kombinacijo vsega omenjenega, se gradi agregat podobno mislečih ljudi z vseh koncev sveta, osvobojenih časovne in prostorske razsežnosti.
- *Tehnologija viša informiranost*: Z uporabo digitalne tehnologije so lahko informacije oblikovane, objavljene, dostopne in uporabljene hitro in enostavno. Novice, mnenja in informacije so globlje kot kdajkoli prej. Znanje pomeni moč in digitalna tehnologija prenaša moč na uporabnika.
- *Filtriranje informacij narašča*: Ker jim tehnologija to omogoča, uporabniki začenjajo filtrirati informacije, ki se jim zdijo pomembne, in ignorirajo tiste, ki se jim ne zdijo. Radi imajo kategorizirane in podane informacije, naj bo to prek e-pošte ali RSS-jev. Uporabniki se lahko izognejo katerikoli neželeni komunikaciji.
- *Združevanje niš se veča*: Obilica in raznovrstnost vsebin na internetu uporabnikom omogočata sodelovanje in oblikovanje lastnih interesov ali hobijev na osnovi različnih identitet, ki jih povzemajo. Združevanje podobno mislečih posameznikov se zdaj zgodi zgolj na liniji, kar pomeni, da se homogene skupine masovnih potrošnikov delijo v manjše nišne interesne skupine.
- *Mikro objavljanje zasebne vsebine*: Interaktivna in povezana narava digitalnih medijev dopušča, da se uporabniki izražajo na spletu. To se dogaja na mnenjskih forumih, blogih, foto galerijah, glasovalnih forumih ipd. Uporabniki na primer objavljajo svoje mnenje ali vprašanja ipd.
- *Kjerkoli, kadarkoli, na zahtevo*: Z vseprisotnostjo digitalne tehnologije postajajo uporabnikove zahteve čedalje hitreje zadovoljene. V digitalni ekonomiji postajajo

čas, prostor, lokacija in fizično navzoče trgovine manj pomembne. Živimo v svetu, ki zahteva takojšnje zadovoljstvo in tehnologija to omogoča.

3.1.3 SOCIALNA OMREŽJA

Spletna socialna omrežja predstavljajo širok pojem, ki v najširšem pomenu obsegajo vsako spletno stran, na kateri imajo uporabniki možnost komuniciranja z drugimi uporabniki in pridobivanja novih stikov. Tako med tovrstne spletne aplikacije uvrščamo najrazličnejše spletne storitve, od blogov pa vse do portalov za objavljanje slik. Najpogosteje pa s pojmom spletna socialna omrežja označujemo spletne storitve, pri katerih je poudarek predvsem na pridobivanju oziroma širjenju socialnega kapitala v zasebnem ali poslovnem življenju (Huber 2007).

Spletna socialna omrežja z različnimi tehnološkimi orodji nudijo široko področje interesov in praks. Večina izmed tovrstnih spletnih strani podpira vzdrževanje že prej obstoječih socialnih omrežij, medtem ko ostale pomagajo popolnim neznancem, da se povežejo med seboj na podlagi skupnih interesov, političnih vidikov ali dejavnosti. Nekatera spletna omrežja svoje uporabnike združujejo, na primer s pripadanjem le določeni skupini ali prepričanju, kot tistemu boljšemu oziroma slabšemu, druga pa jih privlačijo na podlagi skupnega jezika ali skupne rasne, spolne, verske in nacionalne pripadnosti. Socialna spletna omrežja se tudi razlikujejo glede na vsebnost novih informacijskih in komunikacijskih orodij, kot so bloganje in objavljanje ter pošiljanje slik in zvočnih zapisov (Boyd in Ellison 2007).

Spletna socialna omrežja so sestavljena iz seznama profilov, ki se oblikujejo v seznamu prijateljev. Javni prikaz stikov ali prijateljev je ključna sestavina internetnih socialnih omrežij, saj s tem omogoča povezavo do ostalih prijateljev. Seznam pa tudi omogoča, da vsak uporabnik s klikom na različne sezname prijateljev brska po omrežju, saj je v večini primerov seznam spletnih prijateljev oziroma stikov dostopen vsakomur, ki ima dostop do profila posameznega uporabnika (Boyd in Ellison 2007).

3.2 KIBERNETSKI PROSTOR

Izraz kibernetski prostor (Cyberspace) je skoval pisatelj znanstvene fantastike William Gibson. V svojih delih ga je uporabil za oznako sveta v virtualni resničnosti, kjer poteka interakcija človeških misli[5] (Ulčar 2002).

Kibernetski prostor ni prostor v klasičnem pomenu besede, saj nima ne dimenzij ne drugih fizičnih značilnosti prostora. V pravu je kibernetski prostor konstrukt, ki so ga postavili ameriški pravni teoretiki in ki omogoča lažje reševanje pravnih problemov, povezanih z izmenjavo informacij prek interneta. S pojmovno ločitvijo kibernetskega prostora (torej prostora, kjer potekajo interakcije med uporabniki interneta) in interneta (komunikacijskega omrežja, sestavljenega iz računalnikov in kablov) se lažje spopademo tudi s to problematiko (Ulčar 2002).

Toplišek (1998) kibernetski prostor poimenuje elektronski (navidezni) prostor in navaja, da gre za splošni pojem za povezana računalniška omrežja, računalnike in za množico njihovih stalnih in naključnih uporabnikov. Elektronski prostor je možen zaradi poenotenja ključnih tehnoloških rešitev, hitro pa se porajajo tudi uporabniška in druga pravila ravnanja, ki elektronskemu prostoru postopoma dajejo obrise tehnološko, pravno in sploh civilizacijsko opredeljenega prostora.

Za pravno pojmovanje je bistvena razlika med realnim in kibernetskim prostorom v odsotnosti meja v kibernetskem prostoru. Globalna oziroma brezmejna narava kibernetskega prostora povzroča teritorialnim konceptom mednarodne pristojnosti velike težave. Problemi pri določanju sodne pristojnosti namreč nastanejo, ko je treba nek sporni dogodek, ki se je zgodil povsod in nikjer hkrati, v teritorialno neomejenem kibernetskem prostoru, povezati z določenim na načelu teritorialnosti temelječim pravnim redom in tako rešiti pravni primer (npr. kibernetski spor). Povedano drugače, ali se zaradi nekrajevne oziroma vsekrajevne narave kibernetskega prostora oseba, ki opravlja določeno dejavnost (najpogosteje gre za vzpostavitev spletne strani z

[5] V romanu Nevromat (1994) ga opiše takole: "Kiberprostor. Skupna halucinacija, ki jo vsak dan doživijo milijarde povsem legitimnih operaterjev, povsod po svetu, celo otroci, ki se učijo matematičnih pojmov ... Grafična predstavitev vseh podatkov, abstrahiranih iz bank vseh računalnikov človeškega sistema. Nepredstavljiva kompleksnost. Svetlobni žarki, razporejeni v neprostoru uma, gruče in ozvezdja podatkov."

neomejenim dostopom, na kateri se nahajajo določene informacije), zaradi tega izpostavi sodni pristojnosti vseh držav, v katerih je mogoč dostop do spletne strani (Ulčar 2002)?

Definiranja oz. opredeljevanja kibernetskega prostora se v različnih sodobnih znanstvenih prispevkih med seboj razlikujejo. Tako, na primer, Michael Heim kibernetski prostor opredeli kot:

> *»elektronsko omrežje, v katerem se nahaja virtualna resničnost. Virtualna resničnost je pa samo eden od fenomenov v tem elektronskem prostoru. V okviru vsakdanjega sveta je kiberprostor skupek orientacijskih točk, s pomočjo katerih lažje iščemo znotraj podatkovne baze«.* (Heim 1993 v Šajatovič, 9). Zanj je kibernetski prostor tudi prostor, telefonskih pogovorov, virtualnnega denarja in elektronske pošte. (Šajatovič 1998)

Zelo pogosta so pojmovanja kibernetskega prostora kot interaktivnega dela širšega okolja virtualne resničnosti. Takšno opredeljevanje je značilno za Sherry Turkle – po njenem vključitev v kibernetski prostor posamezniku omogoča doživljanje rutin vsakdanjega življenja, in sicer na več načinov: z branjem elektronske pošte, pošiljanjem sporočil ali rezerviranjem letalske karte prek računalniške mreže. V kibernetskem prostoru se posamezniki lahko pogovarjajo, si izmenjujejo ideje, ustvarijo osebnost in gradijo nove skupnosti. (Slevin 2000)

Številne razprave v okvirju kibernetskega prostora se ukvarjajo s problemi javnega delovanja udeležencev v tem prostoru. Kibernetski prostor tako pojmujejo kot novo obliko javnega prostora, javne sfere, kjer bi posamezniki ali skupine lahko svobodno izražali svoja mnenja ali kako drugače javno-politično (so)delovali. Gre za primerjave kibernetskega prostora z nekdanjimi angleškimi kavarnami in pariškimi saloni (Dalhgren 1991 in Oblak 1999). Za Jana Fernbacha je tako kibernetski prostor »v svojem bistvu ponovno vzpostavljena javna sfera, namenjena družbeni, politični, ekonomski in kulturni integraciji« (Fernback v Oblak 1999, 40).

Zaradi "nekrajevne" narave interneta je eno najzahtevnejših vprašanj, kako neko sporno elektronsko dejavnost povezati z območjem določenega sodišča (pri tem gre lahko tudi za znotrajdržavno sodno razmejitev). Problem ilustrira povsem mogoč primer z interneta: Katero pravo oziroma sodišče uporabiti, če nemški državljan v Mehiki napiše žaljivo sporočilo, ki se nanaša na norveškega državljana, sporočilo pa je bilo poslano s strežnika v ZDA in ga je prebral nekdo na Češkem (Toplišek 1998)?

3.3 VARNOST

Grizold pojem varnosti povezuje z eksistencialnimi vprašanji posameznika (kakovost življenja po smrti) ter višjimi ravnmi družbenega organiziranja (družba/država, meddržavna skupnost in svet kot celota). Pravi, da je varnost »strukturna prvina obstoja delovanja posameznika, družbe/države in mednarodne skupnosti oziroma sveta kot celote, ki zajema tako stanje uravnoteženega fizičnega, duhovnega in duševnega ter gmotnega obstoja omenjenih entitet kot tudi njihovo občutenje ter zavestno prizadevanje po nenehni vzpostavitvi tega stanja (Grizold 1998, 2).

Baylis pravi, da se večina avtorjev strinja, da je koncept varnosti sporen, a ne toliko v njenem bistvu, odsotnosti nevarnosti za osrednje družbene vrednote (za posameznike in skupine), kot v tem, ali bi moralo biti osrednje težišče raziskovanja varnosti individualna, nacionalna in mednarodna varnost (Baylis 2008, 27).

Buzan je opredelil zanimiv paradoks; kolikor se moč države povečuje, toliko bolj postaja ta država vir groženj za posameznika. V bistvu gre za problem, kako uravnotežiti svobodno delovanje posameznika pri zagotavljanju varnosti na individualni ravni ter sistemsko zagotavljanje varnosti na ravni celotne družbene skupnosti. Že klasična politična misel je namreč utemeljila spoznanje, da je posameznik v razmerju do drugih posameznikov v anarhičnem odnosu in da je povečanje njegove svobode mogoče le na račun njegove varnosti. Tri temeljne entitete (posameznik, država/družba in mednarodna skupnost) si prizadevajo vzpostaviti stanje varnosti, a med njimi ni nujne harmonije (Buzan 1991, 37).

Buzan (v Anžič 1997) je opredelil, da je varnost, razvojno gledano, vgrajena kot biološki mehanizem, kot težnja organizma po obstoju, kot prilagajanje organizma na ogrožajoče vplive okolja. Biološko je torej varnost pogoj za delovanje osnovnih življenjskih funkcij in tako vzgib za razvoj, zavestno dejanje, da bi se stanje varnosti ponovno vzpostavilo.

Vzpostavitev stanja varnosti je po Anžiču zavestno prizadevanje ter civilizacijska in kulturna kategorija, ki zajema vse vidike varnosti, tj. gospodarsko, socialno, kulturno, politično, pravno, ekološko, obrambno itd., torej tiste pojavne oblike družbenega življenja, ki se štejejo za družbene vrednote. Varnost je imanentna strukturna prvina družbe, ki zajema tako stanje oziroma določeno lastnost stanja kot tudi dejavnost oziroma sistem. Varnost se torej nanaša tako na družbo, državo kakor tudi na mednarodno skupnost. Varnost je torej družbena in politična vrednota, ki označuje okvir socialne in politične skupnosti (Anžič 1997).

Varnost hkrati omogoča obstoj družbene reprodukcije, notranji red in mir, razvoj notranje ureditve ter zagotovitev običajnih procesov diferenciacije in integracije znotraj družbe in države, kjer se odvijajo procesi graditve materialnih in duhovnih vrednot in dobrin ter procesi destrukcije in deviantnosti. Za vzpostavitev ravnovesja teh dveh procesov pa mora država vzpostaviti stanje, v katerem bo preko svojih organov vsem državljanom zagotovila minimalni standard (Anžič 1997).

Vsekakor je na vseh ravneh družbene organiziranosti po terorističnih napadih 11. septembra 2001 varnost dobila nove dimenzije, postala je visoko cenjena vrednota, ki se je danes zaveda sleherni državljan, družba in navsezadnje država s svojim aparatom, saj je posamezniku dolžna nuditi določeno raven varnosti, posameznik pa je zanjo tudi pripravljen tvegati oz. omejiti določeno raven osebne svobode. Kljub temu da se je posameznik pripravljen odreči določenim pravicam, mu država še ni priskrbela večje varnosti.

Ogrožanje varnosti v širšem pomenu vključuje številne oblike vojaških in nevojaških pojavov, ki zmanjšujejo varnost posameznikov, družbenih skupin, družbe v celoti, držav in mednarodne skupnosti. Med pojave štejemo kriminal, terorizem, gospodarske grožnje,

ekološke grožnje, naravne nesreče, informacijske grožnje itd. Sodobne grožnje varnosti se lahko izredno hitro ali pa zelo počasi prenašajo iz ene države v drugo (Prezelj 2003).

Varnost je torej vrednota tako države kot tudi družbe, če pa so te vrednote ogrožene, kršene ali kako drugače diskreditirane, prihaja do pojavnih oblik, ki jih imenujemo varnostni pojavi. Znotraj države je varnost opredeljena kot organizacija, ki zajema vse institucije in pooblastila, ki jih imajo njeni predstavniki, je funkcija sistema v odnosu do družbe in države in je tudi določeno posebno stanje.

3.4 EKSTREMIZEM

Nekateri avtorji nasprotujejo temu, da bi bil ekstremizem nujno tudi nasilen. Ye'or (1996) tako, denimo, trdi, da revivalistična gibanja različnih vrst vsebujejo nasilne elemente, pri čemer je militantnost drugačen fenomen od terorizma, saj prvi opisuje psihološko agresivno stanje ali bojevniški karakter. Ekstremizem označuje prepričanja, ki so iracionalna, neopravičljiva ter nesprejemljiva s strani katerekoli družbe. Člane ekstremističnih skupin druži predvsem občutek pripadnosti, povezanosti in članstva. Občutek pripadnosti je bistvenega pomena za pridružitev, privlačen razlog za vztrajanje v skupini ter močan motiv za delovanje. Želja pripadati je skupaj z nedokončano ali pomanjkljivo osebno identiteto pogost vzrok, ki posameznika privede do tega, da se pridruži ekstremistični organizaciji (Baumeister v Borun, 2004, 26).

Internet je pospešil proces širjenja ekstremističnih idej. Omogoča takojšen, anonimen in kakovosten stik med različnimi in drugače nepovezanimi posamezniki. Poznamo mnogo vrst ekstremizmov, ki gojijo radikalna prepričanja, vendar poznamo tudi taka, ki ne uporabljajo nasilja za uresničevanje lastnih ciljev. V magistrskem delu bom opisal metode in taktike preiskovanj kaznivih dejanj ekstremizmov, storjenih s pomočjo interneta, ki se najpogosteje pojavljajo v Evropi. Gre za terorizem, nacionalizem, rasizem, levi in desni ekstremizem in ne nazadnje sovražni govor, storjene s pomočjo interneta.

Terorizem: Danes je v splošni svetovni javnosti – predvsem po zaslugi javnih občil – terorizem kot oblika kriminalitete razvpit, četudi nejasno definiran pojem. Že dejstvo, da obstaja veliko različnih definicij, kaže na zapletenost pojava. Veliko definicij terorizma

obstaja predvsem zaradi težav pri samem definiranju, deloma pa tudi zaradi nesoglasij o tem, v katerih primerih bi bil terorizem lahko upravičen. V zadnjih letih se množijo argumenti za enotno definicijo, čeprav nekateri strokovnjaki poudarjajo, da gre v celoti za politični pojem in enotna definicija s pravnega stališča ni potrebna. Razlogov, zakaj državam ne uspe sprejeti enotne definicije terorizma, je več. Njena odsotnost je za vlade pogosto prednost, ker jim omogoča oblikovanje svojih definicij glede na lastne politične in ideološke preference. Države v definiciji poudarijo težnje, ki zaznamujejo njihovo zunanjo in notranjo politiko, neredko tako obračunajo s političnimi nasprotniki ali uveljavljajo državne ekonomske interese. Politično občutljivost definicije terorizma dodatno ponazarja dejstvo, da enotna definicija včasih ne obstaja niti znotraj ene države. Tak primer so ZDA, kjer obrambno ministrstvo, FBI in zunanje ministrstvo uporabljajo vsak svojo definicijo (Hohler 2005, 6). Galtung (2002, 41) meni, da za terorizem na splošno velja, da gre za orožje slabotnih proti močni državi. Lahko pa v obratnem smislu navedemo, da gre v primeru uporabe orožja močne države proti slabotnim za državni terorizem.

Nacionalizem: Nacionalizem lahko opredelimo kot zavest o identiteti, pripadnost narodu. Je zavedanje različnosti in zavedanju o ločeni pripadnosti. Moč nacionalizma se meri v njegovi preprostosti sporočanja, ki je čustveno. Ker nacionalizem ni intelektualno zahtevna doktrina, ga je mogoče preprosto propagirati, v tem je tudi skrivnost njegovega uspeha. Vsak človek čuti spontano predanost pokrajinam in ljudem, s katerimi je povezan od otroštva (Lassen 2008, 13). Nacionalizem je politična sila, ki je v zadnjih nekaj desetletjih mnogo bolj vplivala na evropsko in svetovno zgodovino, kot pa ideje svobode in parlamentarne demokracije. Korenine sodobnega nacionalizma je mogoče najti v poznem 18. stoletju v zahodni Evropi in Severni Ameriki, od koder se je razširil po vsej Evropi in kasneje po celem svetu. V 20. stoletju je nacionalizem doživljal uspehe, ki bi jih težko našli v zgodovini – njegovo naraščajočo vlogo ponazarja nagel pohod nacionalizma po Evropi neposredno pred prvo svetovno vojno in po njej, še posebej pa po drugi svetovni vojni po Aziji in Afriki (Alter 1991, 221). Porast nacionalizma v Evropi je povzročil tudi padec komunističnih režimov.

Rasizem: Tradicionalni rasizem temelji na predpostavki o večvrednosti določenih ras, v zadnjem času lahko govorimo tudi o rasizmu nad drugačnimi kulturami. Tradicionalni rasizem je omogočal suženjstvo, rasno razlikovanje apartheid, sistematične diskriminacije in izrecno poniževanje na podlagi barve kože ali kakšne druge očitne razlike. Rasizem omogoča, da se rasisti skrijejo pod načelno tolerantnostjo in prijaznostjo do določenih skupin, vendar le do te mere, do katere se ne začutijo ogrožene, sicer pa postanejo sovražni. Zmotno je prepričanje, da populistične rasistične predsodke izražajo samo ekstremisti, kot so neonacisti, ampak tudi bolj konvencionalne, sredinske stranke in politiki ter mnogi mediji. Tu prihaja do nasprotij v samem jedru liberalnih demokracij, v katerih politiki in medijski uredniki, ki sicer ostro nasprotujejo določenim oblikam rasizma, kot na primer skrajno desničarskim in neonacističnim gibanjem, hkrati še poudarjajo druge oblike predsodkov. Ta oblika »benignega« rasizma je še bolj škodljiva, saj viri nosijo visoko stopnjo legitimnosti (Macmaster 2004, 3–4).

Levi ekstremizem zagovarja teorijo nasilja, strahu, atentatov, ugrabitev, nasilnih demonstracij. Posebna značilnost delovanja levih ekstremističnih sil je njihov poudarjen odnos do politik zahodnih vlad. Levičarski ekstremizem je usmerjen v prihodnost, v preoblikovanje ali uničenje obstoječega sistema ter v oblikovanje nove in pravične družbe. Levi ekstremisti so prepričani, da sta reforma sistema ali pa revolucija potrebni za oblikovanje pravične družbe (Martin 2003, 23).

Desni ekstremizem lahko najbolj splošno opišemo kot zavračanje pravice do obstoja alternativnih idej, hkrati pa poudarjajo, da so njihove ideje edino pravilne. Družbene vrednote razumevajo skozi prizmo »mi–oni«. »Oni« so razumljeni ne samo kot drugačni od »nas«, ampak tudi slabši, kot tisti del družbe, ki družbo ogroža in uničuje. »Oni« so torej tako imenovani sovražniki družbe, ki jih je treba onemogočiti. Na drugi strani so »mi« kot rešitelji družbe pred njenim propadom, kot t. i. borci proti sovražnikom družbe. Nestrpnost, sovraštvo in nasilje »nas« do »onih« se legitimira ravno s predstavitvijo »nas« kot žrtev in »njih« kot tistih, ki napadajo »nas«. Temeljni vidiki desnega ekstremizma so populizem ali pretirana vdanost, zvestoba posameznika skupini, teorija zarote ali tajni načrt t. i. sovražnika družbe (Ramet 1999).

Sovražni govor obstaja že od nekdaj, le da se mu v zadnjih nekaj letih posveča veliko več pozornosti, javnih obravnav in razprav v širšem družbenem kontekstu. Z naglim razvojem množičnih medijev se je sovražni govor razširil na vsa področja človekovega življenja, saj lahko nestrpne in diskriminatorne izjave zasledimo v vsakodnevnem časopisju, na televiziji, internetu, radiu in tudi v vsakdanjem sporočanju, kjer sami kreiramo sovražne izjave ali smo pri tem le pasivni udeleženci. Problem sovražnega govora postaja tudi problem spleta, kjer se pod krinko anonimnosti pojavlja vedno več možnosti za neodgovorno razširjanje sovražnosti in nestrpnosti. Število internetnih uporabnikov iz dneva v dan narašča, internet se popularizira in postaja platforma za konfrontacijo različnih mnenj. Da bi celostno razumeli sovražni govor, se moramo najprej zavedati, da je eno najmočnejših sredstev diskriminacije, še posebno, ker ga težko definiramo in še težje preiskujemo in kaznujemo. Zato je razumevanje in umeščanje sovražnega govora kot sovražnega dejanja izjemno zahtevno, saj gre za dokaj neraziskano področje in je redko predmet znanstvenega interesa. Sovražni govor je najtesneje povezan ravno z diskriminatornim diskurzom ter izražanjem mnenj in idej, ki so po svoji naravi ksenofobične in rasistične ter naperjene predvsem proti raznim manjšinam – etničnim, narodnim, verskim, kulturnim ali marginalnim skupinam (Kovačič 2001, 178).

4 KAZNIVA DEJANJA IN KIBERNETSKI PROSTOR

Oblike računalniškega kriminala so znane, podajo se lahko tudi natančni opisi. Težje je zanesljivo in natančno oceniti število primerov in dejanske škode oziroma izgube, ki pri tem nastanejo. Vzroka za veliko temno polje računalniškega kriminala sta predvsem, da dejanje ostane neznano oziroma ga žrtev niti ne zazna ali je dejanje znano oziroma opaženo, vendar ostane neprijavljeno organom pregona. Predvsem imamo tu v mislih podjetja in druge organizacije, ki primere neradi prijavljajo. Bojijo se namreč, da bi to negativno vplivalo na njihove poslovne partnerje, investitorje in na njihove stranke, torej na splošno na ugled podjetja. Veliko primerov pa tudi verjetno ostane zaznanih le s strani skrbnikov oziroma upraviteljev sistemov v podjetjih, ki zaradi svojega ugleda ali podobnih razlogov podatkov o primeru ne posredujejo vodstvu, temveč poskušajo stvar urediti sami (npr. odprava pomanjkljivosti v sistemu zaščite, nameščanje popravkov požarnih zidov in krpanje varnostnih lukenj informacijskega sistema ipd). Gre predvsem za manjše primere, kjer ni kakšnih posebnih finančnih ali dolgoročnih posledic (uničenje poslovnih podatkov, množičen vnos virusov), temveč je bil cilj napadalcev le vdreti v varovan informacijski sistem (Kastelic 2005, 33).

Tabela 4.1: Kazniva dejanja računalniške kriminalitete, storjena v Sloveniji v letih 2009 in 2010.

Vrsta kaznivega dejanja	**Število kaznivih dejanj**				**Število ovadenih osumljencev**			
	2007	**2008**	**2009**	**2010**	**2007**	**2008**	**2009**	**2010**
Vdor v poslovno-informacijski sistem	4	7	11	18	4	5	6	4
Kršitev materialnih avtorskih pravic na internetu	7	10	5	5	6	13	6	7
Napad na informacijski sistem	88	283	98	76	69	275	78	25
Izdelovanje in pridobitev orožja ali pripomočkov za vdor ali napad na informacijski sistem	13	10	0	2	17	11	0	3
Skupaj	**111**	**309**	**114**	**101**	**96**	**304**	**90**	**39**

Vir: www.policija.si

Število kaznivih dejanj računalniške kriminalitete se je v letu 2010 zmanjšalo s 114 (storjenih leta 2009) na 101 ali za 11,4 %, število ovadenih oseb pa z 90 (leta 2009) na 39 (leta 2010) ali za 56,7 %. To je posledica zmanjšanja števila zlorab elektronskega bančništva, s pomočjo katerih so bila storjena druga kazniva dejanja računalniške kriminalitete; policija se je tudi bolj usmerila v zavarovanje in preiskovanje elektronskih naprav oziroma t. i. računalniško forenziko. Uporabnike elektronskega bančništva, pa tudi interneta in novih tehnologij, je opozarjala na možne nevarnosti njihove uporabe[6].

V zadnjih nekaj letih v Sloveniji beležimo trend, da okrožna državna tožilstva zavržejo kar 70 odstotkov ovadb, obtožni predlog pa je bil vložen le zoper 15 odstotkov ovadenih oseb. Nadaljnji osip se nadaljuje na sodiščih, kjer je bila za odgovorno spoznana le desetina vseh obtoženih oseb. V slabi tretjini primerov je bil postopek na sodišču ustavljen, v dobri četrtini primerov pa so bile obtožene osebe oproščene obtožbe. Polovica vseh obravnav na sodiščih se je končala z zavrnitvijo obtožnice ali zavržbo obtožnega akta.

SI-CERT[7] je v letu 2010 prejel 1.959 sporočil, od katerih je bilo 861 utemeljenih prijav incidentov (ostalo predstavlja vprašanja in sporočila, ki se ne nanašajo na varnostne incidente na omrežju). Na podlagi prijav so obravnavali 478 incidentov, kar predstavlja kar 43-odstotno povečanje v primerjavi z letom 2009. Največ prijav se nanaša na različna vprašanja in splošno svetovanje. Na podlagi takih prijav lahko zaključimo, da lahko z ustreznim izobraževanjem in ozaveščanjem širše javnosti pripomoremo k bolj varni uporabi omrežja. Sledijo preiskave zlonamerne kode, vdori v računalniške sisteme in phishing (več o tem v nadaljevanju). Še vedno torej prednjači "klasično" računalniško vdiranje, čeprav smo porast spletnih goljufij opazili že leta 2009.

Računalniško kriminaliteto bi najprej lahko opredelili kot tiste vrste kriminaliteto, ki je storjena z uporabo računalnikov – tista kriminaliteta torej, katere orodje za izvršitev kaznivega dejanja je računalnik. Vendar pa to velja tudi za mnogo tako imenovanih

[6] Podatki iz letnega poročila za leto 2010 o delu policije.
[7] Slovenski center za obravnavo omrežnih incidentov. Poročilo za leto 2010 je objavljeno na spletni strani http://www.cert.si/fileadmin/dokumenti/si-cert/SI-CERT_obravnavani_incidenti_2010.pdf

kibernetskih kaznivih dejanj, ki bi jih lahko opredelili kot tista dejanja, ki so zagrešena v kibernetskem prostoru ali z uporabo interneta. Ker imajo omreženi računalniki dostop do interneta in so tako lahko navzoči pri različnih kibernetskih lumparijah, omenjeni kriterij razlikovanja ni dovolj natančen, hkrati pa pojasnjuje naslednji pojav. V literaturi lahko namreč zelo pogosto zasledimo, da se izraza »kibernetska« in »računalniška« izmenjujeta, oziroma celo trditve, da gre pri računalniški kriminaliteti za enega od sinonimov za kibernetsko kriminaliteto. Omenjeno prepričanje ni presenetljivo, glede na to, da v mnogih primerih res prihaja do prekrivanja. Zato lahko morda pridemo do bolj natančne tipologije tovrstne kriminalitete, če si pogledamo vlogo, ki jo igra računalnik v teh operacijah (Peršak 2006, 10).

Računalnik je namreč lahko orodje za storitev kaznivega dejanja ali pa tarča napada. Nekateri uporabljajo ta kriterij tudi za pojasnilo razlik med računalniško in kibernetsko kriminaliteto. Tako je po njihovem mnenju računalniška kriminaliteta izraz, ki opredeljuje kazniva dejanja, kjer je računalnik tarča napada, medtem ko kibernetska kriminaliteta označuje kazniva dejanja, storjena preko interneta, kjer je računalnik uporabljen bodisi kot orodje bodisi kot tarča ali žrtev napada. Pri kibernetski kriminaliteti gre torej za uporabo računalnikov in mrež oziroma po definiciji ameriškega FBI za kakršnokoli goljufivo shemo, v kateri igra ena ali več komponent interneta, na primer spletne strani, klepetalnice in elektronska pošta, pomembno vlogo pri ponujanju neobstoječih dobrin ali storitev potrošnikom, navajanju lažnih ali goljufivih predstav o shemah potrošnikom ali prenašanju denarnih sredstev žrtve dostopnih naprav ali drugih vrednostnih predmetov pod nadzor storilca sheme. Samo ime kibernetska kriminaliteta naj bi po Forji (Peršak 2006, 10) skovali konec 90-ih, ko se je internet (zlasti v Severni Ameriki) že dovolj razširil med prebivalstvom. Po sestanku G 8 v Lyonu naj bi iz zaskrbljenosti nad pojavom kriminalnih dejavnosti na internetu izoblikovali podskupino, katere naloga je bila preučiti omenjeno kriminaliteto, ki se je selila na internet oziroma jo je internet porajal. »Lyonska skupina« je tako začela na široko uporabljati izraz kibernetska kriminaliteta za opis vseh vrst dejanj, storjenih v medmrežju oziroma z uporabo novih telekomunikacijskih mrež, ki so postajala čedalje cenejša. Kibernetska kriminaliteta je tako pomenila izkoriščanje novih tehnologij pri storitvi starih tradicionalnih kaznivih dejanj na nov način, pa tudi za vrsto novih kriminalnih dejavnosti. Lažja delitev je torej

na stara kazniva dejanja, storjena na nov (internetni) način, in na nova kazniva dejanja, ki jih je internet šele omogočil (Peršak 2006, 10).

4.1 NAČINI IZVRŠEVANJA KAZNIVIH DEJANJ V KIBERNETSKEM PROSTORU

V kibernetsko kriminaliteto po Konvenciji Sveta Evrope o kibernetski kriminaliteti uvrščamo protipravni dostop, protipravno prestrezanje, motenje podatkov, motenje sistemov, zlorabo naprav, računalniško ponarejanje, računalniško goljufijo, kazniva dejanja, povezana z otroško pornografijo, kazniva dejanja, povezana s kršitvijo avtorske in sorodnih pravic.

Nekateri kibernetsko kriminaliteto definirajo kot vsako obliko kriminala, pri kateri je uporabljena računalniška oziroma, v širšem smislu, celo informacijska tehnologija. Vendar pa sta Douglas Tomas in Brian D. Loader (Kovačič 2006, 87) mnenja, da kibernetska kriminaliteta ni samo uporaba informacijsko-komunikacijske tehnologije v kriminalne namene, pač pa je bistveni element kibernetske kriminalitete v tem, da takšen kriminal ne bi bil mogoč brez uporabe tehnologije, vsaj ne v takšnem obsegu. Poleg tega se kibernetska kriminaliteta po Reitingerju od navadnega kriminala razlikuje še po treh pomembnih značilnostih (Kovačič 2006, 87):

- lahko je izvedena na daljavo,
- identiteto osebe, ki kaznivo dejanje izvede, je mogoče razmeroma preprosto zakriti ali ponarediti (to je tudi razlog za številne internetne prevare, tako imenovani phishing),
- poleg tega pa sledenje izvornemu komunikacijskemu sredstvu, preko katerega se je nekdo povezal v kibernetski prostor, ni vedno mogoče, saj izurjeni napadalci pogosto uporabljajo tehniko povezovanja preko različnih sistemov (angleško: looping ali weaving – gre za tehniko, ko se napadalec s ciljnim sistemom ne poveže neposredno, pač pa preko številnih drugih sistemov, po možnosti lociranih v različnih državah, kar onemogoči ali vsaj oteži sledenje).

Kibernetski kriminal (Cyber Crime), računalniški kriminal (Computer Crime), kriminal v zvezi z računalniki (Computer-related Crime), kriminal visokih tehnologij (High-tech Crime), digitalni kriminal, IT-kriminal so izrazi, ki se uporabljajo pri najnovejših oblikah

kriminala. Definicija kriminala visokih tehnologij navaja, da je to uporaba informacij in komunikacijskih tehnologij pri storitvi kaznivega dejanja zoper osebo, lastnino, organizacijo ali informacijski sistem (Europol 2007). Kibernetski kriminal pojmujemo kot kaznivo uporabo računalniškega omrežja ali drugega sistema na internetu, napade ali zlorabe sistemov in omrežij za kriminalne namene, kazniva dejanja in zlorabe z uporabo novih tehnologij ali nova kazniva dejanja, ki se na novo razvijajo na internetu. Kriminal v zvezi z računalniki lahko pojmujemo kot kriminal, ki ga sestavljajo kazniva dejanja, pri katerih se računalnik pojavlja kot orodje ali kot predmet napada za izvršitev ali poskus izvršitve kaznivega dejanja, za uspešno preiskovanje pa je potrebno določeno znanje iz računalništva ali informatike. Izraz računalniški kriminal se nanaša na dejanja, ki so storjena s pomočjo elektronske opreme za obdelavo podatkov in ki povzročajo nezaželene posledice. Gre za kakršnokoli kriminalno dejavnost, ki zajema kopiranje, odstranitev, vmešavanje, vdor, uničenje ali drugo manipulacijo računalniškega sistema, računalnika, podatkov ali računalniških programov (Kastelic 2005).

Informacijski sistemi, omrežja in komunikacijske naprave postajajo vse bolj povezani. Tovrstno zbliževanje je povečalo možnost vnosov, manipulacij, oviranj, uničenj in kraj podatkov, ki se nahajajo ali prenašajo med temi sistemi. Današnja družba je postala zelo odvisna od omrežij in pretoka podatkov po njih in do elektronske avtomatizacije mnogih dejavnosti, zato je očitno, da je ranljivost velika. Globalna ranljivost »omrežne« družbe je razvidna iz incidentov kraje podatkov, spletnih goljufij, razširjanja zlonamernih virusov, onesposobljenih sistemov in milijonskih škod. Računalniki in internet so kriminalcem dodali na razpolago še eno orodje za povzročanje kaznivih dejanj. Internet jim omogoča globalno razsežnost, anonimnost, neposredno varno komunikacijo, dostop do znanja, večje število žrtev, obilico nelegalnih priložnosti in pomoč pri obstoječih nelegalnih poslih. Računalniški kriminal pogosto kot dejanje ni osamljen, temveč je del kriminalne dejavnosti, ki se pojavlja v fizični obliki. S porastom in sprejetjem interneta s strani družbe so se zelo povečali tipi žrtev in njihovo število, ki so zdaj razširjene po vsem svetu, in sicer od vojaških, vladnih, izobraževalnih ustanov, podjetij in drugih poslovnih uporabnikov, družb, ki skrbijo za infrastrukturo in servise na internetu, do posameznih uporabnikov interneta in kritičnih infrastruktur družbe (preskrba z elektriko, vodo, gorivi, nujno medicinsko pomočjo ipd.). Tako je eden izmed večjih izzivov, s

katerim se srečujejo organi pregona pri boju z mednarodnim računalniškim kriminalom, prav njihova sposobnost učinkovitega usklajevanja preiskav med različnimi zakonodajami in pravnimi ureditvami (Kastelic 2005).

4.2 LASTNOSTI RAČUNALNIŠKE KRIMINALITETE

Računalniško kriminaliteto lahko definiramo tudi kot kriminaliteto belih ovratnikov. Odkrita kazniva dejanja v zvezi z računalniki kažejo, da so storilci pri izvršitvi uporabili strokovno znanje, ki ga ima le malo ljudi. Tovrstni kriminal predstavlja poseben problem in treba je opredeliti njegove glavne posebnosti (Jakulin 1996, 826):

- ni vidnih posledic kaznivega dejanja,
- ni sledi, zato je odkrivanje toliko težje,
- dejanje je izvršeno zelo hitro (v tisočinkah sekunde),
- storjeno je lahko na daljavo, storilec ni navzoč na samem kraju kaznivega dejanja,
- motiv ni vedno gmotna korist,
- preiskovalci so vezani na zapis na papirju, terminalu, mikrofilmu, njegova pravilnost pa je odvisna od tega, ali je narejen na osnovi njihovega lastnega programa,
- storilci so zelo izurjeni, izobraženi in imajo dovolj obsežno znanje s področij računalništva in informatike, da uspešno prikrijejo sledi.

Razvoj računalništva je izjemno hiter, zato je potrebno tudi odkrivanje tovrstnega kriminala hitro razbijati, biti v koraku s časom. En sam človek težko natančno obvladuje vse računalniško znanje, zato sta potrebna specializacija in oblikovanje skupine strokovnjakov, ki bo tako pri odkrivanju kriminalitete v prihodnosti uspešnejša.

Veliko pozornost računalniški kriminaliteti posveča tudi Svet Evrope. Ta je na konferenci leta 1989 sprejel priporočilo št. R (89) 9 o kriminaliteti v zvezi z računalniki, ki predstavlja vodilo za oblikovanje nacionalnih zakonodaj. Svet Evrope je s priporočilom vladam držav članic svetoval, da ob spremembah zakonodaje ali pripravi nove zakonodaje upoštevajo poročilo evropskega komiteja za probleme kriminalitete v zvezi z računalniki ter generalnemu sekretarju Sveta Evrope poročajo o spremembah lastne

zakonodaje, sodni praksi in izkušnjah z mednarodnim sodelovanjem na področju računalniške kriminalitete (Jakulin 1996, 824).

Priporočilo vsebuje minimalni in neobvezni seznam kaznivih dejanj računalniške kriminalitete. V minimalni seznam so uvrščeni (Bequai 1990, 176):

a) z računalnikom povezana goljufija (računalniška goljufija): vključuje vnos, spremembo, izbris ali uničenje računalniških podatkov ali programov ali pa drug poseg v računalniško obdelavo podatkov, ki vpliva na rezultat njihove obdelave, z namenom pridobiti protipravno premoženjsko korist sebi ali komu drugemu;
b) računalniška ponareditev: je vnos, sprememba, izbris ali uničenje računalniškega podatka ali programa ali drug poseg v obdelavo podatkov na način ali pod pogoji, ki jih predpisuje nacionalna zakonodaja za ponareditev, če je storjena proti tradicionalnemu objektu takšnih dejanj;
c) poškodovanje računalniških podatkov ali programov: pomeni neupravičeni izbris, poškodovanje, poslabšanje ali uničenje računalniških podatkov ali programov;
d) računalniška sabotaža: zajema vnos, spremembo, izbris ali uničenje računalniških podatkov ali programov ali drug poseg v računalniške sisteme, katerega namen je ovirati delovanje računalniškega ali telekomunikacijskega sistema. Osnovna značilnost sabotaže je, da storilec navadno nima neposredne koristi, pač pa iz različnih motivov povzroča škodo na strojni in programski opremi ter podatkih;
e) neavtorizirani dostop: zajema vse možne oblike neupravičenega dostopa (vdora) v računalniški sistem ali mrežo s kršenjem zaščitnih ukrepov;
f) neavtorizirano prestrezanje: obsega neupravičeno prestrezanje s tehničnimi sredstvi na komunikacijah računalniškega sistema ali mreže;
g) neupravičeno razmnoževanje zavarovanega računalniškega programa: zajema neupravičeno razmnoževanje, razširjanje ali dajanje v promet računalniških programov, ki so zavarovani z zakonom;
h) neupravičeno razmnoževanje topografije: pomeni neupravičeno kopiranje z zakonom zavarovane topografije, neupravičeno kopiranje polprevodnikov,

neupravičeno gospodarsko izkoriščanje ali uvoz topografije ali polprevodnikov, izdelanih z uporabo topografije.

Neobvezni seznam pa zajema še štiri kazniva dejanja:

- spremembo računalniških podatkov ali programov,
- računalniško vohunstvo,
- neavtorizirano uporabo računalnika,
- neavtorizirano uporabo zavarovanega računalniškega programa.

Najpogostejša kazniva dejanja, ki jih danes zasledimo in ki vključujejo informacijsko tehnologijo, so: goljufija oziroma internetna prevara, tatvina, kraja intelektualne lastnine, piratstvo programske opreme, zlorabe plačilnih kartic, kraja identitete, pedofilija, terorizem, ekstremizem, prekupčevanje z drogami in orožjem, izsiljevanje in oderuštvo, pranje denarja, hekerstvo, napadi DoS (Denial of Service), virusi, črvi, trojanski konji in napadi na kritične infrastrukture družbe.

Na splošno lahko ekstremizem na internetu definiramo kot konvergenco ekstremizma in kibernetskega prostora. To so nezakoniti napadi ali grožnje na računalnike, mreže in informacije, ki so v njih shranjene, pod pogojem, da so izvedeni z namenom ustrahovati ali prisiliti vlado v podpiranje določenih političnih ali družbenih ciljev. Posledica napada mora biti nasilje nad ljudmi ali lastnino ali vsaj tolikšna škoda, da povzroča dovolj velik strah ljudi (Denning v Založnik 2007, 2). Zadnji del definicije je ključen, da takšno dejanje lahko razlikujemo od kibernetske vojne, kakor sta jo definirala John Arquilla in David Ronfeld (Založnik 2007, 2), ki v definiciji ne opredeljujeta fizičnih posledic motenja in uničevanja informacijskih in komunikacijskih sistemov.

Pri informacijskem terorizmu gre torej za napade na računalniške sisteme z namenom prizadejati škodo posameznikom, in ne računalnikom. Značilnosti tega terorizma so potencialna velika učinkovitost v družbah, v katerih računalniški sistemi nadzorujejo večino posameznikovega življenja. To pomeni, da gre za nadzor nad različnimi državnimi podsistemi (zdravstvo, izobraževanje, poslovanje, sodni pozivi), ki so danes del kritične

infrastrukture in njene zaščite. Zloraba takšnih podatkov bi lahko imela hude posledice in bi dejansko lahko ohromila normalno delovanje družb (Svete 2007, 128).

Strokovnjaki se pri definiranju kibernetskega terorizma in ekstremizma na internetu razlikujejo glede na raven te podobnosti med njima. Zgornja definicija se osredotoča na terorizem in internetni ekstremizem le na ravni posledic takšnega dejanja. Nekatere definicije pa k temu dodajo še razsežnost storilcev – dodajajo torej, da je internetni ekstremizem dejanje ekstremistične skupine, kar pojem še bolj omeji. Definicija je zelo ozka, vendar je to potrebno, da se lahko internetni ekstremizem razlikuje od drugih oblik računalniških zlorab, kot so hekerstvo, aktivizem, gospodarsko vohunstvo, internetno goljufanje in podobni zločini (Založnik 2007, 2).

Vprašanje grožnje ekstremizma na internetu obstaja na dveh ravneh: ali so kritične infrastrukture, ki so možna tarča takšnih napadov, ranljive in v kolikšni meri so ekstremisti usposobljeni za takšen tip napadov. Kritične infrastrukture, kot so vojaške, letalske, medicinske, energetske itd., so ranljive do neke mere. Sami računalniški sistemi so zelo ranljivi, še zlasti zaradi vzajemne odvisnosti in medsebojne povezanosti, tako da obstaja možnost napada. Vsi računalniški sistemi pa imajo nadzornika; vedno je prisoten človek, ki bi v primeru napada interveniral. Dokler bo v procese kontrole vpletenih dovolj ljudi, kibernetski terorizem ali drugi ekstremizmi ne bodo resna grožnja (Založnik 2007).

Če le sprejmemo ranljivost tarč do neke mere kot dan faktor, pridemo do vprašanja sposobnosti in motivacije ekstremistov. Običajni hekerji imajo znanje, sposobnosti in orodja, da bi takšen napad izvedli, vendar nimajo v sebi motivacije, da bi povzročali nasilje, hudo ekonomsko ali družbeno škodo. Po drugi strani pa ekstremisti, ki to motivacijo imajo, nimajo sposobnosti ali motivacije, da bi takšno škodo povzročali v kibernetskem prostoru. Ekstremisti sicer uporabljajo internet kot podporo tradicionalnih oblik terorizma, kot je, na primer, nastavljanje eksplozivnih teles. Vzpostavljajo spletne strani, ki razširjajo njihove politične ali družbene cilje, pridobivajo nove člane, med seboj komunicirajo in koordinirajo napade (Založnik 2007, 3).

4.3 VRSTE KRIMINALNIH DEJAVNOSTI V INTERNETNEM PROSTORU

Vedno večja uporaba sodobnih tehnologij pri kaznivih dejanjih (vzrok je tudi cenovna dostopnost opreme) je povzročila, da je prav računalnik v današnjem času udeležen v širokem spektru kaznivih dejanj. Vlogo računalnika, ki jo ima ta pri kaznivih dejanjih, lahko razdelimo na več delov (Kastelic 2005):

1. računalnik kot orodje za storitev kaznivega dejanja,
2. računalnik kot tarča oziroma žrtev kaznivega dejanja,
3. računalnik kot naprava, ki hrani dokaze kaznivega dejanja,
4. računalnik kot pomoč organom pregona.

Računalnik kot orodje za storitev kaznivega dejanja

Primerov, kjer računalnik nastopa kot orodje za storitev kaznivega dejanja, je vedno več in prav tu najpogosteje prihaja do novih oblik kriminalitete. Nekateri primeri uporabe računalnika so:

orodje hekerjem:

- vdor v računalniški sistem,
- brisanje, spreminjanje in/ali vnašanje podatkov v napadeni računalnik,
- onesposobitev ali oviranje delovanja omrežij,
- kraja informacij, gesel, številk kreditnih kartic;

orodje pedofilom:

- izmenjava otroške pornografije,
- udeležba v spletnih klepetalnicah za dogovarjanje srečanj z otrokom;

orodje kriminaliteti belega ovratnika:

- spletne bančne goljufije,
- ponarejanje čekovnih in kreditnih kartic,
- sleparske oziroma goljufive reklame in prodaje,
- piramidne igre,
- intelektualna lastnina.

Računalnik kot tarča oziroma žrtev kaznivega dejanja

V teh primerih računalnik nastopa kot žrtev oziroma tarča kaznivega dejanja, to pa je lahko hekerski napad. Taki računalniki so najpogosteje zanimivi zaradi podatkov, ki se nahajajo v njih. Tu je pomembno omeniti industrijsko vohunstvo, ki je v nekaterih industrijsko in informacijsko razvitih državah v velikem porastu. Nekateri primeri, pri katerih je računalnik žrtev, so:

- dostop do shranjenih zaupnih informacij,
- poslovne skrivnosti,
- pridobitev brezplačnih storitev,
- posrednik za napad na druge računalnike.

Računalnik kot naprava, ki hrani dokaze kaznivega dejanja

Zaradi razširjenosti računalnikov v gospodarstvu, gospodinjstvih in pri kriminalcih tovrstne naprave v vedno večjem številu primerov kaznivih dejanj vsebujejo pomembne podatke, ki lahko služijo kot dokaz. Razni seznami, imeniki, poslovna dokumentacija ipd. so v večini primerov iz »papirne oblike« prešli v elektronsko obliko. Najpogosteje gre za:

- sezname oseb z naslovi, telefonskimi številkami ipd.,
- koledarje s seznami pomembnih dogodkov,
- baze podatkov,
- osebno in poslovno korespondenco:
    - elektronska sporočila,
    - pisma, pogodbe ipd.,
- fotografije,
- finančne podatke.

Računalnik kot pomoč organom pregona

Nenazadnje so računalniki lahko tudi odličen pripomoček organom pregona pri odkrivanju, preiskovanju in dokazovanju kaznivih dejanj. Glede na to lahko navedemo nekatere primere uporabe računalnika:

- uporaba baz podatkov,
- izdelava preglednic o finančnih transakcijah,
- iskalna orodja na internetu,

- predstavitve za sodišča.

Storilci kaznivih dejanj s pomočjo interneta izvršujejo kazniva dejanja zaradi različnih motivov, najpogostejši pa so (Europol 2007):

- pridobitev premoženjske ali druge koristi (pridobitev informacij, tatvina storitev, izogibanje plačilu za blago ali storitve),
- politični motivi,
- zlonamernost, škodoželjnost,
- radovednost,
- osebne spodbude (npr. občutek moči, sposobnost, dokazovanje).

4.4 HEKERJI IN NJIHOVE TEHNIKE

Heker je oseba, ki eksperimentira z omejitvami sistema zaradi radovednosti ali samega užitka. Hekerji se po tej definiciji z vdiranjem v sisteme ukvarjajo predvsem ljubiteljsko in niso organizirani. So stereotipni moški na družbenem robu. Hekerji so razpršena skupina ljudi, ki udari, kjer lahko, in tudi tekmuje med seboj in ni homogena. Motivira jih predvsem lastni ego, uporništvo in izziv, ki ga vdor predstavlja (Wenger v Svete 2005, 37).

Za hekerje je značilno, da jih v računalniški kriminal ne vodi osebna korist ali škoda, ki jo povzročijo, ampak gre pri njih za intelektualni izziv in v informacijski sistem vdirajo za zabavo. Pogosto se zamenjuje pojma heker in kreker, ki se pogosto pojavljata kot glavna akterja pri zlorabah interneta. Glavna razlika med njima je, da hekerja definiramo kot osebo, ki pogosto dokazuje svoje sposobnosti, moč in dovršenost ter odkriva luknje v računalniških sistemih iz različnih vzrokov. Hekerji tako nenehno težijo k iskanju novega znanja, k dokazovanju svojih sposobnosti in znanje pogosto delijo z ostalimi, pri tem pa ne uničujejo in si ne prilaščajo oziroma ne uporabljajo podatkov, ki bi lahko škodili ostalim uporabnikom interneta. Zato so hekerji pogosto osebe, ki so strokovnjaki s področja programskega jezika in računalniških sistemov. Ker pa jih ljudje pogosto ocenjujejo kot negativne osebe, ki nezakonito vdirajo v sisteme, jih nekateri delijo na »white-hat« in na »black-hat«, glede na njihov motiv. Krekerja lahko prav tako definiramo kot osebo, ki vdira v računalniška omrežja, vendar ne z namenom iskanja

novega znanja, temveč z namenom povzročati težave svojim »tarčam«, uničiti sistem ali izvajati nezakonite dejavnosti, kot sta kraja in vandalizem (Turban 2003, 393).

Izraz heker je prvi uporabil Joseph Weizenbaum leta 1976, popularno pa izraz danes opisuje posameznika, ki ima veliko računalniško-tehničnega znanja, to znanje pa izkorišča za napad na računalniške sisteme, kar hekerje uvršča v polje računalniške kriminalitete. Izraz hekanje se večinoma uporablja za »kompleksno mešanico legalnih in nelegalnih dejavnosti, od legitimnega kreativnega programiranja do prepovedanega vdiranja in manipulacije svetovnih telefonskih ali računalniških sistemov«; najpogosteje pa se ga dojema kot sofisticirano ilegalno dejavnost. Čeprav z izrazom heker danes poljudno označujemo kateregakoli kibernetskega kriminalca, pa Thomas in Loader kibernetske kriminalce delita v tri kategorije (Kovačič 2006, 87):

- hekerje in phreakerje (angleško: phreaker; gre za »telefonske hekerje«, ki se ukvarjajo z zlorabo telefonskih sistemov; phreakerji so bili predhodniki hekerjev, formirati pa so se začeli v ZDA konec sedemdesetih let, v današnjem času jih skorajda ni več), ki vdirajo v sisteme večinoma iz radovednosti in ne povzročajo škode,
- trgovce z informacijami, katerih glavni motiv je dobiček, ter
- teroriste, ekstremiste in deviantneže, ki informacijske sisteme uporabljajo za nezakonite politične ali družbene dejavnosti (na primer razširjanje sovražnega govora, otroške pornografije, napade na strežnike sovražnih držav).

Obstaja pa še druga delitev, ki kaže, kako se je pojem (in odnos do njega) razvijal skozi čas. Levy (Kovačič 2006, 87) pravi, da obstajajo štiri generacije hekerjev, s katerimi se je pojem hekerja spreminjal skozi čas. Prva generacija, ki izvira iz MIT (Massachusetts institute of technology, v njihovih laboratorijih so prvič uporabili izraz heker) je v petdesetih in šestdesetih letih prejšnjega stoletja razvila prve programske tehnike. Drugo generacijo predstavljajo tisti posamezniki, ki so razvili prve osebne računalnike in s tem omogočili dostop do računalniške tehnologije širšim množicam. Tretjo generacijo označujejo vodilni razvijalci računalniških iger. Četrto pa osebe, ki na nedovoljene načine vstopajo v tuje računalnike. Iz te delitve tudi izhaja, da so bili prvotni hekerji predvsem

ustvarjalni, zadnja generacija hekerjev pa naj bi bila že v večji ali manjši meri destruktivna.

Po samodefiniciji pa se hekerji v hekerskem slovarju opisujejo kot »osebe, ki uživajo v raziskovanju računalniških sistemov in iskanju njihove uporabe, osebe, ki navdušeno, celo obsedeno programirajo, osebe, ki uživajo v intelektualnih izzivih, v aktivnem premagovanju in zaobhajanju omejitev« (Kovačič 2006, 87).

Vsaka oseba ima za določeno ravnanje svoje motive in vzgibe. Motivi, ki vodijo hekerje po svetu, so:

- ugled, veljava (kot pri vsakem poklicu so tudi tu prisotni prestiž, ugled in sloves najboljšega, ki je zelo cenjen),
- zbirka (ni pomemben samo en uspešno izveden napad, šteje čim večja zbirka, nabor »žrtev« v zbirki hekerja),
- odskočna deska (v primeru uspešno izvedenega načrta heker pridobi na ugledu in cenjenosti, kar je ključnega pomena za njegovo življenjsko pot in uspešnost na tem področju),
- informacije, podatki (informacije so v današnjem času informacijske družbe vedno vredne, dragocene in iskane, ljudje so zanje pripravljeni odšteti velike vsote),
- maščevanje (dejavnik, ki pogosto usmerja bivše zaposlene ali pa tudi zaposlene, ki niso zadovoljni s svojo plačo, z delovnimi razmerami, s svojimi predpostavljenimi).

Načini, s katerimi hekerji uresničujejo svoje načrte:

- neposredni napad (uporaba skripte),
- družbene tehnike (navezovanje stikov, poznanstev z namenom pridobiti podatke in informacije),
- kazniva dejanja (vlom, kraja, uporaba fizične sile, podkupovanje, napeljevanje, izsiljevanje zaposlenih z namenom uresničiti želene cilje).

Osnovna orodja in tehnike hekerjev so trojanski konji, skenerji, vohljači (angleško: Snifferes) in socialni inženiring. Dodatna hekerska orodja so razbijalci gesel in orodja za skrivanje identitete in brisanje sledi. Med uničevalne programe in tehnike pa sodijo logične bombe, virusi, črvi in DoS (angleško: Denial of Service) (Podjet 2008).

Trojanski konji

Med zelo znane varnostne grožnje sodijo trojanski konji, saj so precej učinkoviti in jih je zelo težko odkriti. V bistvu so to majhni programi, ki so najpogosteje skriti v drugih programih. Izvirne programe lahko hekerji spremenijo, tako da vanje dodajo svoje programe, lahko pa izdelajo na videz povsem dobre programe, vanje pa pred uporabniki skrijejo še dodatne funkcije, ki izvajajo neavtorizirane operacije. Namen trojanskih programov je predvsem v zbiranju želenih sistemskih informacij (na primer gesel, privilegijev) ali v uničevanju sistemov (Podjet 2008).

Zlasti nevarni so trojanski konji, ki odpirajo tako imenovana zadnja vrata (angleško: back door) računalniških sistemov, saj je njihov učinek v tem, da omogočajo napadalcu oddaljen dostop do informacijskega sistema. Med najbolj znane trojanske konje, ki so napadalcem puščali odprta zadnja vrata, sodi program »Back Orifice«. Večina teh orodij je narejena pod krinko legalnosti, saj naj bi sistemskim administratorjem olajšala delo. Uspešnost napadov s trojanskimi konji je odvisna od različnih računalniških programov, s katerimi preverimo pomanjkljivosti poljubnega računalniškega sistema. Pomagamo si lahko tudi s protivirusnimi programi, ki jih moramo nenehno posodabljati, na voljo pa imamo tudi kopico programov, ki preverjajo, ali so bile datoteke spremenjene (Podjet 2008).

Skenerji

Skener je eno izmed najbolj priljubljenih hekerskih orodij. To je program, ki samodejno išče šibke točke v varnosti poljubnih omrežnih strežnikov, torej strežnikov, ki se nahajajo kjerkoli na svetu. Skenerji delujejo tako, da zaporedoma napadajo vrata računalnikov in različne storitve, ki skrbijo za komunikacijo računalnika z zunanjim svetom. Poznane varnostne pomanjkljivosti, imenovanje luknje oziroma odgovore računalnika, si skenerji

zapišejo in te pozneje lahko heker izkoristi. Napade starejših skenerjev zlahka odkrijemo z opazovanjem dejavnosti strežnika, novejših, prikritih skenerjev pa skorajda ne moremo odkriti. Pred skenerji se zaščitimo z dobrimi požarnimi zidovi in tudi z rednim dodajanjem popravkov, ki odpravljajo pomanjkljivosti našega operacijskega sistema (Podjet 2008).

Razbijalci gesel

Razbijalci gesel so različni programi, ki omogočajo prebiranje šifriranih podatkov, najpogosteje gesel. Mehanizmov odkrivanja gesel je precej, kakor je precej tudi postopkov šifriranja. Razbijalce gesel heker najpogosteje uporablja na svojem računalniku. Računalnik pa mora biti precej zmogljiv, saj mora opraviti ogromno operacij. Iz tega sledi tudi preventiva. Dobra gesla so dolga gesla, za katera heker potrebuje ogromno časa, da jih razbije, in gesla ne smejo biti preproste besede. Uporabljamo le najboljše programe za šifriranje (Podjet 2008).

Orodja za skrivanje identitete in brisanje sledi

Ta orodja se uporabljajo za zakritje napadalčevih sledi. Če napadalec namesti zlonamerni program, ki je potem odkrit, lahko napadalec s tem izgubi nadzor ali dostop do sistema v prihodnosti. Zaradi tega se s pomočjo teh orodij skrije prisotnost zlonamernih programov v sistemu. Podobne zlorabe dajejo skrbniške pravice nepooblaščenim uporabnikom, saj so zelo uporabne za napadalce in dovoljujejo vsem, ki imajo kakršenkoli dostop do sistema, da si sami povečujejo pravice in izvajajo dejavnosti, ki jih želijo. Uničevalni programi so namenjeni poškodovanju ali popolnemu uničenju podatkov. Namen uničevanja je lahko objestnost, izsiljevanje ali škodovanje tekmecem. Uničevalne programe lahko odkrijemo precej hitro, z ustreznimi programskimi dodatki in izobraževanjem osebja pa se jim lahko precej uspešno upremo (Podjet 2008).

DoS (Denial of Service)

DoS je tehnika, s katero hekerji ali krekerji poskušajo zlomiti sistem, tako da preobremenijo medpomnilnik, diske, centralno procesno enoto ali samo omrežje. Izkoriščanje različnih prenapolnjenosti je danes eden izmed največjih problemov računalniške varnosti. Tovrstni napadi predstavljajo kar polovico vseh napadov. Vse aplikacije izrabljajo določen del medpomnilnika, ki vsebuje podatke, in ta del ima fiksno

velikost. Če napadalec pošlje preveč podatkov v enega izmed medpomnilnikov, pride do njegove prenapolnjenosti. Strežnik prelisičimo na takšen način, da poganja programe, ki so v prenapolnjenem medpomnilniku, kar lahko pomeni, da bo lahko celo program pošiljal gesla tretjim osebam, prišlo bo do odprtja zadnjih vrat ali česa drugega. Vse je odvisno od tega, kakšne podatke bo napadalec poslal medpomnilniku. Tovrstne zlorabe so zelo pogoste, relativno preproste in tudi zelo učinkovite (Podjet 2008).

Virusi

Najbolj znani uničevalni programi so virusi. Te delimo na nekaj osnovnih skupin, a vsem je skupno to, da najpogosteje nekaj uničijo in se, za razliko od trojanskih konjev, samodejno širijo od računalnika do računalnika. Proti njim se borimo s protivirusnimi programi, najpogosteje s takšnimi, ki v realnem času nadzirajo vse prenesene podatke, sposobni pa so tudi občasno temeljito pregledati računalniški sistem (Podjet 2008).

Črvi

Črvi so zlonamerni programi, ki se sami širijo po internetu in napadajo različne strežnike ter izkoriščajo njihov ranljivost. Nove oblike črvov, kot sta Code Red in Nimda, so pripomogle k veliko nevarnejšemu in učinkovitejšemu napadanju strežnikov po internetu. Napadalci črve uporabljajo za napadanje številnih organizacij hkrati (Podjet 2008).

Hiter razvoj interneta in računalniške tehnologije je pripeljal do novih oblik izvrševanja kaznivih dejanj. Zaradi široke povezanosti in velikega števila dostopov do interneta je ranljiv prav vsak uporabnik interneta. Ravno internet je povzročil, da za izvrševanje nekaterih kaznivih dejanj s pomočjo interneta ni potrebno računalniško predznanje, temveč se storilec lahko o načinu izvrševanja pouči kar na svojem računalniku, s katerim nato izvrši kaznivo dejanje.

4.4.1 RIBARJENJE (PHISHING)

Phishing ali ribarjenje je najpogostejša vrsta socialnega inženiringa na internetu. Je kraja zasebnih podatkov s pomočjo ponarejenih elektronskih sporočil in spletnih strani. Najpogosteje so ponarejene spletne strani finančnih organizacij, strani spletnih prodajaln

oziroma oglasnikov in ponudnikov internetnih storitev (Tipton in Krause 2008, 2856). Vse pogosteje pa so tarča ribarjenja strani, namenjene socialnemu omreževanju uporabnikov, kot denimo Facebook, MySpace ipd. (Artur 2009). Sama beseda phishing izvira iz besede »fishing« (ribarjenje), kjer sta črko »f« zamenjali črki »ph«. Ta zamenjava črk pa izvira iz začetkov računalniškega vdiranja v omrežja, in sicer vdiranj v telefonska omrežja, ki so se imenovali »phreaking«. Ta beseda pa izhaja iz »phone freaking« (Tipton in Krause 2008, 2856). Druga razlaga izvora besede phishing je skovanka besed »password« (geslo) in »fishing« (ribarjenje), torej ribarjenje gesel (Škrt 2005).

Postopek ribarjenja je tak, da »ribič« najprej izbere organizacijo, za katero se bo pretvarjal, ter nato izdela podobno oziroma identično stran. Ko je stran izdelana, potrebuje uporabnike, ki bi tej strani nasedli. Te privabi z elektronskimi sporočili, ki jih pošlje na mnoge naslove. Načinov, kako uporabnike privabi, je veliko. Običajno uporabnika storitev obvesti, da je prišlo do določenega zapleta ter da je treba ponovno vnesti uporabnikove podatke, da bodo lahko nadaljevali z uporabo storitve. Izmed ogromnega števila poslanih sporočil se jih mnogo zaustavi že na prejemnikovih filtrih za nezaželeno pošto. Čeprav se le določen odstotek sporočil prebije do uporabnikov, je ta številka še vedno lahko zelo velika. Število napadov se zmanjša tudi s tem, ker uporabniki enostavno ignorirajo neznana sporočila. Sporočilom podležejo tisti uporabniki, ki so v strahu, da bi izgubili določeno storitev (Tipton in Krause 2008, 2856).

4.4.2 PHARMING

Pharming[8] je prevara, zelo podobna phishingu, s to razliko, da se jo težje odkrije. Pharming predstavlja preusmerjanje z legitimnih strani na nelegitimne z namenom pridobitve zasebnih podatkov (Whitman in Mattord 2007, 72). Gre za neposredne napade na strežnike DNS[9] ali pa na datoteko o gostiteljih (ang. hosts file), ki se nahaja na uporabnikovem računalniku. Posledica tovrstnih napadov je ta, da so uporabniki, ne da bi to sploh vedeli, preusmerjeni na zlonamerne spletne strani (ang. malicious sites),

[8] Besedo »pharming« uporabljajo tudi v farmacevtski industriji. Beseda, ki je skovanka besed "farming" (kmetijstvo) in "pharmacy" (lekarništvo), predstavlja eno izmed tehnik genskega inženiringa.
[9] DNS je angleška kratica za Domain Name System/Service/Server (slovenski prevod je sistem domenskih imen).

čeprav v naslovno vrstico brskalnika pravilno vnesejo URL naslov strani, ki bi jo radi obiskali. Ker so lažne strani največkrat popolne kopije originalnih, uporabniki sploh ne opazijo, da se nahajajo na lažnem naslovu in da se v ozadju dogaja nekaj škodljivega. Ravno na to karto nevednosti pa igrajo napadalci, saj od uporabnikov, ki se nahajajo na lažni strani, ni težko izvabiti zaupnih podatkov, med katerimi so še posebej zaželene številke kreditnih kartic ter podatki, ki so potrebni za dostop in uporabo e-bančnih storitev. Posledica napada pharming je torej, da je uporabnik brez svoje vednosti preusmerjen na lažno stran, ki je popolna kopija originalne, vendar posebej narejena za zbiranje zaupnih podatkov z namenom njihove kasnejše zlorabe (Škrt 2005).

5 PRIJAZNA STRAN INTERNETA

Internet oziroma, natančneje, svetovni splet je zelo učinkovito orodje za hranjenje in dostop do želenih informacij. Večina iskanj informacij poteka tako, da iskalec preko iskalnikov, ki se uporabljajo kot orodje za iskanje informacij na spletu, v iskalno polje vpiše besedo ali besedno zvezo, ki opisuje oziroma zajema iskano vsebino. Prikažejo se rezultati in iskalec izbere tisto spletno stran, ki mu najbolj ustreza. Iskanje informacij je ena najbolj uporabljanih možnosti interneta tudi zato, ker je enostavno. Internet omogoča izmenjevanje informacij tako med posamezniki kot tudi skupinami iz različnih delov sveta, takšen način je hiter in poceni. Omogoča tudi skupinsko komunikacijo (forumi, novičarske skupine, razpravljalne deske, interaktivne konference …) z drugimi člani. Internet se je danes razvil v pravi velikanski elektronski katalog, v katerem si lahko izberemo poljubne izdelke iz katerekoli države. Imamo dostop do svoje banke, plačujemo račune in urejamo vrsto finančnih obveznosti. Pomembno je le paziti, da storitev opravljamo preko zaščitenih in predvsem znanih spletnih strani, da ne pride do zlorab.

Internet se je marsikateremu uporabniku priljubil prav zaradi svoje diskretnosti. Kdorkoli lahko kadarkoli išče kakršnekoli podatke, ne da bi za to vedel kdo drug. Seveda obstajajo programi, ki beležijo, katere naslove obiskuje posameznik, koliko časa porabi na posameznem strežniku in podobno. To je vidno predvsem pri nakupih preko spleta. Pogosto se zgodi, da uporabnik prek iskalnega mehanizma išče določen izdelek, na primer knjigo s področja politologije, ob tem pa si strežnik, ki posreduje želene podatke, shrani naslov uporabnikovega računalnika in naslednjič, ko želi uporabnik podatke o glasbeni plošči, mu iskalnik, ne glede na to, da uporabnik nikjer in nikomur ni zaupal svojega imena, posreduje tudi podatke o najnovejših politoloških publikacijah.

Ravno diskretnost je vodila tudi policijo, da je preko svojih spletnih strani uvedla tudi pomoč žrtvam kaznivih dejanj in možnost prijave kaznivih dejanj. Spletna stran policije vsebuje del, kjer so navedeni različni opisi z življenjskimi situacijami iz varnostnega področja. Elektronsko naznanilo kaznivega dejanja poteka tako, da državljani izpolnijo že pripravljen spletni obrazec za naznanilo kaznivega dejanja in ga oddajo na operativno-komunikacijski center policije (OKC). Policija po prejemu naznanila na OKC naznanitelja

posebej obvesti, da je bila njegova vloga sprejeta. Žrtve kaznivih dejanj se kaznivo dejanje pogosto bojijo prijaviti. Bojijo se groženj in različnih vplivanj, že sama prijava pa jim nudi nekakšno jamstvo, da se bo njihova težava nekako uredila. Na žalost slovenska kazenska zakonodaja še ne nudi možnosti, da v nadaljevanju žrtve kaznivega dejanja ne bi soočili s storilcem.

Na spletni strani policije je posebna rubrika, namenjena oškodovancem in žrtvam kaznivih dejanj. Državljani dobijo nasvete, kako se ubraniti različnih kaznivih dejanj, kako spoznajo, da so različna vedenja do njih kazniva dejanja, in kako primer prijavijo policiji. Življenjski dogodki so bili izbrani glede na število posameznih primerov v Sloveniji in na to, da so to kazniva dejanja, ki pogosto ostajajo neprijavljena, ali dejanja, ki lahko potencialno ogrozijo državljane. Tako se lahko dobi informacije in nasvete o:

- nasilju,
- spolni zlorabi oseb,
- terorizmu,
- tihotapstvu,
- spolnem nadlegovanju in
- trgovini z ljudmi.

Tudi Policija se zaveda, da razvoj informacijske tehnologije in interneta kot svetovnega spleta omogoča popolnoma nova razmišljanja in nov pristop k organizaciji dela in s tem približanje svojega dela državljanom.

5.1.1 WIKILEAKS, DRUGAČEN POGLED NA INTERNET – RESNICA ALI POGUBA

Konec marca 2010 je avstralski državljan Julian Paul Assange na Islandiji najel manjšo hišo. Lastniku je povedal, da bo s skupino novinarjev pripravil dokumentarec o bruhajočem vulkanu. V resnici je Julian Paul Assange s sodelavci pripravil spletno objavo polurnega video posnetka ubijanja ljudi v Iraku, ki so ga zagrešili ameriški vojaki. Video posnetek je posnel ameriški vojaški helikopter. Posnetek so na neizsledljivih računalnikih gostili hekerski somišljeniki Assanga po vsem svetu, ki so z zapletenimi tehničnimi triki

poskrbeli, da ameriška vlada po objavi ne bi mogla preprečiti dostopa do spornega videa, če ne bi ravno izključila svetovnega spleta. Vsa elektronska komunikacija med udeleženci je bila skrbno šifrirana, uporaba osebnih imen ni bila dovoljena niti v zasebnih pogovorih, imena vira zaupnega helikopterskega video posnetka pa zaradi lastne varnosti domnevno ni poznal niti sam Assange (Kučić 2010).

Objava video posnetka o zločinih v Iraku je bil le začetek dela WikiLeaksa. Sledili so Afganistanski vojni dnevniki, Iraški vojni dnevniki in objava 250.000 dokumentov iz ameriške diplomatske komunikacijske mreže. Objavljeni dokumenti razkrivajo komunikacijo med ambasadami in konzulati ZDA ter State Departmentom v Washingtonu.

Afganistanski vojni dnevniki

Afganistanski vojni dnevniki, serija poročil o vojni v Afganistanu, ki jih je objavil Guardian, temeljijo na ameriških, internih vojaških dnevnikih o konfliktu, ki se je odvijal med januarjem 2004 in decembrom 2009. Material, s strani ZDA večinoma označen kot tajni, so pridobili »whistleblooevrs[10]« internetne strani WikiLeaks, ki so tudi objavili celoten arhiv. Guardianu, skupaj z New York Timesom in nemškim dnevnikom Der Spiegel je bil omogočen dostop do dnevnikov pred njihovo objavo, zaradi potrditve avtentičnosti in ocene pomembnosti (Leigh 2010).

Ekipa preiskovalnih novinarjev, specialistov za to regijo in strokovnjakov za podatkovne baze, je več tednov preiskovala podatke za zadeve javnega interesa. Potem ko so prepoznali pomen več kot 400 okrajšav in vojaških kratic, so bili pripravljeni potrditi verodostojnost dnevnikov, tako da so jih primerjali z drugimi zapisi in navzkrižno primerjali z drugimi viri. Tako so lahko izločili nekatera bolj grozljiva obveščevalna poročila kot neutemeljena in ugotovili, da so nekateri deli koalicijskega poročanja o civilnih žrtvah nezanesljivi.

[10] Whistleblooevrs, slovensko žvižgači: termin, ki se uporablja za poimenovanje tistega, ki ugotovi napako – ko ugotovi napako, požvižga.

Toda če vse skupaj povzamemo, dnevniki zagotavljajo odkrito in pomembno sliko o tem, kako je vojna potekala: stopnjevanje konflikta; šibkost večine koalicijskih obveščevalnih struktur; vrzel med olepšano verzijo vojne za javnost in kaotična realnost, s katero so se soočali poveljniki na terenu. To je po eni strani surova, neposredna verzija konflikta, kot se je zgodil (Leigh 2010).

Kljub temu da je bil material označen z relativno nizko stopnjo tajnosti, je Guardian poskrbel, da ni objavil informacij, s pomočjo katerih bi bilo mogoče identificirati vire podatkov, neznane tehnike zbiranja obveščevalnih podatkov ali ogroziti koalicijske sile. Iz tega razloga niso omogočili dostopa do celotne zbirke. Namesto tega so objavili izbor dnevnikov, ki se nanašajo na pomembne dogodke, objavljene v časopisih in na internetu. Internetna stran je za lažje branje opremljena s slovarčkom.

Guardian, New York Times in Der Spiegel so se strinjali, da objavijo poročila simultano, sočasno z WikiLeaksovo objavo celotne zbirke podatkov na njihovi internetni strani. Guardian ni seznanjen z originalnim virom podatkov (Leigh 2010).

Iraški vojni dnevniki

Današnji velikanski odliv podatkov iz te dolgo trajajoče bitke, 391.832 tajnih terenskih poročil ameriške vojske, podrobnosti neolepšane in pogosto neznane realnosti vojne v Iraku. To je zgodovina v grobem. Zgodba, ki jo ti dokumenti pripovedujejo, je grda in pogosto šokantna.

Med leti 2004 in 2009 se je vojna med civilnimi sektami zlila z vojno "odpora" nacionalističnih Iračanov in z brezobzirno džihadistično kampanjo tujih podpornikov Al-Kaide, kar je Irak pahnilo v trismerno krvavo kopel obcestnih bomb, ubojev in zelo eksplozivnega granatiranja (obstreljevanja) vasi in mest.

Iraški dnevniki podrobno prikazujejo, kako so vojaki, civilisti, tuji prostovoljci, zasebni pogodbeniki, stari možje in mlada dekleta, Američani, Britanci, Arabci in predvsem Iračani sami, postali žrtve nove dinamike »asimetričnega vojskovanja«, v katerem so gverilci, oboroženi pretežno z improviziranimi pohodnimi minami, tekmovali z osupljivo, visokotehnološko orožarno ameriških zračnih sil (Leigh 2010).

Več kot 100.000 ljudi je umrlo in cela mesta, kot je Faludža, so bila skoraj spremenjena v ruševine, v času obtožb brutalnih zlorab nekaterih ameriških in britanskih vojakov v zaporu Abu Grajb in drugje.

Surovi material teh iraških vojaških dnevnikov, podobno kot podatkovne banke predhodno tajnih dokumentov, ki jih je Guardian objavil o vojni v Afganistanu, izvira iz ameriških vojaških arhivov. Bivši ameriški obveščevalni analitik Bradley Manning, ki je bil pred tem razporejen v Bagdad, se trenutno sooča s sojenjem zaradi odtekanja tovrstnih dokumentov k WikiLeaksu, internetnim žvižgačem (Leigh 2010).

Ameriške diplomatske depeše

1,6 gigabajta besedila na spominskem ključku pomeni več kot 250.000 depeš zunanjega ministrstva, poslanih z ameriških ambasad ali pa na ameriške ambasade po svetu.

Kar se je pojavilo po objavi, je prvič videna slika skrivne diplomacije, kot jo izvaja edina svetovna supersila. To je v celoti 251.287 depeš iz več kot 250 ameriških ambasad in konzulatov. Odkrivajo ameriški način dela tako z zavezniki kot sovražniki – pogajanja, pritiski in včasih osorno klevetanje tujih voditeljev, vse to za požarnimi zidovi šifer in označevanja tajnosti, za katere diplomati domnevajo, da zagotavljajo varnost. Odkriti dokumenti imajo oznake vse do stopnje SECRET NOFORN, kar pomeni, da naj bi jih nikoli ne pokazali nekomu, ki ni državljan ZDA. Guardian bo objavil izvlečke originalnih dokumentov, če s tem ne bo ogrožal posameznikov (Leigh 2010).

Poleg klasičnih političnih analiz nekatere depeše vsebujejo podrobne opise korupcije v tujih režimih, pa tudi obveščevalne podatke o pošiljkah orožja, trgovini z ljudmi in prizadevanjih za odpravo sankcij držav, ki želijo proizvajati jedrsko energijo, kot sta Libija in Iran. Nekatere temeljijo na intervjujih z lokalnimi viri, medtem ko so ostale večinoma splošni vtisi in kratka dejstva, napisani za vodilne obiskovalce z zunanjega ministrstva, ki niso seznanjeni z lokalnimi razmerami. Guardian bo objavil izvlečke originalnih dokumentov, če s tem ne bo ogrožal posameznikov (Leigh 2010).

Ker so namenjene v branje uradnikom v Washingtonu, vse do ravni državnega sekretarja, so depeše večinoma napisane s strani ambasadorja oziroma njegovih pomočnikov. Kljub temu da so depeše pogosto presenetljive in problematične, pa ne bodo podprle teorij zarote. Ne vsebujejo dokazov o načrtovanih atentatih, podkupninah CIE ali podobnih kriminalnih podvigih, kot je bil škandal Iran-Contra v Reaganovih letih, ko so tajno financirali gverilo v Nikaragvi. Guardian bo objavil izvlečke originalnih dokumentov, če s tem ne bo ogrožal posameznikov (Leigh 2010).

WikiLeaks kljubuje Pentagonu s posredovanjem teh podatkov več medijem, vključno z Guardianom. Prav tako WikiLeaks namerava večino podatkov objaviti na njihovi internetni strani. Guardian bo objavil izvlečke originalnih dokumentov, če s tem ne bo ogrožal posameznikov.

Assange je ustanovitelj organizacije WikiLeaks, katere glavna naloga je razkrivati krivice in razvijati novo obliko »znanstvenega novinarstva«, ki bo temeljila na analizi »necenzuriranih in neobdelanih podatkov«. Prizadeva si za popolno svobodo vseh informacij – brez cenzure, uredniških odločitev in medijskih posrednikov. To, da je način pridobivanja informacij sporen, gibanja WikiLeaks ne moti. Vojak Bradley Manning, ki naj bi Assangu predal diplomatske depeše, je bil kmalu prijet in se trenutno nahaja v zaporu. Zaradi izdaje državne skrivnosti mu grozi celo kazen do 50 let zapora (Kučić 2010).

Evgenij Mozorov (v Paolo Alto 2010) meni, da WikiLeaks in z njim Julian Assange stopa na čelo novega političnega gibanja, ki bo temeljilo na načelu absolutne spletne svobode, preglednosti, ohlapnih zakonov o avtorskih pravicah in podobnem. To gibanje se poraja že po vsem svetu, predvsem pa v Evropi. Prav mogoče je, da bo lov na WikiLeaks pripomogel k še radikalnejšemu razmišljanju mladih ljudi in jih spodbudil, da se bodo pridružili boju za svobodo medmrežja, kot si ga razlagajo sami. Tako bi postali nekakšna digitalna ustreznica zelenemu gibanju v Evropi. Druga možnost je veliko manj privlačna. Če bodo oblasti do Assanga stroge in mu bodo zaradi objav depeš sodili in ga obtožili terorizma, se gibanje utegne izroditi v nasilno obliko upora. Glede na to, da je veliko pripadnikov gibanja računalniško pismenih in da je čedalje večji del naše javne

infrastrukture digitaliziran, bi morebitni hekerski napadi gibanja pomenili hudo oviro za svetovno gospodarstvo.

Ko je podjetje za poslovanje s kreditnimi karticami Mastercard blokiralo donacije WikiLeaksu, je skupina hekerjev takoj izvedla spletni napad na njihovo spletno stran. Računalniški aktivisti pod imenom "anonimneži" so zagrozili s hekerskimi napadi tudi na druga podjetja, ki bodo kakorkoli blokirala nakazila sredstev WikiLeaksu.

6 EKSTREMISTIČNE IDEJE NA INTERNETU

V sodobni družbi, ki jo med drugim opredeljuje porast različnih komunikacij in razvoj novih (informacijskih) tehnologij – tako za izmenjavo informacij kot za raznovrstne oblike prikritega nadzora – pomeni ustrezno varstvo komunikacijske zasebnosti in osebnih podatkov toliko in še več, kot sta pred desetletji in stoletji pomenila nedotakljivost stanovanja in prepoved arbitrarnih odvzemov prostosti. Že leta 1928 je znameniti sodnik Vrhovnega sodišča ZDA, Lois Brandeis, v najbrž prvem sodno dokumentiranem primeru telefonskega prisluškovanja na svetu v svojem, ločenem mnenju preroško zapisal: "Napredek znanosti, ki državi omogoča nove možnosti vohunjenja, se ne bo ustavil pri prisluškovanju telefona. Nekega dne bo razvoj znanosti omogočil reproduciranje papirjev, ne da bi jih dejansko fizično vzeli iz obdolženčevega predala, in bodo tako lahko sodišču razkrite najbolj intimne informacije iz njegove zasebnosti« (Klemenčič 2007, 1).

Internet za ekstremistične skupine pomeni medij širjenja ideološkega in političnega ekstremizma, ki ga zagovarjajo. Internet postaja za te skupine najpomembnejši prostor komunikacije in diskusij. Poleg širjenja ideologij se ekstremistične skupine poslužujejo interneta tudi za napadanje in motenje računalnikov, ki upravljajo omrežja kritične infrastrukture in omrežja gospodarskih družb, kot so denimo banke ali spletne strani, ki omogočajo dostop do spletnih storitev.

Ekstremistične skupine potrebujejo medije, zaradi hitrosti širjenja informacij je zanje najpriročnejši ravno internet, s pomočjo katerega najhitreje širijo svoje ideje. S klasičnimi napadi jim mediji zagotovijo pozornost, z informacijami, ki jih objavijo na svojih spletnih straneh, pa pridobijo zanimanje širše javnosti. Internet je poceni, hiter, lahko dostopen in ima svetovni doseg. Vse to so prednosti, ki ga naredijo tako privlačnega in zaradi česar ga cenijo tudi navadni ljudje, ki spoštujejo zakone in jim internet koristi v vsakodnevnem življenju, na žalost pa ga izkoriščajo tudi pripadniki ekstremističnih gibanj, ki odlično razumejo, kakšne možnosti ta ponuja kot orodje za širjenje propagande, usmerjene v mobilizacijo in novačenje, ter za zagotavljanje navodil in priročnikov, ki so namenjeni usposabljanju ali načrtovanju napadov z izredno majhnim tveganjem in stroški.

Najpogostejše in najbolj znane storitve, ki jih ponuja internet in ki jih uporabljajo tudi storilci kaznivih dejanj, so (Europol 2003, 21):

- elektronska pošta,
- uporaba spletnih strani www (World Wide web) in http (Hypertext Transfer protocol),
- storitev FTP (File Transfer Protocol), ki je namenjena izmenjavi podatkov oziroma datotek,
- spletne klepetalnice (IRC – internet relay Chat), ki omogočajo komunikacije oziroma izmenjavo sporočil v realnem času,
- storitev P2P (Peer-to-peer), ki omogoča hitro in zanesljivo izmenjavo datotek; predvsem gre za izmenjavo velikih datotek, kot so filmi, igre, programi ipd.,
- novičarske skupine (Newsgroups), pri katerih gre za različne internetne forume, na katerih potekajo razprave med uporabniki teh forumov, ki so razdeljeni glede na temo, ki jo pokrivajo,
- telnet, to je servis, ki omogoča povezavo z oddaljenimi računalniki in njihovo uporabo,
- storitev VOIP (Voice over Internet protocol), ki omogoča uporabo interneta za prenos govora, saj glas ali video razdeli v podatkovne pakete, ki jih nato z internetnim protokolom prenaša med uporabniki.

6.1 TERORIZEM

Internet uporabljajo praktično vse teroristične skupine, ker jim predstavlja obliko komunikacije. Predvsem gre za propagando, uporabo svetovnega spleta za promoviranje svojih idej in svoje resnice. Islamske ekstremistične skupine ga uporabljajo za širjenje »proti zahodni« in proti izraelski propagandi. Več spletnih strani, ki so jih ustanovili pristaši Hamasa, objavlja politična in vojaška sporočila, v katerih odkrito zahtevajo umore Judov in drugih zahodnjakov.

Druge radikalne islamistične spletne strani, kot denimo Hizb-Tahrir, radikalna islamistična organizacija s sedežem v Veliki Britaniji, uporablja svojo spletno stran za seznanjanje javnosti o rednih sestankih članov skupine. Nekatere druge skupine internet

uporabljajo za zbiranje sredstev, Hezbolah ga uporablja za prodajo knjig in publikacij. Nekateri izraelski in ameriški uradniki menijo, da teroristi iz Hamasa in Islamskega džihada internet uporabljajo za prenašanje navodil teroristom, vključno z zemljevidi, fotografijami in tehničnimi podrobnostmi o tem, kako se uporablja eksplozive.

Osama Bin Laden in njegova islamistična teroristična mreža so ustvarili prefinjeno medijsko kampanjo, ki se kaže predvsem v seriji faksiranih sporočil, avdio posnetkov, video posnetkov in internetnih objav. Teroristični analitiki verjamejo, da so bila sporočila oblikovana z namenom izzvati psihološke reakcije pri širši javnosti. Bin Laden je poudaril pomembnost mednarodnih in domačih medijev za delovanje Al Kaide. Ustanovili so tudi poseben komite (medijskokomunikacijski komite), katerega naloga je predvsem pošiljati sporočila in izjave, ki podpirajo teroristične operacije islamistov. Največji učinek imajo objavljeni posnetki Bin Ladna, v katerih širi idejo Islamskega džihada in izraža politične zahteve. Po terorističnih napadih na ZDA leta 2001 je izdal ogromno javnih sporočil in se v očeh javnosti prikazal predvsem kot strateški vodja, ki za svoja nasilna dejanja izkorišča specifične politične razmere (Blanchard 2004).

Spletne strani z radikalnimi islamističnimi vsebinami pogosto menjajo spletne naslove, vsebina strani pa praviloma ostaja ista. Spletne strani radikalnih islamističnih skupin lahko razvrstimo po več kriterijih:

- strani, ki vsebujejo elemente psihološke vojne – zastraševanja prebivalcev zahodnih držav;
- propagandne strani – poveličevanje boja proti Zahodu;
- zbiranje informacij – nekatere spletne strani so namenjene zbiranju informacij in idej (zaznali so stran, ki je zbirala podatke o ambasadah ZDA po Evropi);
- iskanje somišljenikov – strani s širjenjem različnih idej;
- rekrutiranje – predvsem iskanje kandidatov za džihad;
- informativne strani – teh je veliko in vsebujejo podatke o izdelavi različnih eksplozivnih naprav, podatke o orožju, navodila za streljanje;
- strani o različnih načrtovanjih – predvsem grožnje, kaj se lahko zgodi, če Zahod ne bo prenehal gonje proti muslimanom (Gelbart 2007).

Do zdaj niso našli spletne strani, ki bi konkretno napovedovala določen napad in bi se ta tudi zgodil. Veliko je različnih groženj, ki pa so po večini presplošne, da bi lahko točno določili objekt napada. Predstavljajo veliko sovraštvo proti zahodnemu sistemu, predvsem ZDA in državam, ki sodelujejo v koaliciji v Iraku in Afganistanu. Veliko spletnih strani zelo natančno in sproti spremlja vojno v Iraku, predvsem prikazujejo zločine proti Iračanom.

Med terorizmom in spletnim okoljem obstajata dve temeljni povezavi. Spletno okolje postaja vse bolj primarno komunikacijsko okolje, v katerem oz. preko katerega si teroristi, logisti, simpatizerji idr. vpleteni zagotavljajo[11]:

- komunikacijo,
- načrtovanje napadov,
- pripravljalna dejanja.

Na spletnih straneh terorističnih organizacij običajno najdemo podatke o zgodovini organizacije, dejavnosti, bibliografije voditeljev, ustanoviteljev in junakov, informacije o političnih in ideoloških ciljih, dnevne novice, kritiko sovražnikov ipd. Glede na vsebino terorističnih spletnih strani je občinstvo lahko trojno: trenutni in potencialni privrženci, mednarodno javno mnenje in nasprotnikova oziroma sovražna publika (Weimann 2004).

Zaradi poplave terorističnih video posnetkov na svetovnem spletu, lahko te kategoriziramo na naslednje načine (Žibert 2007, 81):

- **Propagandni video**

  Tipični propagandni teroristični video posnetki največkrat prikazujejo pomembne teroristične akterje, kot so npr. Osama Bin Laden, Zawahiri, Abu Musab Al Zarkavi. Zelo popularni so tudi posnetki napada na svetovni trgovinski center v New Yorku ter

[11] Namestnik direktorja FBI Keith Lourdeau (2004) je dejal, da teroristične skupine z neverjetnim stopnjevanjem izrabljajo možnosti, ki se ponujajo z razvojem IT-tehnologije in kibernetskega prostora. Teroristi uporabljajo tovrstno tehnologijo za načrtovanje, rekrutiranje, propagando, vzpostavitev medsebojne komunikacije, nadzorovanje akcij ipd.

mučenje iraških zapornikov, ki so ga izvajali ameriški vojaki. Glavni cilj objave teh včasih zelo krutih posnetkov je prikazati sovražnike islama v najslabši možni luči, torej tako, kot jih vidijo teroristi.

- **Mučeništvo**

  Takšen primer so poslovilni govori samomorilskih napadalcev v digitalnem zapisu, ki jih posnamejo tik pred napadom. S tem širši javnosti prikažejo svoje občutke ter motivacijo, ki jih vodi v samomorilski napad. Eden izmed bolj znanih mučeniških posnetkov predstavlja video Ahmeda Al-Hazwania, enega izmed ugrabiteljev letala, ki je strmoglavilo na svetovni trgovinski center v New Yorku. Na video posnetku je med drugim tudi zagrozil ameriškemu narodu, da jih bo napadel v njihovi lastni domovini in jih pozval h končanju poniževanja ter podjarmljanja muslimanov.

- **Posnetki usmrtitve talcev**

  Nobeni video zapisi niso imeli tako velikega vpliva na javnost kot prav posnetki usmrtitve talcev. Na omenjenih posnetkih je v ospredju predvsem kruta, hladnokrvna ter izjemno grozljiva narava pripadnikov terorističnih organizacij in odkrita sovražnost do zahodnih držav. Grozljivi način usmrtitve talcev je spremljala popolna nemoč javnosti in držav. Teroristi so odziv smatrali za velik uspeh in kmalu se je v medijih pojavilo še veliko podobnih posnetkov.

Islamistični teroristi na video posnetkih, objavljenih na svetovnem spletu, najpogosteje poudarjajo sveto vojno (džihad) ter maščevanje vsem nasprotnikom islama. Zahtevajo, da se iz Iraka in Afganistana umaknejo vse okupatorske sile in prepustijo vladanje ekstremističnim skupinam.

Svetovni splet ima čedalje večjo vlogo v našem vsakdanjem življenju. Uporabljamo ga za komuniciranje, trgovanje in izmenjavo podatkov; nenehno se veča naša odvisnost in vzporedno tudi občutek nebogljenosti in izgubljenosti v tem ogromnem sistemu. V ZDA pa se je v zadnjih nekaj letih v medijih, filmih, znanstvenih in drugačnih razpravah ter v zakonodaji pojavil pojem kibernetski terorizem. Pri tem so ključna vprašanja, ali kibernetski terorizem sploh obstaja; ali res obstaja grožnja napadov preko interneta, ki

lahko ogrozijo življenja, in kako se obvarovati pred njimi. Glede na strokovne definicije pojma lahko rečemo, da se dogodek takšne razsežnosti do zdaj še ni zgodil. Tudi možnosti takšnega napada so omejene, če pomislimo, da računalniški sistemi po večini ne delajo sami po sebi, vedno je nekje vpleten človeški faktor. Ali je torej kibernetski terorizem pojem, katerega realizacija je imanentna, ali je le teoretični konstrukt (Založnik 2007, 2)?.

V današnjem času množičnih medijev je tudi za separatistične skupine komunikacija postala preprosta in učinkovita. Odločilni komponenti za uspešno sporazumevanje sta učinkovitost in pravočasna objava določenega sporočila. Sporočilo mora biti v razumljivi obliki, tako da je dostopno čim večjemu številu širše javnosti. Prav tako mora biti podano ob natančno določenem času, da ima na javnost čim večji vpliv (Martin 2003, 279).

Teroristična skupina ETA[12] za širjenje svojih idej uporablja vrsto medijev. Značilnost baskovskih separatistov je izrazita manipulacija z mediji, z namenom, da bi čim bolj opozorili nase. Pred napadi vedno obvestijo javnost, teroristične operacije ponavadi izvedejo takrat, ko so prepričani, da bodo dobili popolno medijsko pozornost in da njihovega napada ne bo zasenčil noben drug aktualni dogodek (Cralley in Garfield 2004, 127). Podporniki nacionalistov oblikujejo tudi spletne strani, na katerih so objavljene najnovejše novice v zvezi z bojem za neodvisnost. Računalniška tehnologija je naredila množično komuniciranje bolj preprosto in dostopno vsem, ki želijo izvedeti kaj več o baskovski kulturi. Uporaba svetovnega spleta kot sredstva za izražanje politične volje je izredno popularna, vendar ima lahko tudi negativne učinke. Leta 1997 so baskovski separatisti usmrtili mladega mestnega svetnika Miguela Blanca. Na spletnih straneh časopisov Euskal Herrira Journal in Egin se je vnela goreča razprava. Zaradi prevelikega števila elektronske pošte sta bili obe spletni strani kmalu zatem začasno ukinjeni, kar je povzročilo velik odziv španske javnosti in medijev. To je tudi eden izmed razlogov, da je večina novih baskovskih internetnih strani namenjenih širjenju nenasilja in podpori miru v Baskiji (Linstroth 2002, 10).

[12] ETA – Euskadi Ta Askatasuma (Baskovska dežela in svoboda). Imenujejo se "revolucionarno baskovsko gibanje za narodno osvoboditev". ETA za izpolnitev svojih ciljev – pravica do politične neodvisnosti – kljub temu da je separatistična organizacija, uporablja teroristične metode.

Ena izmed glavnih tarč baskovskih separatistov so tudi novinarji, predvsem tisti, ki nasprotujejo ETI in svoja politična prepričanja tudi javno izražajo. Baskovski separatisti uboje novinarjev opravičujejo s tem, da jih obsodijo centralizma in brezpogojne lojalnosti španskim oblastem. ETA se načeloma ne pojavlja na televiziji. Za svojo propagando skrbi preko amaterskih posnetkov, ki jih objavlja na svetovnem spletu in so dostopni širši množici. Najpomembnejši spletni časopis, ki podpira ETO, je Online Euskal Herria Journal[13]. Druga najbolj obiskana spletna stran je Basque Red Net[14], ki so jo ustanovili baskovski nacionalisti, ekologi in skupina feministk (Knight in Ubayasiri 2005, 8).

Tudi čečenske ekstremistične skupine za objavo svojih sporočil uporabljajo svetovni splet. Vodja čečenskih upornikov Doku Umarov je po terorističnih napadih na postajah moskovske podzemne železnice Lubjanka in Park Kulturi, prevzel odgovornost za napad. Na videoposnetku, objavljenem na spletni strani čečenskih upornikov KavkazCenter[15], je dejal, da je napad naročil ravno on. Dodal je, da so se uporniki z napadoma maščevali za smrt ubogih čečenskih in ingušetskih civilistov, ki so jih februarja ubile ruske varnostne sile. Umarov je poleg tega še napovedal, da se bodo napadi na ruski zemlji nadaljevali. »*Vojna bo prišla na vaše ulice ... in občutili jo boste na lastni koži,*« je posvaril ruske državljane (http://m.24ur.com/bin/mobile/index.php?article_id=3253616).

Že pred njim se je spletnih strani posluževal tudi nekdanji voditelj čečenskih upornikov Abdallah Shamil Basajev. V sporočilu, objavljenem po zajetju talcev v Beslanu, je na spletni strani zapisal, da je zajetje talcev odgovor na delovanje ruskih varnostnih sil v Čečeniji. Objavil je tudi, da so zajetje talcev in napad na dve potniški letali izvedli pripadniki skupine Rijadus-Salikhin, ki jim poveljuje.

Teroristična organizacija PKK[16] daje propagandi velik poudarek že od nastanka. Sprva je ustanovila lažna krila, z namenom zavarovati njihovo propagando in operacijske

[13] http://www.ehj-navarre.org
[14] http://www.seprin.com
[15] http:www.kavkazcenter.com
[16] Nekaj spletnih strani, ki podpirajo PKK: http://www.mediatv.com, http://wwwpkk.org,

sposobnosti. Za propagando je skrbelo njeno politično krilo ERNK (Eniya Rizgariya Netewa Kurdistan), ki je manipuliralo in vodilo različne frontalne organizacije, pod pretvezo da so to socio-kulturna združenja. Te institucije so zagotavljale politično, moralno, materialno ter finančno podporo, ki je bila nepogrešljiva za preživetje PKK. Ta ima danes široko mrežo medijske podpore. Deluje televizijska postaja, ki podpira njeno delovanje – Roj TV, s sedežem na Danskem. Roj TV ima tudi svojo spletno stran http://www.roj.tv/ (Dovč 2005).

6.2 DESNI EKSTREMIZEM

Internet vsebuje tudi veliko strani, ki jih urejajo skupine, ki zagovarjajo desni ekstremizem[17]. Uporabljajo jih za promocijo svojih radikalnih idej in programov. Internet je omogočil predvsem sovražno delovanje rasističnih skupin v ZDA. To je povezano z ameriško neomejeno svobodo govora, ki predstavlja idealno okolje za rasistične skupine, kot je Ku Klux Klan. Ker ameriška zakonodaja vsakomur omogoča javno izražanje mnenja, pa naj bo to še tako rasistično, nacionalistično, homofobično ali kako drugače nastrojeno. ZDA predstavljajo ideal demokratične države, po kateri se zgleduje tako rekoč celotni svet, kar je seveda velika ironija. Država, ki preostalemu svetu predstavlja ideal, h kateremu je treba stremeti, obenem predstavlja državo, katere zakonodaja in prepričanja predstavljajo tudi idealno okolje za nastanek sovražnih skupin, ki lahko svobodno širijo svoja prepričanja, ne da bi bile za to kakorkoli kaznovane (Gustainis 2002).

Desne skupine so v Evropi doživele preporod po padcu Berlinskega zidu v devetdesetih letih, ki je sovpadal z družbenimi neenakostmi in vzponom desno-populističnih in neonacističnih gibanj, ki so za poslabšanje ekonomskih razmer krivile povečan pretok migrantov v vse bolj globaliziranem svetu (Revieli v Brand in Hirsch 2004, 372–373). Nastale so organizacije, kot so angleška Blood & Honour, ki ima svoje mreže v mnogih državah, med drugim tudi v Sloveniji, in Nacionalna fronta ter ameriška organizacija

---

http://www.kongra-gel.com, http://www.kongra-gel.net, http://www.kongra-gel.org, http://www.hpg-online.com (spletna stran vojaškega krila Kongra-Gel), http://www.hazenparastine.com, http://www.hpg-online.com, http://www.pkkgercegi.net.

[17] Skupine »Skinhead«, "Supremacist« ali »White Power« ipd.

Hammerskins iz Teksasa, ki poveličuje prevlado bele rase in je močno povezana z ameriškim ruralnim rasističnim in ultrapatriotskim gibanjem Ku Klux Klan.

Desne skupine so privržene Hitlerju, nacionalsocializmu, rasizmu in podobno, tega zunaj svojih krogov ne obešajo na veliki zvon. Člani glasbene zasedbe SkullCrusher, ki s svojimi besedili spodbuja rasno nadvlado bele rase, so v intervjuju za spletno stran britanske Blood & Honour[18] sami še najbolje pojasnili: »Verjamemo, v kar verjamemo, vendar se med seboj strinjamo, da ne omenjamo stvari, kot je »ubijte črnuhe«, direktno. Prepevanje provokativnih in prepovedanih besedil ni način, da bi se približali mladim, pravzaprav bi bil učinek obraten. Ker imamo nacionalsocialistične ideje zapisane »med vrsticami«, lahko nastopamo tudi na drugih festivalih in širimo svoje ideje tudi med druge ljudi« (Valenčič 2010).

6.3 LEVI EKSTREMIZEM

V skupino levega ekstremizma spadajo skupine, ki s svojim delom združujejo mrežo družbenih gibanj, pogosto združenih pod imenom protiglobalizacijsko gibanje, gibanja za globalno pravičnost ipd. Značilnost gibanj je dajanje prednosti produciranju alternativ, za razliko od tradicionalnih načinov in nestrinjanja in reševanja konfliktov z vladajočimi silami družbe (Day 2005). Po Graeberju anarhizem leži v središču sodobnega protiglobalizacijskega gibanja kot praksa, ki daje prednost direktni akciji, torej neposredni konfrontaciji z vladajočimi silami onkraj uveljavljenih, reprezentativnih političnih kanalov (Graeber 2002).
Nova družbena gibanja so izrazito računalniško podprta in temeljijo na »komunikacijskem internacionalizmu«. Informacijo smatrajo kot kolektivno lastnino, spletne medije pa kot avtonomen in odprt prostor produciranja in prejemanja informacij. Digitalna tehnologija je postala eksperimentalni prostor, v katerem se neposredno gradijo in uveljavljajo načela alternativne družbe (Waterman 1998).

Ena od spletnih strani, ki se pogosto povezuje z gibanji radikalne levice, je Indimedia[19]. Nejn slogan »postani medij« odraža idejo da informacij in medijske mreže Indymedie ne

[18] http://www.bloodandhonourworldwide.co.uk/
[19] http://www.indymedia.or.uk

krojijo profesionalni novinarji, odtujeni od dejanskega dogajanja in zavezani interesom korporativnih medijev, temveč aktivisti, ki so neposredno udeleženi v dogajanju. Aktivisti imajo več nadzora nad medijsko produkcijo in hitrostjo pretoka informacij (Juris 2005, 201). Indymedia je odigrala ključno vlogo pri zbiranju protestnikov na političnem srečanju voditeljev držav članic G20, ki je potekalo leta 2009 v Londonu. Na svoji spletni strani so objavljali datume in kraj zbiranja, čas prihoda in čas selitve na druge lokacije in o splošnem policijskem nasilju.

Tudi nemiri priseljencev in delavcev socialnega dna v Parizu leta 2005 so bili koordinirani s pomočjo mobilnih telefonov in interneta. Najbolj učinkoviti so bili internetni blogi, preko katerih so demonstranti, predvsem najstniki iz vse Francije med seboj tekmovali v številu požganih avtomobilov in stopnji sovražnega govora. Za komunikacijo so uporabljali bloge na radijski postaji Skyrock[20] (Tonnevold 2009).

Uradno spletno stran ima tudi sicer v zadnjem času neaktivna italijanska teroristična organizacija Rdeče brigade[21]. Prednost uporabe interneta vidijo v možnosti anonimno izraziti najbolj radikalne, nasilne ali uničujoče ideološke teorije ter hitro pridobivati privržence. Za komunikacijo s pripadniki skupine, ki so na begu ali v tujini so uporabljali spletno stran svojega časopisa »La Voce« (Ceresa 2005).

Ena izmed vidnih dejavnosti aktivistov levega ekstremizma se je zgodila v Mehiki. Februarja 1996 so po ofenzivi mehiške vojske proti zapatistični vstaji v mehiški državi Chiapas aktivisti zasedli spletno mesto mehiške vlade in upočasnili delovanje spletnega mesta. Uporabili so metodo napadov DoS, pri čemer je množica aktivistov ob istem času obiskala spletno mesto mehiške vlade (Medosch 2002).

6.4 SOVRAŽNI GOVOR

Sovražni govor na internetu je močnejše orodje za spodbujanje nestrpnosti kot v tradicionalnih medijih, ker se »sovražno spletno stran, ki ponižuje posameznike ali skupine na osnovi rase, veroizpovedi, nacionalne pripadnosti, spolne usmerjenosti ali

[20] http://wwwskyrock.com
[21] http://www.brigaterose.org

invalidnosti, lahko uporabi za spretno trženje zla, ker odjemalcev nikoli ne zmanjka« (Petrovec 2003, 37).

Sovražni govor obstaja že od nekdaj, le da mu je v zadnjih nekaj desetletjih posvečene več pozornosti, javnih obravnav in razprav v širšem družbenem kontekstu. Z naglim razvojem množičnih medijev se je sovražni govor razširil na vsa področja človekovega življenja, saj lahko nestrpne in diskriminatorne izjave zasledimo v vsakodnevnem časopisju, na televiziji, internetu, radiu in tudi v vsakdanjem sporočanju, kjer sami ustvarjamo sovražne izjave ali smo pri tem le pasivni udeleženci. Problem sovražnega govora postaja tudi problem spleta, kjer se pod krinko anonimnosti pojavlja vedno več možnosti za neodgovorno razširjanje sovražnosti in nestrpnosti. Število internetnih uporabnikov iz dneva v dan narašča, internet se popularizira in postaja platforma za konfrontacijo različnih mnenj. Da bi celostno razumeli sovražni govor, se moramo najprej zavedati, da je eno najmočnejših sredstev diskriminacije, še posebno, ker ga težko definiramo in še teže preiskujemo in kaznujemo. Zato je razumevanje in umeščanje sovražnega govora kot sovražnega dejanja izjemno zahtevno, saj gre za dokaj neraziskano področje in je redko predmet znanstvenega interesa. Pozornost na sovražni govor tudi zaradi dostopnosti interneta narašča, predvsem zaradi zavedanja o učinku izgovorjenih diskriminatornih besed (Kovačič 2001, 178).

Pri sovražnem govoru gre najpogosteje za besede, katerih namen je poniževati, razčlovečiti, odvzeti dostojanstvo, postaviti v podrejen položaj, in vplivajo na to, kakšen položaj bodo imele skupine, proti katerim je usmerjen, kako bodo živele, kako bodo z njimi ravnali in, ne nazadnje, kako bodo razumele sebe (Leskovšek 2005, 81). Namen takšnih destruktivnih sporočil je upravičiti neenakosti in ustvariti temelje za ravnanje, ki je v nasprotju z demokratičnimi vrednotami. Sovražni govor krši temeljne ustavne pravice po osebni varnosti pred tiranijo večine in enakem obravnavanju. Cilj sovražnega govora je razčlovečiti, ponižati, prestrašiti, spodbuditi nasilje in druge akcije glede na rasne, etnične, spolne, religiozne, nacionalne ter telesne izvore in značilnosti teh skupin (Walker v Leskovšek 2005, 82).

S sovražnim govorom se v družbi vzpostavlja in ohranja ideologija, s katero sledimo »našim« interesom in prepričanje, da bi »drugi« tem interesom škodovali. Ustvarjajo se družbene prakse o tem, kdo smo, za kaj se zavzemamo, kakšne so naše vrednote, kakšne odnose imamo z ostalimi družbenimi skupinami, zlasti s svojimi sovražniki in nasprotniki. Z razlikovanjem in klasificiranjem ustvarjamo lastno in skupinsko identiteto, iz katere izločimo vse tiste, ki naj vanjo ne bi sodili (Hall v Šabec 2006, 168).

6.5 OTROŠKA PORNOGRAFIJA NA INTERNETU

Ena izmed glavnih zlorab interneta se odraža v širjenju otroške pornografije. Otroška pornografija je v zadnjih letih zelo narasla, predvsem na račun interneta in sodobne tehnologije, vendar je obstajala tudi že prej. Gre za zelo dobičkonosen posel, saj mu razvoj vedno nove in nove tehnologije to omogoča (digitalne kamere, fotoaparati, internet …).

Internet je globalen medij, ki ima veliko prednosti, ki bistveno olajšajo delo pedofilom, ki se ukvarjajo z otroško pornografijo ali katerokoli obliko pornografije nasploh. Njegove prednosti so predvsem hiter prenos podatkov oziroma materiala z otroško pornografijo in, kar je najvažnejše, relativno visoka stopnja varnosti in anonimnosti. Večina ljudi se na internetu počuti varne, saj se ne zavedajo, koliko sledi puščajo za seboj, kar lahko razkrije njihovo zanimanje na internetu (Trček, Kovačič 2001).

Otroška pornografija in z njo povezani posli se vedno bolj odvijajo preko komercialnih (plačanih) internetnih strani; te so zaščitene z gesli ali z vstopom s kreditno kartico. Večina teh strani se nahaja v Rusiji ali v ZDA. Otroška pornografija se med pedofili širi na več načinov. Eden od načinov je preko programov, ki omogočajo izmenjavo datotek, denimo eMule, Bit Torent ipd. Treba je omeniti tudi različne spletne pošte. Pedofili preko spleta ne komunicirajo samo s somišljeniki, temveč si na ta način izbirajo otroke, svoje potencialne žrtve (safe.si).

Internet ustvarja pomembne okoliščine, ki lahko privedejo posameznika, da se začne zanimati za otroško pornografijo. Te okoliščine so (Taylor in Quayle 2003):

- *socialne*: na internetu se ustvarijo virtualne skupnosti za uporabnike otroške pornografije, s katerimi uporabniki opravičujejo svoja dejanja oziroma nagnjenja;
- *individualne*: posamezniki z uporabo interneta dostopajo do gradiva in komunicirajo z ostalimi s pomočjo računalnika, s tem navidezno ustvarijo privatno sfero, kjer izražajo svoje spolne fantazije;
- *tehnološke*: internet in digitalna tehnologija (fotografija, video ipd.) uporabnikom otroške pornografije omogočata, da lahko sčasoma postanejo obsedeni zbiralci in razpečevalci pornografskega materiala. Preko interneta se lahko dogovarjajo za osebna srečanja ter zadovoljevanje in izpolnjevanje svojih spolnih fantazij.

6.6 EKSTREMIZEM NA SLOVENSKIH SPLETNIH STRANEH

V Sloveniji imamo največ izkušenj pri preiskovanju kaznivih dejanj s pomočjo interneta pri obravnavanju kaznivega dejanja po 297. členu KZ-1, tj. javno spodbujanje sovraštva, nasilja ali nestrpnosti. Policija v zadnjih dveh letih beleži povečan obseg suma storitev kaznivih dejanj, povezanih s ksenofobijo ter rasno in versko nestrpnostjo. Še zlasti se je povečal obseg prijavljenih in zaznanih kaznivih dejanj, ki so storjena z uporabo svetovnega spleta, in sicer na način, da posameznik ali skupina preko svojih spletnih strani ali v obliki komentarjev na forumih javno razpihuje versko, rasno nestrpnost ali ksenofobijo. Ugotavljamo, da državna tožilstva dejanj, ki pomenijo javno spodbujanje rasnega in verskega sovraštva, storjenih preko elektronskega spleta, ne preganjajo kot kazniva dejanja po členu 297. KZ-l. Pričakujemo, da se bodo tožilstva odzvala podobno tudi pri drugih kaznivih dejanjih, storjenih s pomočjo interneta.

6.6.1 ISLAMISTIČNI EKSTREMIZEM

V Sloveniji že nekaj časa deluje spletna stran Resnica-Haq[22]. Namenjena je odgovarjanju na vprašanja in razčiščevanju nejasnosti v zvezi z muslimansko vero in privabljanju čim več mladih v islam, med drugim tudi prek ponujanja prevodov nagovorov različnih muslimanskih učenjakov in spreobrnjencev v islam. Spletna stran je zanimiva, ker že površen pregled pove, da so njeni ustvarjalci pripadniki konzervativnejšega islama, zato jih nekateri označujejo za tako imenovane vahabite (Valenčič 2009).

[22] www.resnica-haq.com

Spletnih strani, ki bi širile ekstremistične ideje s področja islamističnega ekstremizma v slovenskem jeziku, ni. Nekaj spletnih strani deluje v bošnjaškem jeziku ali v drugih evropskih jezikih, vendar ni spornih člankov, ki bi se nanašali na Slovenijo. V nekaterih tovrstnih medijih so bili objavljeni članki in nato komentarji v zvezi z odškodninami nekdanjih varčevalcev v Ljubljanski banki, ki po razpadu Jugoslavije niso dobili svojih prihrankov. V zvezi s Slovenijo so bili objavljeni tudi članki in komentarji glede problema t. i. izbrisanih. V nobenem od naštetih primerov ni šlo za komentarje, ki bi pomenili kakršnokoli grožnjo varnosti v Sloveniji.

Ena izmed aktualnih debat o pripadnikih muslimanske veroizpovedi v Evropi je bilo vprašanje nošenja burke v javnosti. Glede na množico člankov po medijih se je na spletnih forumih muslimanske skupnosti v Sloveniji o problematiki pisalo zelo malo. Novice na spletni strani Slovenske muslimanske skupnosti[23] in spletni strani Resnica-haq so bile omejene na hitro povezavo na nekaj člankov v slovenskih medijih. Mnogo več debat o prepovedi burk se je pojavilo na forumih drugih slovenskih medijev, ob novicah o prepovedi burk na Danskem, Belgiji ali Franciji.

V komentarjih so se pojavili dokaj miroljubni komentarji zagovornikov nošenja burk v Sloveniji. Do sovražnega govora ali celo do povračilnih ukrepov zoper vse, ki nasprotujejo nošenju burk, kot se je to zgodilo v Franciji, Danski, Švici, Belgiji, Portugalski in drugih državah, v Sloveniji ni bilo. Pojavili so se komentarji kot denimo »Prepoved nošenja burk v javnosti je samo ena od številnih prepovedi«, »V Evropi se danes zelo grobo posega v življenje muslimanov«, »Nič o muslimanih brez muslimanov«, »Le malokdaj se zgodi, da so muslimani vključeni v kreiranje nacionalnih programov, pravilnikov, zakonov, ki zadevajo njihova življenja« ipd.

6.6.2 DESNI EKSTREMIZEM

V Sloveniji deluje tudi vrsta spletnih strani, ki podpirajo in razpihujejo desne ekstremistične ideje. Ena najbolj znanih je spletna stran slovenske divizije Blood and

[23] http://www.smskupnost.si/

Honour (www.bhslovenia.org), neonacistične skupine, ki zanika obstoj holokavsta, poveličuje belo raso in poziva k uporu proti t. i. židovski zaroti (Jakopič 2005).

Pri nas so za zdaj najbolj aktivne neonacistične spletne strani Blood&Honour[24], Headhunters Domžale[25], Slovenski radikali[26] in rasistični Tu je Slovenija[27] ter Hervardi[28]. Skupini Tu je Slovenija in Blood&Honour posameznike, ki jima nasprotujejo, na svojih spletnih straneh označujeta za »levičarske ekstremiste«. Hkrati pa se že v uvodu omejita od domnevnih napadov neonacistov, za katere menijo, da so zgolj manipulacija (izjava na spletni strani http://www.28slovenia.com/ z dne 10. 1. 2011 in izjava na spletni strani http://www.tu-je.si/?id=1 z dne 9. 8. 2010).

Na spletni strani Blood&Honour se z izjavami za javnost redno odzivajo na članke v drugih časopisih, v katerih jih domnevno blatijo. Odzvali so se na nedavne zapise časopisov Dnevnik in Žurnal, da širijo isto vsebino kot neonacisti. V komentarju na svoji spletni strani so navedbe zanikali, za incidente pa krivijo »narkomane, brezdelneže, alternativce brez alternative, homoseksualce in ostale, ki bogatijo našo družbo«. Blood&Honour tako na svoji spletni strani pojasnjuje: »Res je, da še vedno večino članov predstavljajo »skinheadi,« kar pa ni noben pogoj za samo članstvo v Blood&Honour. Ne delamo razlik med skinheadi, metalci, nogometnimi navijači ...«

Tu je Slovenija in Hervardi medtem pod pretvezo domoljubja širita sovraštvo, v glavnem do priseljencev, muslimanov, Romov, gejev, Afričanov, Hrvatov in seveda »skrajnih levičarjev«. Vse to je razvidno iz pregleda vsebine njihovih spletnih strani in forumov. Zelo dejavni so po srednjih šolah. Propagiranje »ljubezni do domovine« uporabljajo za novačenje novih članov in za poliranje svojega imidža v javnosti, ko s slovenskimi in »karantanskimi« zastavami paradirajo po Ljubljani ob kakem državnem prazniku in podobno. A v osnovi so rasisti in nestrpneži. Omenimo še žolčen protest Hervardov, ki so leta 2006 sprožili celo kampanjo proti univerzitetnemu profesorju mariborske pedagoške fakultete Dragu Roksandiću, ker je predaval v hrvaščini. Hervardi niso upoštevali, da gre

[24] http://www.28slovenia.com/
[25] http://www.headhunters-domzale.com/index.php
[26] http://www.slovenski-radikali.com
[27] http://www.tu-je.si/
[28] http://www.hervardi.com/

za v Evropi zelo cenjenega akademika, niti tega, da je bil na njegovih predavanjih stalno prisoten tudi profesor Andrej Hozjan, ki je študentom pomagal pri morebitnem nerazumevanju določenih terminov. Bolj kot kaj drugega je Hervarde očitno motilo to, da gre za človeka hrvaškega rodu na slovenski univerzi (Valenčič 2010).

Po mnenju Jakopičeve (2005) je najbolj sporna spletna stran slovenske divizije Blood and Honour, neonacistične skupine, ki zanika oziroma relativizira obstoj holokavsta, poveličuje belo raso in poziva k uporu proti t. i. židovski zaroti. Blood and Honour (B&H) je mednarodna neonacistična organizacija s koreninami v angleškem gibanju skinhead, ki se je v drugi polovici 80. let organiziralo okoli glasbene skupine Skrewdriver pod parolo "rock proti komunizmu". Ko je slovenska divizija B&H na medmrežje postavila svojo spletno stran, na kateri je med drugim tudi arhiv tekstov z antisemitsko in rasistično vsebino, katalog prodajnih artiklov in arhiv datotek s posnetki glasbenih skupin, ki poveličujejo belo raso, so se v javnosti oglasile kritike, da gre v tem primeru za očitno kršitev 300. člena Kazenskega zakonika RS, ki prepoveduje izzivanje ali razpihovanje narodnostnega, rasnega, verskega sovraštva, razdora ali nestrpnosti ter širjenje idej o večvrednosti ene rase. Stran, ki je bila do zdaj na mnogih strežnikih, med drugim tudi na strežniku Kluba idrijskih študentov, se je pojavila tudi na Siolovem strežniku. Siol je takoj po prejemu pritožbe in preveritvi dejanskega stanja ukrepal v skladu s splošnimi pogoji, od uporabnika so najprej zahtevali umik sporne strani, ker pa je do določenega roka ni umaknil, je Siol uporabniku onemogočil uporabo njihovih storitev, ki so bile zlorabljene. Stran je tako izginila, vendar se je kmalu spet pojavila v medmrežju. Pojavila se ja na strežniku družbe ZoneEdit s sedežem v New Yorku[29], ki uporabnikom ponuja zakup oziroma prodaja gostovanje na njihovem strežniku, po

[29] Leta 2001 je Svet Evrope pripravil posebno Konvencijo o kibernetski kriminaliteti, ki jo je prvi dan podpisalo kar 26 držav, tudi ZDA, vendar se v končni verziji besedilo konvencije ni ukvarjalo s problemom sovražnega govora. Pozneje, leta 2003, je Svet Evrope državam ponudil v podpis Dodatni protokol h Konvenciji, ki obravnava inkriminacijo rasističnih in ksenofobičnih dejanj, storjenih v računalniških sistemih. Protokol jasno kriminalizira razširjanje rasističnih in ksenofobičnih materialov, groženj ter žalitev, hkrati pa tudi poudarja pomemben princip: internetnim servisom (ISP) odvzemajo odgovornost za kriminalna dejanja, če sicer na svojih internetnih straneh ne izražajo očitnega napeljevanja h kaznivemu dejanju. Še več, internetni servisi niso dolžni aktivno nadzorovati vsebine na svojih straneh. Kritiki takšnih novih ukrepov, ki jih je predlagal Svet Evrope, so takoj opozorili, da bo posledica le prehod "spornih" strani na ameriške strežnike, na katerih bodo skupine oziroma posamezniki lahko brez težav registrirali svoje strani, sovražni govor pa bo seveda ostal.

navedbi nekaterih pa na malezijskem strežniku[30]. Uporabnike je na strani B&H čakalo sporočilo: »Končno je stran spet tu. Naj se SIOL in mediji zavedajo, da smo močnejši, kot si oni predstavljajo, in bomo tudi na internetu imeli svoj prostor. Nikoli nas ne bodo utišali, lahko pa jih je sram, da hočejo nekomu kratiti pravico do izražanja mnenja« (Jakopič 2005).

6.6.3 LEVI EKSTREMIZEM

Opredelitev slovenskih spletnih strani z vsebinami, ki podpirajo levi ekstremizem, ni enostavna. Zajema več skupin, od Greenpeaca, kritičnih intelektualcev, anarhističnega bloka do protiglobalistov, ki so najdejavnejši. Značilnost tovrstnih slovenskih aktivistov je, da se zberejo in začnejo ukrepati ob določenem aktualnem problemu, ki se pojavi v slovenskem prostoru ali svetu. Veliko protestnikov, ki so se udeležili protiglobalističnih protestov v Pragi, Genovi ali Münchnu je bilo aktivno vključenih pri sporu med Slovenskimi železnicami in t. i avtonomno cono Molotov, kasneje pa tudi pri podpori stavkajočim tujim delavcem, ki so izgubili delo v slovenskih gradbenih podjetjih.

V protiglobalistična gibanja lahko uvrstimo skupine, ki so se leta 2001 pridružile novo ustanovljenemu Socialnemu forumu. Poleg posameznikov so se forumu pridružile naslednje skupine: Urad za intervencije[31], Politični laboratorij, Globala[32], KUD Anarhiv[33], KUD Knap[34], Mladi forum, Inštitut za ekologijo, Neodvisni sindikati Slovenije in Civilno združenje za nadzor nad institucijami[35]. Opredeljujejo se kot mreža različnih skupin in posameznikov, ki se zavzemajo za »sožitje za mir med državljankami in državljani

[30] Ko je neka francoska organizacija tožila ameriško internetno podjetje Yahoo!, ker je Francozom omogočalo dostop do nakupa nacističnih "spominkov" na njihovih internetnih dražbah in je torej kršilo francosko zakonodajo, ki prepoveduje nacistično propagando in prodajo nacističnih artefaktov, je francosko sodišče od Yahoo! zahtevalo blokado za francoske državljane. Podjetje je po razsodbi sicer res omejilo in poostrilo pravila na svojih dražbah, na ameriškem sodišču pa dokazalo, da sodba francoskega sodišča ne more veljati za ameriško podjetje. Torej kadar evropske države najdejo sporne vsebine na internetnih straneh, ki gostujejo na ameriških strežnikih, ne morejo pričakovati, da bo ameriško sodišče zahtevalo blokado njihovega dostopa, saj jih varuje prvi amandma (Jakopič 2005).
[31] http://eko.ljudmila.org/
[32] http://www.ljudmila.org/globala/
[33] http://www.ljudmila.org/anarhiv/
[34] http://www.jiga.org/kudknap/
[35] http://www.czni-drustvo.si/

sveta«, nasprotujejo »sistematični uporabi in upravičevanju nasilja, tako terorizmu kot vsakršni vojni in tudi poskusom nepotrebnega uvajanja izrednih razmer«. Zavračajo »težnje po omejevanju človekovih pravic v imenu varnosti«. Večina je prej delovala še pod Uradom za intervencije (UZI), katerega namen »je bil analizirati stanje svobode govoru, svobode javnega delovanja, človekovih pravic in demokracije ter proces krčenja in oženja političnega in kulturnega prostora nasploh.« UZI je nehal obstajati z ustanovitvijo socialnega foruma.

Skupine v okviru socialnega foruma so organizirale nekaj shodov. Eden izmed odmevnejših je bila manifestacija proti ksenofobiji, na kateri so udeleženci izrazili solidarnost s pribežniki, ki so se je udeležili tudi protestniki iz tujine. Protesti so bili organizirani tudi ob srečanju ameriškega in ruskega predsednika na Brdu.

6.6.4 SOVRAŽNI GOVOR

Pri pregledu slovenskih spletnih časopisov, ki vsebujejo tudi forume ali komentarje, že zelo hiter pregled pokaže vrsto sovražnega govora na internetu. Saj so že sami vzdevki posameznikov, ki debatirajo na forumih, zelo pomenljivi: "opre roma", "hitlerjugend", "slo-nacist", "bosanc", "plemeniti" ipd. Na večini forumov se morajo namreč uporabniki, preden pošljejo svoj komentar, s posebnim obrazcem registrirati, vpisati svoj veljavni elektronski naslov in ime, ki ga bodo uporabljali kot udeleženci foruma. Na forumih spletne strani Mladine[36] so obvezno registracijo uvedli prav zaradi sporne kakovosti večine odzivov na članke in novice, ki so jih uporabniki pisali. Kot pravi Jaka Železnikar, urednik spletne strani Mladine, so poleg registracije uvedli tudi pregledovanje in izločanje odzivov, ki so napeljevali k sovraštvu in nestrpnosti ali pa so celo posegali v zasebnost (na primer objave osebnih telefonskih številk, naslovov bivališč s pozivi k fizičnemu obračunu), toda tudi takšni dodatni ukrepi niso veliko pripomogli k dvigu ravni odzivov. Obvezna registracija, ki so jo na forumih Radiotelevizije Slovenija (RTV SLO)[37] uvedli že takoj na začetku, ne more ustaviti t. i. nestrpnežev, poudarja Zvezdan Martič iz Multimedijskega centra RTV SLO, saj si v primeru blokade uporabniki odpirajo nove elektronske naslove in nadaljujejo s sovražnim govorom. Tako kot na forumih RTV tudi

[36] http://www.mladina.si
[37] http://www.rtvslo.si

na forumih Siola[38] za posamezne sklope oziroma rubrike skrbijo moderatorji, ki jih urejajo, po presoji pa tudi brišejo ali režejo objave. Kot poudarja Helena Čerin iz službe za odnose z javnostmi pri Siolu, njihove forume nadzorujejo tudi administratorji, v primeru zlorab pa teme tudi brišejo ali uporabnika opozorijo, kadar pa se neprimerno "obnašanje" na forumih nadaljuje, ga zaklenejo ali pa tudi odklopijo, poleg tega uporabljajo tudi poseben filter "neprimernih" besed (Jakopič 2005).

Da bi komunikacijo na spletu spravili v zakonite okvire, so v organizaciji Spletno oko[39] pozvali urednike spletnih portalov k podpisu kodeksa regulacije sovražnega govora. Novost, ki jo predvideva kodeks, je še gumb »prijavi sovražni govor«, ki nakazuje, da je portal del skupine medijev, ki si prizadevajo za izkoreninjenje sovražnega govora na spletnih portalih. Kodeks je nastal kot odziv na vse več težav, ki jih imajo mediji na spletu zaradi žaljivih in sovražnih komentarjev, zlasti zaradi nejasne definicije sovražnega govora in pomanjkanja sredstev za njegovo preganjanje ter za moderiranje komentarjev.

V Sloveniji deluje kar nekaj nevladnih in vladnih organizacij, še posebej bi izpostavil Mirovni inštitut in Projekt »Spletno oko« ter, ne nazadnje, dejavnost Varuha človekovih pravic, ki budno spremljajo nepravilnosti na internetu in neposredno prijavljajo domnevna kazniva dejanja policiji.

Za prijavo sovražnega govora na internetu je možnih kar nekaj točk. V prvem koraku obravnave prijave pregledovalci določijo, ali je prijavljena vsebina po slovenskih zakonih nezakonita. V primeru, da je vsebina domnevno nezakonita, poskušajo pregledovalci poiskati lokacijo gostitelja obravnave internetne vsebine. Če se strežnik nahaja v Sloveniji, pregledovalci prijavo posredujejo slovenski Policiji, ki nadaljuje s preiskavo. Če se strežnik nahaja v tujini, je prijava domnevno nezakonite vsebine posredovana slovenski Policiji in članici omrežja INHOPE iz tiste države, kjer gostuje strežnik z domnevno nezakonito vsebino. Policija prijavo, ki se nahaja na strežniku v tujini, posreduje Interpolu, partnerska prijavna točka pa začne s postopki v skladu z

[38] http://www.siol.net
[39] Institucija civilne družbe, ki deluje v okviru Centra za varnejši internet Slovenije na Fakulteti za družbene vede.

zakonodajo in prijavnimi postopki v svoji državi (Letno poročilo Centra za varnejši internet 2009).

Tabela 6.1: Število kaznivih dejanj javnega spodbujanja sovraštva, nasilja ali nestrpnosti po 297. členu Kazenskega zakonika in kršitve enakopravnosti po 131. členu Kazenskega zakonika, storjenih v Sloveniji.

ŠTEVILO KD		**Leto**			
Zaključni dokument	**Kaznivo dejanje**	**2007**	**2008**	**2009**	**2010**
OVADBA[40]		**10**	**19**	**9**	**34**
	Javno spodbujanje sovraštva, nasilja ali nestrpnosti	8	13	9	34
	Kršitev enakopravnosti	2	6	0	0
POROČILO[41]		**10**	**9**	**16**	**29**
	Javno spodbujanje sovraštva, nasilja ali nestrpnosti	8	6	7	18
	Kršitev enakopravnosti	2	3	9	11
Skupna vsota		**20**	**28**	**25**	**63**

Dogaja se, da policija uspe pravočasno odkriti storilca in zavarovati dokaze, vendar pa v nadaljevanju tožilstvo ne sledi naporom policije. Največkrat tožilstva v odklonskih ravnanjih ne prepoznavajo vseh znakov kaznivega dejanja, dejanje umeščajo v kontekst trenutnega aktualnega dogajanja, ki povzroča izražanje sovražnega govora, sam dogodek pa označijo kot provokacijo ipd. Tožilstva pogosto ne sledijo ukrepom policije, ki sicer pravočasno odkrije storilca in zavaruje posamezne dokaze. O razlogih za nepregon teh dejanj tožilstvo podrobneje ne seznanja policije. Po mnenju tožilstva so kazenskopravni mehanizmi skrajno sredstvo, ki jih sme družba uporabiti za reševanje svojih problemov, zato se ta aparat sproži šele, ko so izčrpana vsa druga alternativna sredstva. Storilci kaznivih dejanj na internetu so večinoma anonimni, kar oteži postopek.

[40] Določila 148/9. člena ZKP: Na podlagi zbranih obvestil policija sestavi kazensko ovadbo, v kateri navede dokaze, za katere je zvedela pri njihovem zbiranju. V kazensko ovadbo ne vpiše vsebine izjav, ki so jih posamezne osebe dale pri zbiranju obvestil. Kazenski ovadbi priloži tudi predmete, skice, fotografije, priskrbljena poročila, zapise o tem, kaj je ukrenila in storila, uradne zaznamke, izjave in drugo gradivo, ki utegne biti koristno za uspešno izvedbo postopka. Če policija po vložitvi kazenske ovadbe izve za nova dejstva, dokaze ali sledove kaznivega dejanja, mora zbrati potrebna obvestila in poslati o tem državnemu tožilcu poročilo v dopolnitev kazenske ovadbe.

[41] Določila 148/10. člena ZKP: Policija pošlje poročilo državnemu tožilcu tudi v primeru, če na podlagi zbranih obvestil ni podlage za kazensko ovadbo.

Da tožilstvo začne pregon, mora biti namreč identiteta storilca nedvoumno znana. Tožilstvo v nobenem primeru ne more začeti pregona zoper neznanega storilca. Preiskava in s tem pregon primera, pri katerem je storilec neznan ali je storilca težko ugotavljati, kot npr. v primeru pošiljanja komentarjev iz javnega računalnika, sta torej lahko zelo otežena (Ribič 2011).

Eden izmed obravnavanih primerov sovražnega govora v Sloveniji je bila izvršitev kaznivega dejanja javnega spodbujanja sovraštva, nasilja ali nestrpnosti po 1. odstavku 297. člena Kazenskega zakonika. Storilec je z uporabo svojega osebnega računalnika na spletnem forumu objavil sovražni komentar, s katerim je javno spodbujal in razpihoval sovraštvo, razdor in nestrpnost. Pri pregledu internetnih strani spletnega ponudnika družbe SIOL je policist zaznal, da je na spletnem naslovu novic Siola objavljen članek z naslovom: »SDS: Zakaj se izbrisani obravnavajo drugače kot žrtve vojnih zločinov?« Na članek je bilo objavljenih več komentarjev porabnikov internetnih storitev, med njimi je bil zabeležen tudi komentar: »ZBIRAM PRAVE SLOVENCE ZA NAPAD NA UDBOGOLAZN IN KOMUNAJZERJE- TO GAMAT MORAMO POBITI,ČENE BOMO KRUHA LAČNI,JAVLJAJTE SE MI V TRBOVLJE- NEKAJ NAS JE ŽE.« Pri pregledu omenjenega članka in komentarjev so bili ugotovljeni razlogi za sum, da je neznani storilec pod omenjenim vzdevkom »Majmun« z javno objavo komentarja na spletni strani izvršil kaznivo dejanje javnega spodbujanja sovraštva, nasilja ali nestrpnosti po I. odstavku 297. člena KZ-1, saj je javno spodbujal in razpihoval sovraštvo ali nestrpnost, pri čemer je očitno pozival druge državljane k tovrstni dejavnosti. Storilca so dobili, zoper njega je policija na pristojno državno tožilstvo podala kazensko ovadbo.

Drugi primer kaže na dobro sodelovanje policije in nevladne organizacije Spletno oko. Policija je obravnavala osebo, ki je utemeljeno osumljena storitve kaznivega dejanja javnega spodbujanja sovraštva, nasilja ali nestrpnosti po členu 297/I KZ, ker je 21. 6. 2009 na spletnem forumu časopisa Žurnal objavila komentar in s tem javno spodbujala sovraštvo. Kaznivo dejanje je prijavila organizacija Projekt Spletno oko zaradi suma storitve kaznivega dejanja Javnega spodbujanja sovraštva, nasilja in nestrpnosti po členu 297/I KZ-1. Iz prijave je razvidno, da je bil na spletnem naslovu http://www.zurnal24.si/Ves-teden-ponosa/novice/kultura/116694 objavljen članek, ki govori o tednu parade ponosa, ki se je odvijala v Ljubljani. Pod člankom je bil odprt javni

forum, kjer je uporabnik z vzdevkom »patriotPARTIZANslovenec« napisal komentar z naslednjo vsebino »bodte pripravljeni na smrt ali pretep s pestmi če se pojavite v ljubljani na javnem prostoru boste odgnan skrijte se v nek klub in se tam analno posiljujte!! ZA SLOVENIJO PROTI PEDROM!« Storilca so dobili in zoper njega je bila podana kazenska ovadba.

Preiskovanje tovrstnih kaznivih dejanj je zaznamovano z izredno tanko mejo med varovanjem svobode govora in spoštovanjem posameznikove zasebnosti na eni strani ter zagotavljanjem varnosti na drugi strani. Poleg tega so tako cilj napada kot tudi storilci največkrat izredno ranljivi predstavniki manjšinskih skupin (Ribič 2011).

Dodatno težavo preiskovanja sovražnega govora na internetu predstavljajo tudi tehnične omejitve, kot so zavarovanje elektronske komunikacije v različnih spletnih servisih in socialnih forumih (Facebook, Yahoo ipd.), kjer je treba za zavarovanje uporabiti inštitut mednarodne pravne pomoči, kar pa se lahko izvede šele, ko policija zbere dovolj dokazov, ki omogočajo podajo kazenske ovadbe. Poleg tega nekateri ponudniki ne hranijo vsebin oziroma zgodovine komunikacije, zaradi česar je pravočasnost ukrepanja bistvenega pomena (Ribič 2011).

Določeno odgovornost pri objavi sovražnega govora na internetu, predvsem v obliki komentarjev pod članki, ima tudi urednik oz. namestnik urednika, če je bilo kaznivo dejanje storjeno s sredstvi javnega obveščanja. Problem se pojavi, ker ni jasno, ali spletni portal spada pod sredstvo javnega obveščanja. To bo pokazala sodna praksa. Na poziv so portali dolžni umakniti komentar, ki vsebuje elemente sovražnega govora, in sicer nemudoma, kar v praksi pomeni v 24 urah.

7 PREISKOVANJE KAZNIVIH DEJANJ, STORJENIH S POMOČJO INTERNETA

Internet je že zdavnaj zabrisal državne meje. Z brisanjem mej v EU in zagotovljeno svobodo gibanja raste potreba po novih, prožnejših ukrepih, ki bodo ekstremistom preprečili nadaljnje izkoriščanje razlik v pravni ureditvi držav članic. Internet je fizično determiniran medij, ki pa kljub temu v prvi vrsti predstavlja nekakšen virtualni prostor, v katerem udeleženci niso omejeni s svojo fizično lokacijo. Ta virtualni prostor ne pozna državnih mej. Vsako pozitivno dogajanje s seboj nujno prinese tudi nekaj negativnih plati. Če je mogoče o padanju državnih meja, vse večji kohezivnosti narodov in nastajanju združene Evrope govoriti kot o pozitivnih procesih, ni mogoče prezreti, da se prav zaradi teh procesov Evropa vedno bolj srečuje s pojavi, ki jih prej ni bilo zaznati v takšnem obsegu.

Teroristične skupine sicer uporabljajo internet kot podporo tradicionalnim oblikam terorizma, kjer se denimo teroristi naučijo različnih načinov izvedbe terorističnega napada, kot so na primer navodila za izdelavo eksplozivnih teles. Vzpostavljajo spletne strani, ki širijo njihove politične ali družbene cilje, pridobivajo nove člane, med seboj komunicirajo in koordinirajo napade. Trenutno preiskovalci v večini varnostnih organov priznavajo, da je internetni terorizem zaenkrat samo teoretični pojem, da možnosti realizacije niso velike (Thomas 2000).

Preiskovanje internetnega kriminala in ekstremizma je povezano s številnimi problemi.

- Prvi problem je ravnanje z računalniškimi sistemi in računalniško opremo. Kompleksnost te vrste orodij laikom in tudi preiskovalcem, ki niso strokovno usposobljeni, z računalniško tehniko in programi onemogoča spopadanje s to vrsto kriminala in terorizma.
- Spremljati in ocenjevati je treba številne spletne strani v različnih jezikih, za kar so potrebna zajetna tehnična sredstva in človeški viri.
- Zaradi ogromnega števila spletnih strani prihaja tako na nacionalni kot na mednarodni ravni do težav glede količine in kakovosti preiskovalcev, zlasti v zvezi s potrebnim znanjem jezikov.

- Preiskovalci v posamezni državi skorajda ne morejo spremljati vseh sumljivih in z ekstremizmom povezanih dejavnosti na internetu (Vodušek 1992 in Zupančič 1997).

Spremljanje in ocenjevanje interneta bi bilo torej treba okrepiti tako, da bi sodelovali na mednarodni ravni, pri tem pa upoštevali posebne jezikovne in strokovne usposobljenosti varnostnih agencij posameznih držav. Poleg izmenjave informacij prek Europola se lahko države članice odločijo, da si bodo prostovoljno razdelile delo in tako dosegle čim bolj učinkovito uporabo virov. Vendar pa bi, ne glede na morebitno delitev prednostnih nalog, odgovornost odločanja o spremljanju, prekinitvi ali zaprtju določenih spletnih mest ostala v pristojnosti držav članic (Vodušek 1992 in Zupančič 1997).

7.1 NAČIN DELA VARNOSTNIH ORGANOV

Danes pri delu policije in izvajanju preiskav ne smemo prezreti računalnika. To bi bilo tako, kot bi šli mimo cele vrste omar, ki vsebujejo osebno ali poslovno dokumentacijo. Računalnikov trdi disk lahko primerjamo z omaro, namenjeno shranjevanju papirne dokumentacije. Poglavitna razlika med zaseženimi papirnimi dokumenti in tistimi v digitalni obliki je v strokovnem znanju, ki je potrebno za pregled digitalnih podatkov oziroma dokazov, v obsegu podatkov, ki so lahko shranjeni, in v enostavnosti, s katero se ti digitalni podatki lahko poškodujejo ali uničijo. Podatki v elektronski obliki so dodaten vir dokazov, ki lahko predstavljajo kaznivo dejanje samo po sebi, ali pa so le podaljšek kaznivega dejanja, storjenega v fizičnem svetu. To organom pregona prinaša nove izzive pri zaseganju, izločanju in ravnanju s tovrstnimi podatki oziroma dokazi. Storilci kaznivih dejanj za seboj puščajo digitalne sledi, ki pa lahko vodijo v slepo ulico, prav tako je z njimi lahko manipulirati z namenom ovirati preiskave. Zato forenzične preiskave, ki hranijo digitalne podatke, predstavljajo vse pomembnejši člen pri preiskavah kaznivih dejanj, tako s področja računalniškega kriminala kot tudi ostalih, bolj klasičnih oblik (Barrett 1998).

Preiskovanje kaznivih dejanj, povezanih z ekstremizmom na internetu, od preiskovalcev zahteva posebne tehnike in pristope, saj se srečujejo z elektronskimi dokazi. Elektronski

dokazi, ki so povezani s kaznivimi dejanji, storjenimi s pomočjo interneta, so pogosto latentni (podobno, kot je latentna sled papilarnih linij) in krhki, lahko se hitro poškodujejo, celo uničijo. Pri iskanju dokazov o internetnem ekstremizmu morajo biti preiskovalci pozorni predvsem na dnevnike klepetov, digitalne kamere, elektronsko pošto, zapiske, pisma, skice, propagandne filme ipd. Elektronske dokaze nato obravnavajo v štirih fazah (Kastelic 2011):

1. Zbiranje dokazov: Sem uvrščamo iskanje dokazov, zbiranje in dokumentiranje, shranjevanje fotografij in ostalega gradiva. Pomembno je, da z gradivom ravnamo skrajno previdno.
2. Preiskovanje: Dokaz poskušamo narediti viden, s tem lahko ugotovimo izvor in pomembnost. V tem procesu lahko dokumentiramo vsebino in stanje dokaza, poiščemo skrite informacije in izpostavimo najpomembnejše.
3. Analiza: Iskanje dokazne vrednosti elektronskega dokaza.
4. Poročilo: Preiskovalci morajo po končanem delu napisati pisno poročilo, ki zajema opis vseh postopkov in pristopov preiskovanja in zbiranja dokazov, prav tako pa morajo biti navedeni tudi vsi elektronski dokazi.

7.1.1 OVIRE PRI DELU VARNOSTNIH ORGANOV

Na malo področjih preiskovanja kaznivih dejanj je odkrivanje storilcev tako težavno kot v digitalnem svetu. Seveda kot storilci teh dejanj še vedno nastopajo ljudje, vendar sta njihovo delovanje in identiteta pogosto prikrita. Hitrost, s katero se prenašajo podatki, prav tako povzroča težave pri odkrivanju. Razne transakcije se lahko opravijo v sekundi, pri tem pa pustijo zelo malo ali skoraj nič sledi, s pomočjo katerih bi lahko odkrili kršitve. Mnoga kazniva dejanja računalniškega kriminala so lahko povzročena brez kakršnegakoli fizičnega stika in brez fizičnega dokaza (Graboski in Smith 1998, 214).

Varnostni organi se soočajo z velikimi težavami in novimi izzivi, ki jih povzročajo novi načini komunikacije, naraščа softiciranost in hiter napredek tehnologije. Tako lahko komunikacijski kanali, ki jih uporabljajo storilci, potekajo skozi številne in različne vrste tehnologij, kot so npr. fiksna telefonija, lokalni ali mednarodni ponudniki teh tehnologij, brezžične in satelitske povezave. Prav tako lahko potekajo skozi številne države z

različnimi časovnimi območji in pravnimi sistemi. Vse te možnosti ovirajo napore organov pregona pri sledenju storilcev in njihovem odkrivanju (Kastelic 2005).

Anonimnost

Storilci lahko uporabljajo kar nekaj poti, da zakrijejo svojo identiteto in zmanjšajo možnost odkritja. Nekatere metode zahtevajo dokaj visoko stopnjo znanja in tehničnih spretnosti, z večino pa se storilci lahko seznanijo v literaturi, ki je prosto dostopna na internetu. Nekatere pogoste metode so posredovanje izmišljenih ali ukradenih osebnih podatkov pri registraciji pri internetnem ponudniku, uporaba anonimne elektronske pošte, predhodni vdor v enega ali več strežnikov, iz katerih nato opravljajo svoje dejavnosti, uporaba anonimnih strežnikov, ki ne posredujejo naprej podatkov o uporabniku (predvsem IP-naslov), in ponareditev podatkov o IP-naslovu, elektronski pošti, spletni strani (angleško spoofing).

Šifriranje

Komunikacijski kanali storilcev so lahko tudi šifrirani (kodirani, kriptirani). Pri tem se v večini primerov uporablja poseben šifrirni sistem. To storilcem omogoča varno komunikacijo, brez strahu pred prisluškovanjem, prestrezanjem ali sploh odkritjem.

Steganografija

Njen cilj je onemogočanje zaznave podatkov, ki so skriti v navidezno nepomembnih podatkih. Na internetu lahko uporabimo orodja, ki nam omogočajo skrivanje sporočil ali datotek v nosilnih datotekah, predvsem slikovnih (jpg, png, bmp, gif), pa tudi v zvokovnih datotekah (wav, mp3).

Lokacija

Dandanes lahko govorimo o virtualnih lokacijah, med katerimi se storilci selijo in se s tem izogibajo pravnim sankcijam in ukrepanjem organom pregona. Spletne strani, preko katerih opravljajo svoje kriminalne dejavnosti (npr. razširjanje sovražnega govora ali otroške pornografije ipd.), največkrat postavijo na strežnikih, ki so locirani v državah s pomanjkljivo zakonodajo, z neobstoječimi mednarodnimi sporazumi in manj usposobljenimi organi pregona.

Pravo

Eden izmed največjih izzivov organov pregona pri preiskovanju računalniškega kriminala je gotovo učinkovito sodelovanje in usklajevanje mnogih različnih pristojnosti in pravnih sistemov.

Policija in drugi organi pregona se pri računalniškem kriminalu soočajo z naslednjimi težavami (Kastelic 2006):

- veliko število neprijavljenih kaznivih dejanj; oškodovanec nerad prijavi kaznivo dejanje zaradi »dobrega imena«, banke, večja in manjša podjetja skušajo to reševati sama, redko se obrnejo na policijo, razen, če ta vdor ni viden navzven (povzročena škoda, vidna na internetni strani),
- anonimnost storilcev (sledi se hitro izgubijo),
- občutljivost dokazov; dokazi so hitro izbrisljivi, hitro prenosljivi, kar otežuje delo forenzike, ki ni nikoli zanesljivo,
- hiter razvoj, obsežnost in zapletenost tehnologije zahtevajo, da se morajo specializirati tožilci in policija. Težava pri tem je pomanjkanje časa za učenje,
- šifriranje,
- globalnost, ki je povezana z anonimnostjo; v primeru, da vdor v informacijski sistem poteka preko več držav, predstavlja težavo pridobivanje podatkov in dokazov preko držav. Postopki so lahko dolgotrajni,
- različna in pomanjkljiva zakonodaja; razlike med državami predstavljajo težave
- kar je v eni državi kaznivo, v drugi državi mogoče ni kaznivo dejanje,
- različna usposobljenost organov pregona (policije in sodstva),
- različni poudarki oziroma teža tovrstne kriminalitete pri vladnih organizacijah; težava pri predstavljanju tovrstne kriminalitete v državi, ker je vedno prioriteta druga vrsta kriminala (mamila, terorizem).

Nadzor zasebne elektronske pošte

Klemenčič (2001) upravičeno opozarja na razlikovanje pojma prestrezanje e-pošte v realnem času ter zasega e-pošte. Hkrati meni, da bo upravičenec (policija, sodišče) od upravljavca e-poštnega strežnika zahteval, da priredi sistem tako, da bo računalnik izdelal kopijo določenih ali vseh bodočih sporočil, prispelih na uporabnikov naslov, in jih

shranjeval v njemu oz. državnemu organu dostopnem mestu. Čeprav gre po njegovem mnenju na prvi pogled za zaseg e-pošte, s pravnega vidika to pomeni prestrezanje komunikacij.

Pri izvajanju prikritih preiskovalnih ukrepov, oz. pri proaktivnem delovanju policije bo zaseg (že prispele pošte) običajno le redko prišel v poštev, saj prispele pošte oz. informacije, ki jo e-pošta nosi, ne bo mogoče povezati s samo aktivnostjo osumljenca, aktivnostjo oseb, s katerimi komunicira, niti s samim kaznivim dejanjem, ki je šele v pripravi ali v teku. Zaseg e-pošte bo prišel v poštev bolj pri preiskovanju že izvršenih kaznivih dejanj oz. pri iskanju sostorilcev, pomagačev, napeljevalcev itd. Informacije pridobljene s prestrezanjem e-pošte imajo neko »dodano vrednost« v primerjavi z enakimi informacijami, ki nimajo predznaka »realnočasovnosti«, saj slednjih ni mogoče nadgrajevati s podatki pridobljenimi z ostalimi prikritimi preiskovalnimi ukrepi niti na njihovi podlagi prilagajati dejavnosti policije.

Klemenčič (2001) ugotavlja, da je slovenska zakonodaja glede zasega in zavarovanja že prispele e-pošte pomanjkljiva. Ena najpomembnejših metod za zbiranje dokazov pri klasičnih kaznivih dejanjih je po njegovem mnenju hišna preiskava in zaseg predmetov oz. dokumentacije, ki bi lahko služila kot dokazno gradivo. To lahko policija na podlagi sodne odredbe opravi v prostorih pošiljatelja ali naslovnika e-pošte ali celo pri upravljavcu strežnika, kjer se pošta nahaja. Pri tem je potrebno opozoriti na dejstvo, da se velika večina e-poštnih strežnikov (gmail, yahoo, hotmail), ki se najpogosteje uporabljajo pri elektronskem komuniciranju, nahaja v tujini, kar bistveno oteži samo izvedbo kakršnegakoli ukrepa (bodisi prestrezanja ali zasege podatkov). Prav tako lahko sodišče od vseh udeležencev v komunikaciji zahteva izročitev e-pošte, ki bi utegnile biti dokazilo v kazenskem postopku (220. člen ZKP).

Pregled informacijskih sistemov na daljavo

Slovenska zakonodaja, kot tudi veliko evropskih zakonodaj, ravno tako ne zajema pravne podlage za oddaljene preglede informacijskih sistemov. Nemški preiskovalni sodnik je novembra leta 2006 zavrnil zahtevo za oddaljeno preiskavo na računalniku osumljenca, osumljenega kaznivega dejanja ustanovitve teroristične združbe. Po mnenju

zveznega državnega tožilca pa je bila taka odločitev neupravičena in neutemeljena, še zlasti, ker je v podobnem primeru februarja istega leta drug preiskovalni sodnik ravnal drugače in preiskavo odobril na podlagi predpisov o hišni in osebni preiskavi. Na ta način so v Nemčiji vzpostavili pooblastilo tajnega oddaljenega preiskovanja (Podpečan 2007).

Tajno oddaljeno preiskovanje se imenuje »Bundestrojaner«, to je računalniški program za nadzor vsebin, do katerih določeni uporabnik dostopa prek spleta. BKA ga od predstavitve 2008 uporablja izključno za namene boja proti terorizmu, v točno določenih primerih. Obravnavajo ga kot »daljinsko forenzično orodje«, ki zahteva prilagoditve za vsak posamezni primer. Predvidevajo, da bo uporaben v največ 5–10 primerih na leto. Obtožni predlog mora biti za vsak primer posebej utemeljen, odobriti pa ga mora sodišče.

Navedena prikrita preiskava se izvaja na način, da se na računalnik osumljenca namestil ustrezen program, t. i. trojanski konj, ki neopazno pregleda vsebino vseh podatkov, vključno s stiki, prejeto in poslano e-pošto, shranjeno na računalniku, shranjenimi dokumenti, obiskanimi spletnimi stranmi, fotografijami itd. Tovrstne podatke je mogoče analizirati in izločati pomembne od nepomembnih že v računalniku preiskovanca, pozneje pa bi se prenesli na računalniški sistem preiskovalcev. Program se kasneje neopazno uniči. S podobnimi programi bi bilo mogoče upravljati tudi s spletno kamero in mikrofonom (Podpečan 2007).

Slovenska zakonodaja v tem trenutku tovrstnega pooblastila oz. pooblastila, ki bi omogočal navedeni poseg v zasebnost, (še) ne pozna, saj oddaljene preiskave ni mogoče enačiti s kontrolo komunikacij, ker prenos podatkov v trenutku preiskave ne poteka, ampak je komunikacija nujna šele zaradi prenosa podatkov v sistem preiskovalcev (Podpečan 2007).

Nedvomno bodo tovrstne preiskave zaradi narave podatkov in načina izvedbe preiskave porajale veliko (upravičenih) dvomov v samo kredibilnost pridobljenih podatkov.

7.2 UREDITEV V SLOVENIJI

S področjem preiskovanja organiziranega kriminala, ekstremizma in terorizma se v Republiki Sloveniji kot centralni organ ukvarja Uprava kriminalistične policije. Poleg tega so na državni ravni v to dokaj široko problematiko vključene tudi druge vladne ustanove, med katerimi velja omeniti naslednje:

- Skupina državnih tožilcev za pregon organiziranega kriminala,
- Slovenska obveščevalno-varnostna agencija,
- Obveščevalno-varnostna služba Ministrstva za obrambo,
- Urad za preprečevanje pranja denarja in financiranja terorizma,
- Urad Vlade Republike Slovenije za preprečevanje korupcije,
- Carinska uprava Republike Slovenije.

Naloge policije se izvajajo med drugim tudi v okviru izvajanja nalog, določenih v aktualni kriminalitetni politiki, ki jo je sprejela država. »Kriminalitetna politika kot praktičen boj proti kriminaliteti sicer obsega politiko kazenskega pregona, kaznovalno politiko, politiko izvrševanja kazenskih sankcij in tudi praktično izvajanje ukrepov za preprečevanje kriminalitete. Izhajajoč iz tega se kriminalitetna politika ne nanaša samo na dejavnost policije, sodišča ali zaporov, temveč tudi na politične reforme v družbi. To pojmovanje torej zajema politiko zatiranja in politiko preprečevanja, obenem pa tudi politiko ukvarjanja s posledicami. Pomembnejši dejavniki, ki določajo kriminalitetno politiko, so (Čurin 2003, 15–16):

- aktualna podoba kriminalitete,
- prevladujoča nazorska usmerjenost in miselnost družbe,
- aktualno politično ozračje v državi,
- zakonodaja in izvedba pravnih norm v praksi.

7.2.1 VLOGA POLICIJE

Ime policija ima korenine v več jezikih. V angleškem jeziku beseda »police« izhaja iz leta 1530 in ima isti pomen kot politika (policy); iz francoščine »police« (pozno 15. stoletje), iz latinske »politia«, kar pomeni civilna administracija, in iz grškega »polis«, ki pomeni mesto. V Angliji se je vse do sredine 19. stoletja uporabljala kot izraz za »civilno

administracijo«; aplikacija na »administracijo javnega reda« izvira iz Francije (1716) in se v originalu navezuje na odnos med Francijo in drugim tujimi narodi[42].

Nastanek policije je povezan z nastankom države oziroma človeka, če se zraven šteje še policijo kot dejavnost ali organizacijo, ki izvaja najrazličnejša policijska opravila. Nekatere naloge in opravila policije so prisotne že ves čas od njenega nastanka, druge pa so več ali manj posledica časa in njegovih posebnosti ter zahtev dejavnikov, ki so imeli moč nad policijo. Policija je v različnih zgodovinskih obdobjih, ob različnih družbeno-političnih ureditvah ter v različnih okoliščinah vselej opravljala določene stalne naloge in opravila, izmed katerih so najpogostejše: odkrivanje in prijemanje storilcev kaznivih dejanj ali drugih prepovedanih dejanj, vzdrževanje javnega reda in miru, urejanje in nadzor varnosti cestnega prometa (po razmahu ustreznih prevoznih sredstev) in nadzorovanje potencialnih prestopnikov. Dejavnost nadzorovanja in zagotavljanja varnosti se je torej od vsega začetka uporabljala za nemoteno delovanje določenih družbenih skupin ali družbenih razredov, ki so bili v tistih trenutkih in na tistih mestih na oblasti ter so tako nadzorovali policijo. Glede na zgoraj opisano lahko tako zatrdimo, da je policija ponavadi nekakšna sestavina določenega aktualnega političnega sistema, ki zahteva, da je do njega lojalna. Ta aktualna politična ureditev pa se nemalokrat zaradi zadovoljevanja svojih potreb tudi brez kakršnekoli strokovne ali organizacijske kompetence vmešava v njeno delovanje (Sluga 2000, 3).

Slovenska policija kot organ v sestavi Ministrstva za notranje zadeve je trenutno organizirana na treh ravneh, in sicer kot generalna policijska uprava, ki deluje na državni ravni in usklajuje, načrtuje in nadzira delo drugih ravni, na regionalni ravni v okviru policijskih uprav, ki v določeni meri usklajujejo in načrtujejo delo lokalnih ravni, ter na lokalni ravni v okviru policijskih postaj, policijskih oddelkov in policijskih pisarn, ki opravljajo osnovne naloge policije na najnižji ravni (Sluga 2000, 19–20).

Eden izmed pomembnih členov policije v boju proti terorizmu in ekstremizmu v Sloveniji je kriminalistična policija, ki je prisotna tako na državni kot na regionalni in lokalni ravni,

[42] Online Etimology Dictionary, geslo Police. Dostopno prek http://www.etymonline.com/index.php?search=police&searchmode=none

kar kaže na njeno življenjsko nujnost in potrebo po delovanju ter s tem zagotavljanju določenih nujnih nalog policije za varnejšo eksistenco upravičencev oz. družbe.

7.3 PREISKOVANJE EKSTREMIZMA V SLOVENIJI

Oddelek za terorizem in ekstremno nasilje skrbi predvsem za načrtovanje, organiziranje, usmerjanje, nadzorovanje ter izvajanje nalog pri odkrivanju in preiskovanju kaznivih dejanj na naslednjih področjih:

- terorizem,
- mednarodni terorizem,
- ogrožanje oseb pod mednarodnim varstvom,
- ogrožanje varnosti Republike Slovenije,
- ugrabitve in zajetja talcev,
- vodenje dela pogajalskih skupin,
- ekstremne oblike nasilja,
- organizirane oblike izsiljevanj,
- spopadi v kriminalnih združbah in med kriminalnimi združbami,
- nedovoljena proizvodnja in promet orožja, razstrelilnih in radioaktivnih snovi,
- zlorabe pri izvozu blaga dvojnega namena in strateških materialov, ki pomenijo sum storitve kaznivega dejanja,
- ogroženi delavci državne uprave in policisti,
- anonimna obvestila in pisanja z grozilno ali nenavadno vsebino,
- druga kriminaliteta z elementi ekstremnega nasilja (Černigoj, Blažina 2010).

Pri tem so ustrezni oddelki na regionalni ravni ali drugi kriminalisti, ki so usmerjeni v delovanje na tem delovnem področju, opremljeni tudi z raznimi, predvsem tehničnimi sredstvi, ki jim omogočajo lažje ugotavljanje prisotnosti eksplozivov pri določeni osebi ali v določenem prostoru.

Oddelek za računalniško kriminaliteto skrbi predvsem za načrtovanje, organiziranje, usmerjanje, nadzorovanje ter izvajanje nalog pri odkrivanju in preiskovanju kaznivih dejanj na naslednjih področjih:

- zlorabe avtorskih in sorodnih pravic, kadar so predmeti kaznivega dejanja računalniška oprema in sredstva,
- računalniške kriminalitete,
- zaseg podatkov iz spornih računalnikov in kasnejši pregled zaseženih podatkov,
- računalniške kriminalitete na internetu,
- razvoj in izpopolnjevanje metod, tehnik in taktik dela na področju računalniške kriminalitete (po MNZ, Policija, GPU, UKP, 2009).

Pri tem so ustrezni oddelki na regionalni ravni ali drugi kriminalisti, ki so usmerjeni v delovanje na tem delovnem področju, opremljeni tudi z raznimi, predvsem tehničnimi sredstvi, ki jim omogočajo lažje ugotavljanje in zavarovanje dokazov glede prisotnosti določenih računalniških ali drugih elektronskih sledi kaznivih dejanj (npr. pregled računalnikov glede dokazovanja prisotnosti elektronskih sledi otroške pornografije itd.).

Sektor za mednarodno policijsko sodelovanje na Upravi kriminalistične policije je glede specialnih nalog in delovnih področij, ki jih pokriva, notranje razdeljen na: Oddelek za Interpol, Oddelek za Europol, Oddelek za Sirene ter Oddelek za telekomunikacije in administracijo.

Oddelek za Interpol skrbi predvsem za komunikacijo in sodelovanje z mednarodno organizacijo kriminalistične policije (Interpol) ter koordinira sodelovanje drugih policijskih enot z Interpolom, poleg tega pa načrtuje, organizira, usmerja in nadzoruje delo še na naslednjih specialnih področjih:

- mednarodne tiralice,
- izročitev prijetih oseb, iskanih z mednarodno tiralico,
- ugotavljanje identitete in istovetnosti oseb,
- posredovanje obvestil svojcem o osebah, ki so v priporu, in obvestil o smrtnih primerih,
- izmenjava operativnih podatkov in informacij o kriminaliteti,
- posredovanje pri organiziranju operativne pomoči pri mednarodnih preiskavah,
- mednarodna kazenskopravna pomoč,
- posredovanje podatkov na podlagi mednarodnih pogodb,

- sodelovanje pri upravljanju in izkoriščanju mednarodnih zbirk podatkov in informacij o listinah, motornih vozilih, vodnih plovilih, zračnih plovilih, umetninah in drugih predmetih, povezanih s kriminaliteto,
- druge naloge posredovanja pri mednarodnem iskanju oseb in pri operativnem sodelovanju pri preiskovanju kriminalitete (po MNZ, Policija, GPU, UKP, 2009).

Oddelek za Europol skrbi predvsem za komunikacijo in sodelovanje z Evropskim policijskim uradom (Europol) ter koordinira sodelovanje drugih policijskih enot z Europolom, poleg tega pa načrtuje, organizira, usmerja in nadzoruje delo še na naslednjih specialnih področjih:

- preprečevanje hujših oblik mednarodne kriminalitete na naslednjih področjih: nezakonita trgovina s prepovedanimi drogami, trgovina z jedrskimi in radioaktivnimi snovmi, kriminaliteta motornih vozil, kazniva dejanja, ki so bila ali verjetno bodo storjena pri terorističnih dejavnostih zoper življenje in telo, osebno svobodo ali lastnino, ponarejanje denarja in plačilnih sredstev, pranje denarja v povezavi z naštetimi oblikami kriminalitete ali njihovimi specifičnimi pojavnimi oblikami ter z njimi povezanimi kaznivimi dejanji,
- skrb za nemoteno in hitro komunikacijo med Europolom in pristojnimi službami v Sloveniji,
- oskrbovanje Europola s podatki in znanjem, potrebnimi za izvajanje njegovih nalog,
- odgovarjanje na Europolove zahteve za podatke, znanje in nasvete,
- posredovanje zaprosil za nasvet, podatkov, znanja ter analitične in tehnične podpore preiskav Europolu,
- oskrbovanje Europola s podatki za shranitev v Europolovo bazo podatkov,
- zagotavljanje skladnosti z zakonom pri vsaki izmenjavi podatkov z Europolom,
- sodelovanje pri razvoju Europola in razvoju sodelovanja z njim,
- skrb za izobraževanje in osveščanje pristojnih služb v Sloveniji glede Europola,
- sodelovanje na raznih konferencah, sestankih in v delovnih skupinah v okviru Europola na strateški ravni,
- sodelovanje v organih Europola, predvsem v Odboru vodij nacionalnih enot Europola,

- sodelovanje v delovnih skupinah Sveta EU, ki se nanašajo na Europol,
- opravljanje drugih nalog posredovanja pri policijskem mednarodnem sodelovanju (po MNZ, Policija, GPU, UKP, 2009).

Oddelek za Sirene skrbi predvsem za nemoteno delovanje dela Schengenskega informacijskega sistema (SIS), ki se veže na Slovenijo, in za vzdrževanje, preverjanje ali vnos podatkov v ta informacijski sistem, poleg tega pa načrtuje, organizira, usmerja in nadzoruje delo še na naslednjih specialnih področjih:

- izvajanje nalog v okviru nacionalnega dela Schengenskega informacijskega sistema v notranjih organizacijskih enotah generalne policijske uprave in policijskih uprav,
- notranje in mednarodne tiralice,
- vodenje in vzdrževanje evidenc iskanih oseb, vozil in predmetov,
- izročitev prijetih oseb, iskanih z mednarodno tiralico,
- ugotavljanje identitete in istovetnosti oseb,
- izmenjava podatkov v zvezi z osebami ali vozili v okviru ukrepov tajne registracije ali točno določene kontrole,
- izmenjava operativnih podatkov v okviru mednarodnega policijskega sodelovanja in za kazenski postopek v okviru mednarodne kazenskopravne pomoči,
- izobraževanje in usposabljanje uporabnikov SIS-a,
- sodelovanje pri upravljanju in uporabi obstoječih mednarodnih zbirk podatkov in evidenc,
- splošne pravne zadeve,
- zaščita in varstvo podatkov,
- druge naloge posredovanja pri policijskem mednarodnem sodelovanju (po MNZ, Policija, GPU, UKP, 2009).

7.4 NAČIN PREISKOVANJA V SLOVENIJI

Pri operativnih postopkih policistov in kriminalistov v zvezi z obravnavano tematiko se iz Zakona o kazenskem postopku v praksi največkrat uporablja klasična in posebna pooblastila tega zakona. Največkrat se pri odkrivanju kaznivih dejanj s področja ekstremizma uporablja pooblastila Zakona o kazenskem postopku. V praksi se največkrat

uporablja t. i. posebne ali prikrite preiskovalne ukrepe in postopke. Tako se največkrat izvaja ukrepe iz 149. a, 149. b, 150., 151., 155., 155. a, 156. in 159. čl. Zakona o kazenskem postopku. Ti ukrepi obsegajo:

- pridobivanje izpisov elektronskih komunikacij, pridobivanje lastništev ali drugih podatkov o uporabnikih komunikacijskih sredstev,
- tajno opazovanje in sledenje ter snemanje oseb,
- nadzor elektronskih komunikacij ali pisemskih pošiljk ter računalniškega sistema bank ali drugih finančnih ustanov,
- prisluškovanje in snemanje pogovorov s privolitvijo vsaj ene osebe, udeležene v pogovoru,
- tajno delovanje,
- navidezni odkup,
- navidezno sprejemanje oz. dajanje daril ali navidezno jemanje oziroma dajanje podkupnin,
- pridobivanje podatkov od bank ali drugih finančnih ustanov brez vednosti strank,
- odlog odvzema prostosti osumljene osebe ali izvršitev drugih ukrepov iz Zakona o kazenskem postopku.

Ti ukrepi so tako namenjeni predvsem prikritemu, usmerjenemu in stalnemu zbiranju dokazov za težje oblike kaznivih dejanj, ki so tudi težje dokazljivi, vsaj za vpletene osumljene z višjih kriminalnih ravni. Ob tem je treba v večini primerov za potrebe izvajanja teh ukrepov predhodno izkazati dovolj visok dokazni standard suma (predvsem utemeljeni razlogi za sum ob obstoju še dodatnih pogojev), prav tako pa večino teh ukrepov policija izvaja na podlagi poprej izdanih ustreznih odredb ali dovoljenj državnega tožilstva ali sodišča.

V primeru, da obstajajo pogoji in relativno ugodna ocena glede možnosti dokazovanja in preiskovanja izvajanja širše kriminalne dejavnosti s strani več oseb (organizirana kriminaliteta), katerih identitete ali okoliščine v tistem trenutku še niso znane, se policija na podlagi dogovorov in usmeritev državnega tožilstva lahko odloči za nadaljnje preiskovanje konkretnih primerov s pomočjo uporabe prikritih preiskovalnih ukrepov. Ko se s kombinacijo izvajanja prikritih preiskovalnih ukrepov in klasičnih ukrepov policije

zbere dovolj dokazov, se podobno kot v navadnem postopku poda kazensko ovadbo po redni poti na pristojno državno tožilstvo (bolj redko) ali pa se osumljenca ali osumljence skupaj s kazensko ovadbo privede pred pristojnega preiskovalnega sodnika (praviloma).

Zaradi vse večjega pojavljanja organizirane in gospodarske kriminalitete in vse bolj sofisticiranih oblik kriminalitete v kazenskih postopkovnih in stranski kazenski procesni zakonodaji se vse pogosteje uveljavljajo t. i. posebna preiskovalna dejanja. Ta so namenjena pridobivanju tistih dokazov, ki jih z običajnimi, se pravi klasičnimi preiskovalnimi dejanji, ne bi bilo mogoče pridobiti in brez katerih učinkovit kazenski pregon tovrstne kriminalitete pravzaprav ne bi bil mogoč (Karakaš v Bavcon 2000, 240–241). Prikrite preiskovalne ukrepe policija pri preiskovanju najhujših oblik kaznivih dejanj uporablja le izjemoma, ob uporabi načela subsidiarnosti ter načela sorazmernosti.

Pri tem se pokažejo nekatere skupne značilnosti, ki jih narekuje uporaba prikritih preiskovalnih ukrepov: obstajati mora večja stopnja verjetnosti, da je določena oseba izvršila, izvršuje ali pripravlja oz. organizira izvršitev določenih kaznivih dejanj (razlogi za sum in utemeljeni razlogi za sum), obstajati mora določljivost osebe, obstajati mora utemeljeno sklepanje, da policisti z drugimi ukrepi ne bi mogli odkriti kaznivega dejanja, ga preprečiti oz. bi bilo to povezano z nesorazmernimi težavami, ukrepi veljajo le za določena kazniva dejanja (hujša, ki so določena z višino zagrožene kazni ali celo kataloško našteta kazniva dejanja), odredbodajalec ni samo policija, ki jih le izvaja, temveč drugi organi (državni tožilec ali preiskovalni sodnik), izvajanje prikritih preiskovalnih ukrepov je časovno omejeno, določena je hierarhija prikritih preiskovalnih ukrepov itd. (Grandič 2007, 99–101).

Določbe 15. člena II. poglavja Ustave Republike Slovenije med drugim določajo, da so človekove pravice in temeljne svoboščine omejene samo s pravicami drugih in v primeru, ki jih določa Ustava. To pomeni, da je pravica in svoboščina enega omejena le z enako pravico in svoboščino drugega in v izrecno v Ustavi predpisanih primerih, pri katerih pa Ustava predpisuje razloge za omejitve. Poseg v pravice drugega hkrati pomeni tudi zlorabo neke pravice, o kateri govorimo takrat, kadar se pravica izvršuje prek tiste meje, ki v kakovostno enakem obsegu tudi drugemu dopušča uresničevati

njemu pripadajočo pravico. Gre torej za izvrševanje pravice v nasprotju z njeno vsebino, obsegom oz. namenom (Rupnik in drugi 1996, 71–73).

Omejitve človekovih pravic so nujno pogojene z načelom sorazmernosti, saj že iz vsebine nekaterih človekovih pravic izhaja, da ena ovira drugo oz. da se medsebojno omejujeta, kar hkrati tudi pomeni, da se obseg varovanja vsake pravice zmanjšuje v obsegu, ki je nujno potreben zaradi uveljavitve druge pravice. Omejitev človekovih pravic s pravicami drugih tako pomeni, da se mora posameznik podrediti tistim omejitvam svoje svobode ravnanja, ki jih določa zakonodajalec zaradi varstva in razvoja sožitja ter napredka v družbi, ob predpostavki, da ostane zagotovljena samostojnost človeka kot posameznika. Ustavno varovane pravice je mogoče omejiti tudi zaradi javnega interesa, če zakonodajalec na podlagi tehtanja javnih koristi (v primeru izvajanja kaznivih dejanj, povezanih z ekstremizmom, itd.) ugotovi, da je omejitev nujno potrebna, in če je ukrep, s katerim zakonodajalec omeji ustavno pravico, utemeljen, ali če iz narave neke dejavnosti izhaja, da so za njeno izvajanje potrebna posebna znanja, sposobnosti in ostale lastnosti, brez katerih bi nastale škodljive posledice ali nevarno stanje. V javnem interesu uzakonjene omejitve norme morajo biti v skladu z načeli pravne in socialne države. Ustavno pravico je praviloma dopustno omejiti samo z zakonom, ne pa tudi z nižjehierarhičnim aktom, vendar iz prakse Ustavnega sodišča poznamo tudi izjeme tega pravila (Grandič 2007, 101–102).

Načelo sorazmernosti se sicer običajno presoja preko skupne presoje podnačel primernosti (sredstva države za dosego svojih ciljev morajo biti primerna, možna, uporabna in učinkovita – takšna pa so takrat, ko neko negativno ravnanje preprečijo, odkrijejo in v primeru kazenskih sankcij tudi ustrezno sankcionirajo ter preganjajo), potrebnosti oz. nujnosti (za dosego cilja ni na voljo alternativnega ukrepa, ki bi bil enako učinkovit in bi hkrati manj posegal v prizadeto pravico) ter proporcionalnosti oz. sorazmernosti v ožjem smislu (enakost oz. neenakost orožij) (Grandič 2007, 34–38).

Temelje za spoštovanje načela sorazmernosti pri posegih države v človekove pravice in svoboščine oseb lahko najdemo v številnih mednarodnih in nacionalnih dokumentih, izmed katerih so najpomembnejši: Splošna deklaracija človekovih pravic Združenih

narodov iz leta 1948, Evropska konvencija o varstvu človekovih pravic in temeljnih svoboščin iz leta 1950 (EKČP), Ustava Republike Slovenije itd. Ne nazadnje se je med izoblikovanjem sodne prakse tudi z odločbami Ustavnega sodišča Republike Slovenije na področju prikritih preiskovalnih ukrepov posegalo v pogoje, načine in obsege izvajanja takih ukrepov, kar je še posebno razvidno iz odločb Ustavnega sodišča št. U-I-25/95, št. U-I-158/95, št. U-I-234/97 in št. U-I-272/98.

Za potrebe učinkovitega izvajanja prikritih preiskovalnih ukrepov in klasičnih nalog policije se mora policija zaradi kompleksnosti in vse bolj tudi mednarodnega delovanja organiziranih kriminalnih združb ali ekstremističnih skupin, ki se po večini ali pa vsaj na višjih ravneh praviloma vedno ukvarjajo z izvrševanjem tovrstnih kaznivih dejanj, vse bolj zanašati na analize poprej pridobljenih podatkov, ki se pridobijo s spremljanjem dejavnosti, gibanja in pojavljanja sumljivih oseb na lokalnih, regionalnih, nacionalnih in tudi širših območjih. Za takšno analitično podporo ob mednarodnem sodelovanju skrbi predvsem Center za kriminalistično analitiko v okviru Urada kriminalistične policije na Generalni policijski upravi.

7.4.1 RAČUNALNIŠKA FORENZIKA

Poklic računalniški forenzik je pri nas še malo poznan, vendar se znanost, ki se je razvila v Ameriki, prebuja tudi v Evropi. Izraz računalniška forenzična znanost so leta 1991 skovali ameriški strokovnjaki prostovoljne neprofitne korporacije ISTS, ki deluje v okviru organizacije strokovnjakov za računalniški kriminal. Osnovni namen računalniške forenzike je iskanje dokaznega gradiva v računalniških sistemih. S pomočjo podatkov, ki jih strokovnjak za računalniško forenziko pri svojem delu analizira, lahko »zavrti čas nazaj« in ugotovi namen uporabe sistema včeraj, pretekli teden, mesec ali preteklo leto. Raziskuje, ali so bili podatki spremenjeni oziroma zbrisani, pri tem pa odgovarja na vprašanja, kdo, kaj in zakaj. Na podlagi analize podatkov naredi poročilo, ki ga lahko naročnik uporabi tudi kot dokazno gradivo na sodišču (Kastelic 2005).

Računalniški forenzik mora pridobiti podatke iz elektronskega medija tako, da ostanejo izvorni podatki nespremenjeni. Osumljenca mora obravnavati kot profesionalca, ki obvlada prekrivanje podatkov in pozna vse ukane forenzičnih strokovnjakov. Z

računalnikom mora ravnati tako, kot bi ravnal osumljenec pri njegovi normalni uporabi. Majhna napaka lahko začne uničevati podatke na disku. Da mora biti znanje forenzika o programski in strojni opremi na visoki ravni, je samo po sebi umevno, opremo, ki jo preučuje, pa mora poznati do popolnosti. Kot rečeno, cilj forenzika je ohranitev digitalnih podatkov, zato je zelo pomemben potek raziskave (Kastelic 2005).

Z računalniško forenziko se torej lahko izognemo izgubi ali okvari podatkov, možnosti, da podatki niso obnovljeni v celoti. Pridobimo možnost, da bodo dokazi, pridobljeni z raziskavo, priznani kot dokaz na sodišču ali v drugih postopkih, ter da se bomo izognili tožbi, ker so bili pomembni podatki, dokumenti ali oprostilni dokazi uničeni ali niso bili najdeni. Da kdo naroči forenzično raziskavo, mora imeti za to podlago: sodno ali v pravilniku podjetja, ki to dovoljuje. Računalniške forenzične raziskave so prvi začeli uporabljati organi pregona, torej policija in vojska. Potem pa so se preselile tudi na zasebno področje; zavarovalnice preko nje dokazujejo primere prevar pri odškodninskih zahtevkih. Računalniške forenzične raziskave so v pomoč tudi pravosodju pri dokazovanju različnih kaznivih dejanj, na primer poneverbe, finančne prevare, otroške pornografije (Banovič 2007).

Obstaja precej različnih naprav, ki jih lahko uporabimo za odkrivanje nedovoljenih dejanj. Nekatere so drage in tehnološko visoko razvite, druge poceni in zelo preproste.
Ukrepe za odkrivanje lahko razdelimo v dve skupini (Icove v Smrkolj 2000, 33):

- Preventivni ukrepi: Ti ukrepi zaznajo dejanje v trenutku, ko se to izvršuje. Za zaščito objekta ali prostora z računalniško opremo je potrebna standardna oprema, kot so protivlomni alarmi. Potrebna je tudi programska oprema, ki deluje podobno kot alarmne naprave. Takšen program sproži alarm v primeru nedovoljenega vstopa v sistem ali tudi nedovoljenega vstopa v območje, za katero nekdo nima avtorizacije.
- Pregledi sistema: Redni pregledi sistema nam omogočajo, da odkrijemo ponavljajoča se dejanja ali dejanje, ki je bilo že storjeno. Večino sistemov zapisuje dnevnik vseh operacij, ki se v njem izvajajo. To lahko s pridom uporabimo pri preiskovanju in odkrivanju kaznivih dejanj. Sistemski dnevnik lahko uporabimo tudi kot dokaz. Oblika in kakovost podatkov v dnevniških zapisih

se razlikujeta od sistema do sistema. Zelo varovani sistemi v teh zapisih vsebujejo veliko informacij. V sistemskem dnevniku je pomembno iskati povezave, ki se dogajajo v času, ki navadno ni čas uporabe sistema, pregledovati neuspele poskuse povezave, pozorni pa moramo biti tudi na poskuse odpiranja datotek brez avtorizacije.

Prijava računalniškega kriminala v Sloveniji se poda na krajevno pristojni Sektor kriminalistične policije (11 uprav po Sloveniji). Pri prijavi je pomembno, da se navedejo naslednji podatki (Kastelic 2006):

- kronološko-tehnični opis incidenta/napada:
- navedba in kratek opis priloženih (digitalnih) dokazov, priloženi digitalni dokazi so odvisni od primera. Lahko so:
    - dnevniške datoteke v zvezi z incidentom (IP-naslov, datum, čas, dejavnost napadalca), opis in morebitna analiza,
    - e-pošta, vključno z glavami – IP-naslov, datum, čas,
    - programi, skripte in druge nameščene datoteke, spremenjene pri napadu/incidentu,
    - morebitne izjave skrbnika sistema (o zaznavi incidenta, o pregledu sistema, zaščiti dokazov),
    - morebitni zapisi s klepetalnic, forumov, spletnih strani;
- podatki o prijavitelju, kontaktni podatki (o odgovorni osebi – direktor, vodja IT, o skrbniku sistema, o morebitnem zunanjem pogodbenem skrbniku, o morebitnih drugih organizacijah, naziv organizacije in kontaktnih oseb, službeni naslov, e-pošta, telefon);
- podatki o napadenem informacijskem sistemu (fizična lokacija, IP- in DNS-naslov, datum, čas in trajanje incidenta, vloga – spletni, poštni strežnik in opis informacijskega sistema – varnostna oprema, navedba in vrsta napadenih, uničenih, poškodovanih, kopiranih, spremenjenih ali vnesenih podatkov – osebne, poslovne, avtorsko zaščitene narave, spletne strani);
- podatki o incidentu:

- narava in metoda incidenta: vdor, oviranje delovanja, poškodovanje sistema, poškodovanje spletne strani - defacement, trojanski konj, virus, izkoriščanje ranljivosti,
- domnevni storilec: zaposleni, tekmec, poslovni partner, bivši zaposleni,
- izvedeni ukrepi: izključitev sistema, izdelava varnostne kopije, pregled dnevniških in sistemskih datotek.

Pri prijavi poškodovanja oziroma vdora v informacijski sistem se je treba zavedati, da vsak incident nima suma kaznivega dejanja. Vsak sum kaznivega dejanja ni utemeljen in dokazan, kar pomeni, da ni zakonske podlage za nadaljnje ukrepanje.

7.4.2 NADZOR INTERNETA V SLOVENIJI

Ena izmed glavnih značilnosti internetne komunikacije je relativno velika stopnja anonimnosti uporabnika. Uporabnika, ki komunicira s pomočjo interneta ali se pojavlja na določenih spletnih straneh, je težko določiti. Ravno tako kot vse uporabnike je težko določiti prisotnost preiskovalcev. To je ena izmed prednosti anonimnosti, ker tudi delavci varnostnih organov lahko prikrito vzpostavijo stike z osebami, ki na spletu širijo ekstremistične ideje, in lahko na ta način od njih zbirajo podatke.

Klemenčič (v Bogataj 2007) primerja policijsko patruljiranje v fizičnem svetu in patruljiranje po internetu, pri čemer najde veliko skupnih točk. Patruljiranje po internetu je stalna ali občasna prisotnost policistov na internetu, kjer pregledujejo njegovo vsebino z namenom iskanja protipravnih dejavnosti (npr. otroške pornografije, piratstva, sovražnega govora ipd.), prav tako je na ta način mogoče odkriti storilce različnih klasičnih kaznivih dejanj (npr. prodaje ukradenih stvari preko spletnih borz) in zbirati operativne podatke o dejavnostih različnih operativno zanimivih skupin (npr. športni huligani). Klasičnega patruljiranja ni mogoče v celoti enačiti z internetnim tudi zaradi (ne)vidnosti tistega, ki patruljiranje izvaja.

Pri presoji dopustnosti posameznega posega je v praksi uveljavljena maksima, da kar sme na javnih in odprtih prostorih zakonito početi posameznik, to sme brez posebnega dodatnega pooblastila (npr. sodne odredbe) početi tudi policist; tako ne more biti sporno ogledovanje spletnih vsebin in pregledovanje javnih forumov in novičarskih skupin.

Sprejemljiva je tudi (čeprav deloma tudi sporna) aktivna komunikacija policistov v klepetalnicah in IRC-u, in sicer vse dotlej, dokler komunikacija poteka v javno odprtem delu interneta, in se ne nanaša na določljivo konkretno osebo z namenom pridobivanja podatkov, ki bi se lahko uporabili v (pred) kazenskem postopku. Vsakršen poseg policije v nejavni ali zaščiteni del interneta brez ustreznih zakonskih pooblastil in sodnih odredb pa je brez dvoma nezakonit. Pri tem bi bilo treba (zaradi različnih možnosti omejevanja dostopa različnim uporabnikom) opredeliti, kdaj določena komunikacija še poteka v javnem delu interneta oz. kaj tako javno komunikacijo definira (Bogataj 2007).

Ali bi npr. policist deloval nezakonito, če bi na primer od prijatelja pridobil uporabniško ime in geslo za dostop do določenega zaprtega dela foruma in se na ta način udeležil komunikacije med radikalnimi pripadniki navijaških skupin. Ni sporna komunikacija, ki bi jo policist na zaprtem delu foruma vzpostavil z nedoločljivo osebo z namenom, da pridobi podatke o določenem varnostno problematičnem dogodku (npr. organizaciji protestov, organiziranem delovanju navijačev ipd.). Pri tem ne moremo govoriti o določljivosti osebe, če razpolagamo samo z e-naslovom ali vzdevkom, ki jih soudeleženec uporablja pri komunikaciji. Taka internetna dejavnost policije bi postala nezakonita v trenutku, ko taka oseba postane določljiva in bi se krog njegovega zanimanja iz poskusa pridobivanja podatkov o varnostno relevantnem dogodku preusmeril na pridobivanje podatkov o dejavnosti določljive osebe, za kar bi bilo potrebno dovoljenje (odredba) državnega tožilca za tajno delovanje (Erten 2009).

V zadnjem času veliko večino tako imenovanega internetnega patruljiranja opravljajo tudi nevladne organizacije, na primer organizacija Spletno oko.

7.4.3 ZASEG ELEKTRONSKIH PODATKOV

V Sloveniji se zaseg in zavarovanje informacijskih sistemov in podatkov izvaja po nekoliko arhaičnih določilih ZKP o hišni preiskavi in zasegu predmetov. Hišno preiskavo lahko policija na podlagi sodne odredbe opravi tako pri samem uporabniku informacijskega sistema kot tudi pri ponudniku internetnih storitev oziroma skrbniku strežnikov. Zakonska podlaga, ki ureja zaseg in zavarovanje elektronskih podatkov, je urejena v ZKP-J, Uradni list RS, št. 77/09 (Bogataj 2007). Prav tako lahko sodišče od

uporabnikov in skrbnikov strežnikov zahteva izročitev določenih podatkov, ki se nahajajo v informacijskih sistemih in bi utegnili biti dokazilo v kazenskem postopku (220. člen ZKP).

Zaseg informacijskih sistemov in že shranjenih podatkov praviloma zahteva tudi pregled računalnika oziroma omrežja, na katerem so shranjeni. Pojavljajo se vprašanja zaščite interesov tretjih oseb, ki uporabljajo isti računalnik oziroma računalniško omrežje, (ne)dovoljenega obsega preiskave (ali se ta lahko z določenega računalnika razširi na celotno računalniško omrežje, v katerega je računalnik povezan) ter ravnanja s podatki, zaseženimi v elektronski obliki, in njihove dokazne vrednosti (Erten 2009).

7.5 POLICIJSKA POOBLASTILA IN PRAVNI AKTI, KI UREJAJO MEDNARODNO POLICIJSKO SODELOVANJE

V praksi se pri preiskavi kaznivih dejanj, povezanih z ekstremizmi na internetu, uporablja vrsta mednarodnih dokumentov, ki zakonodajno urejajo to področje. Na tem mestu so predstavljeni nekateri ključni nacionalni pravni viri, ki urejajo področje ekstremizma. Navedeni so tudi nekateri ključni mednarodni ter evropski pravni viri, h katerim je pristopila Republika Slovenija.

Potreba po mednarodni koordinaciji izvira iz kriminala kot globalnega pojava, ki presega državne meje. Računalniške mreže in računalniški podatki, ki prav tako ne upoštevajo fizičnih meja, ustvarjajo globalni kibernetski prostor. Poleg tega računalniške mreže, kakršna je internet, omogočajo razvoj novih oblik tehnologije, s pomočjo katerih lahko uporabniki ohranijo anonimnost, sodelujejo v skriti komunikaciji in pri prenosu in hrambi podatkov uporabijo napredne šifrirne programe (Whine 1999 in Edwards ter Zanini 2001).

Leta 2001 je Republika Slovenija sprejela Resolucijo o strategiji nacionalne varnosti, v kateri opredeljuje nacionalne interese, varnostna tveganja in vire ogrožanja države, njenih institucij, državljank in državljanov ter usmeritve, ukrepe in mehanizme za zagotavljanje nacionalne varnosti. Med strateškimi interesi Republike Slovenije je omenjena tudi zagotovitev delovanja demokratičnega parlamentarnega političnega

sistema, krepitev pravne in socialne države, dosledno spoštovanje človekovih pravic in temeljnih svoboščin, vključno z zaščito pravic narodnih manjšin ter zagotavljanjem ohranjanja in razvoja slovenskih avtohtonih narodnih manjšin v zamejstvu, zagotovitev stabilnega gospodarskega razvoja in krepitev konkurenčnega gospodarstva ter vključevanje v Evropsko unijo in Severnoatlantsko pogodbeno zvezo (NATO). Med viri ogrožanja Republike Slovenije sta našteta tudi terorizem in organizirani kriminal, saj se Republika Slovenija, predvsem zaradi svoje lege, sooča s transnacionalnimi grožnjami v obliki organiziranega kriminala, ilegalnih migracij, trgovanja z belim blagom, trgovanja z mamili, ilegalne trgovine z orožjem in materiali, terorizma in pranja denarja, notranje pa jo ogrožajo tudi posebne oblike kriminalitete.

Leta 2004 je bil sprejet Zakon o ratifikaciji Mednarodne konvencije o zatiranju financiranja terorizma, ki ratificira že zgoraj omenjeno konvencijo in njene določbe.

Istega leta je bil sprejet Zakon o ratifikaciji Konvencije Združenih narodov proti mednarodnemu organiziranemu kriminalu, ki ratificira že zgoraj omenjeno konvencijo in njene določbe.

Leta 2004 je bil sprejet Zakon o evropskem nalogu za prijetje in predajo, ki določa pogoje in postopke predaje oz. ekstradikcije obdolžencev ali obsojencev med Republiko Slovenijo in ostalimi državami članicami Evropske unije, ki pa je leta 2007 prenehal veljati z dnem uveljavitve Zakona o sodelovanju v kazenskih zadevah z državami članicami Evropske unije.

Leta 2004 je Republika Slovenija sprejela Zakon o elektronskih komunikacijah, ki je bil kasneje še noveliran in ki se pri preiskovanju organizirane kriminalitete, terorizma ter s tem povezanem preiskovanju kriminalitete v zvezi z ekstremizmi na internetu v določenih delih neposredno navezuje tudi na obravnavano problematiko. Zakon med drugim določa pogoje za poseganje v pravico do zasebnosti pri elektronski komunikaciji oz. za izvajanje posebnih ter prikritih preiskovalnih ukrepov s strani policije ali drugih pristojnih inštitucij.

Prav tako leta 2007 je bil sprejet Zakon o sodelovanju v kazenskih zadevah z državami članicami Evropske unije, ki ukinja Zakon o evropskem nalogu za prijetje in predajo iz leta 2004 ter smiselno podobno ureja postopke za medsebojno pravno sodelovanje in pomoč med državami članicami Evropske unije, podrobneje pa ureja tudi postopke predaj oz. ekstradikcij določenih oseb.

Leta 2007 je Republika Slovenija sprejela Zakon o ratifikaciji Pogodbe med Kraljevino Belgijo, Zvezno republiko Nemčijo, Kraljevino Španijo, Francosko republiko, Velikim vojvodstvom Luksemburg, Kraljevino Nizozemsko in Republiko Avstrijo o poglobitvi čezmejnega sodelovanja, predvsem pri zatiranju terorizma, čezmejne kriminalitete in nezakonite migracije, in skupne izjave Kraljevine Belgije, Zvezne republike Nemčije, Kraljevine Španije, Francoske republike, Velikega vojvodstva Luksemburg, Kraljevine Nizozemske in Republike Avstrije k pogodbi z dne 27. 5. 2005 o poglobitvi čezmejnega sodelovanja, predvsem pri zatiranju terorizma, čezmejne kriminalitete in nezakonite migracije. Zakon predvsem vzpostavlja določila za medsebojno sodelovanje pri komuniciranju ali nudenju podatkov iz operativnih baz, pri elektronski primerjavi DNK-profilov ter daktiloskopskih podatkov, pri uporabi službenih orožij na letalih itd.

Istega leta je Republika Slovenija sprejela Zakon o preprečevanju pranja denarja in financiranja terorizma, ki med drugim določa tudi pomen pojma "pranje denarja", kar po tem zakonu pomeni katerokoli ravnanje, s katerim se prikriva izvor denarja ali drugega premoženja, pridobljenega s kaznivim dejanjem, in vključuje zamenjavo ali kakršenkoli prenos denarja ali drugega premoženja, ki izvira iz kaznivega dejanja ali pa vključuje skrivanje ali prikrivanje prave narave, izvora, nahajanja, gibanja, razpolaganja, lastništva ali pravic v zvezi z denarjem ali drugim premoženjem, ki izvira iz kaznivega dejanja. Nadalje zakon določa pomen pojma "financiranje terorizma", kar po tem zakonu pomeni zagotavljanje ali zbiranje oz. poskus zagotavljanja ali zbiranja denarja ali drugega premoženja zakonitega ali nezakonitega izvora, posredno ali neposredno, z namenom ali zavedajoč se, da bo v celoti ali delno uporabljeno za izvedbo terorističnega dejanja ali da ga bo uporabil terorist oz. teroristka ali teroristična organizacija. Določen je tudi pomen pojma "terorist", ki po tem zakonu pomeni fizična oseba, ki stori ali poskuša storiti teroristično dejanje na kakršenkoli način, oseba, ki je udeležena pri storitvi terorističnega

dejanja kot sostorilec, napeljevalec ali pomagač, oseba, ki organizira storitev terorističnega dejanja, ali oseba, ki prispeva k terorističnemu dejanju skupine ljudi, ki deluje s skupnim ciljem, če ravna namerno in z namenom prispevati k nadaljevanju izvajanja terorističnega dejanja ali je seznanjena z namenom skupine, da stori teroristično dejanje. Pojem "teroristična organizacija" je po tem zakonu opredeljen kot katerakoli skupina teroristov, ki storijo ali poskušajo storiti teroristično dejanje na kakršenkoli način, ki so udeleženi pri storitvi terorističnega dejanja, ki organizirajo storitev terorističnega dejanja ali ki prispevajo k terorističnemu dejanju skupine ljudi, ki deluje s skupnim ciljem, če ravnajo namerno in z namenom prispevati k nadaljevanju izvajanja terorističnega dejanja ali so seznanjeni z namenom skupine, da stori teroristično dejanje. Nadalje so v zakonu določeni tudi pogoji, načini preiskovanja in ugotavljanja pranja denarja ali povezav oseb s terorizmom.

Leta 2008 je bil sprejet nov Kazenski zakonik, ki zamenjuje prejšnji Kazenski zakonik Republike Slovenije in med drugim tudi na novo ureja kazenske določbe glede terorizma.

7.6 RAZVOJ MEDNARODNEGA POLICIJSKEGA SODELOVANJA

»Policijsko mednarodno sodelovanje zahteva tudi nadzor mednarodne policijske dejavnosti in upoštevanje določil glede uporabe dokazov na sodiščih, uporabe posebnih metod in sredstev in nacionalno koncentracijo pravosodnih, policijskih in vladnih institucij« (Oberstar 2001, 22).

Mednarodno in tudi evropsko povezovanje ter sodelovanje na policijski ravni ni nov pojav. Predvsem na neformalni ravni so se poskusi mednarodnega sodelovanja in povezovanja v okviru Evrope pojavili že konec 19. stoletja, poskusi globalnega povezovanja in sodelovanja pa že na začetku 20. Stoletja, tik pred prvo svetovno vojno. Leta 1923 je bila ustanovljena mednarodna kriminalistična policija – Interpol oz. njegova predhodnica Mednarodna komisija kriminalistične policije. Mednarodno policijsko sodelovanje je med obema svetovnima vojnama precej zamrlo, se je pa ponovno razmahnilo v 60. letih 20. stoletja, in sicer na začetku predvsem s ciljem obvladovanja problemov glede prepovedanih drog, terorizma in organiziranega kriminala. Leta 1975 je bilo izvedeno pomembno srečanje dvanajstih notranjih ministrov članic takratne

Evropske gospodarske skupnosti, ki je leto kasneje povzročilo ustanovitev več delovnih skupin na policijskem področju, s skupnim imenom TREVI[43]. Namen skupine TREVI je bilo predvsem pospeševanje mednarodnega sodelovanja in integracije različnih policijskih organizacij na evropskem prostoru. Nadalje je bil leta 1985 sklenjen sporazum o postopnem ukinjanju nadzora oseb na notranjih skupnih mejah držav podpisnic – Schengenski sporazum, ki se je razširil na nove države podpisnice in ki se je leta 1990 utrdil še s podpisom konvencije o izpeljavi Schengenskega sporazuma. Schengenski sporazum določa tudi številne pomembne izravnalne ukrepe, ki so namenjeni tudi reševanju problematike glede prepovedanih drog, organiziranega kriminala in terorizma. Leta 1990 je bila na predlog skupine TREVI sprejeta odločitev o ustanovitvi Evropske obveščevalne enote za boj proti mamilom (EDU), ki je nekakšen predhodnik sodobnega Europola. Osnovni temelj za ustanovitev Europola je bil sprejet leta 1992 s podpisom Maastrichtske pogodbe, ki med drugim predvideva tudi ustanovitev evropskega policijskega urada – Europola (Celar 1996, 6–10).

Leta 1956 se je dotedanja Mednarodna komisija kriminalistične policije, ki je bila ustanovljena sicer že leta 1923, preimenovala in razširila v Interpol. Interpol sicer ni javnopravna mednarodna organizacija, saj ne temelji na mednarodni pogodbi oz. ni produkt medvladnega sporazuma. Kljub temu ga lahko glede na vsebino njegovega delovanja in glede na način delovanja lahko označimo kot mednarodno nevladno organizacijo (Sluga 1996, 10–119).

Slovenija je polnopravna članica Interpola postala leta 1992. Glavne naloge Interpola so:

- zagotoviti in realizirati največje možno sodelovanje med kriminalističnimi policijami, ne glede na razlike v pravnih sistemih držav in v skladu z deklaracijo o človekovih pravicah,
- vzpostaviti in razvijati vse potrebne ustanove, ki naj z medsebojnim sodelovanjem prispevajo v boju proti kriminalu.

V vsaki posamezni državi članici Interpola je policija zasnovala specifično službo, pod nadzorstvom vlade, da zagotovi in odgovori na vse preiskave oz. operativne zadeve –

[43] Kratica TREVI pomeni Terrorism, Radicalism, Extremism and Violence – International.

zaprosila od lokalnih in tujih policij ter pravosodnih organov. Taka služba se imenuje Nacionalni centralni biro (NCB).

Urad za evropsko pravosodno sodelovanje (Eurojust) je bil s strani Evropske unije ustanovljen leta 2002 in šteje 27 nacionalnih članov, po enega iz vsake države članice Evropske unije. Nacionalni člani so starejši, izkušeni tožilci, sodniki ali policijski uradniki z enakovrednimi pristojnostmi. Pri preiskavah in pregonu, ki zadevajo dve ali več držav članic, si Eurojust prizadeva spodbuditi in izboljšati koordinacijo med organi držav članic. Pri tem upošteva zahtevke pristojnih organov držav članic in informacije, ki jih posreduje katerikoli organ s pooblastili na podlagi pogodb (Evropska pravosodna mreža (EJN), Europol in Evropski urad za boj proti goljufijam (OLAF)). Zavzema se tudi za izboljšanje sodelovanja med pristojnimi organi, zlasti glede zagotavljanja mednarodne vzajemne pravne pomoči in izdajanja evropskih nalogov za prijetje. Med drugim si prizadeva tudi za večjo učinkovitost dela preiskovalnih organov in organov kazenskega pregona, kadar se spopadajo s težjimi oblikami čezmejnega in organiziranega kriminala, kot so terorizem, trgovina z ljudmi, trgovina z drogami, goljufije in pranje denarja, saj je treba storilce kaznivih dejanj čim prej privesti pred sodišče. Eurojust pri izpolnjevanju svojih nalog deluje prek nacionalnih članov ali kot kolegij. Eurojust lahko pristojne organe držav članic zaprosi, da:

- izvedejo preiskavo ali kazenski pregon določenih dejanj;
- soglašajo, da je drug organ lahko v boljšem položaju za izvedbo preiskave ali pregona določenih dejanj;
- se pristojni organi med seboj uskladijo; ustanovijo skupno preiskovalno skupino ali da zagotovijo vse informacije, ki jih skupina potrebuje za opravljanje svojih nalog.

Eurojust je pristojen za medsebojno obveščanje pristojnih organov in zagotavlja najboljše možno usklajevanje in sodelovanje teh organov. Za reševanje pravnih vprašanj in praktičnih težav nudi tudi materialno-tehnično podporo ter pripravlja usklajevalne sestanke med pravosodnimi in policijskimi organi različnih držav (po Agenciji Evropske unije 2011[44]).

[44] Dostopno prek: http://europa.eu/agencies/pol_agencies/eurojust/index_sl.htm

Strnjeno torej lahko rečemo, da se različne represivne ali druge organizacije v okviru Evropske unije ali pa tudi širše v mednarodnem globalnem okviru ukvarjajo predvsem z dejavnostmi, ki omogočajo učinkovitejši boj proti problematiki ekstremnega nasilja ter s tem povezani problematiki organiziranega kriminala in terorizma, ne pa toliko z reševanjem operativnih zadev, kar je še vedno prepuščeno nacionalnim policijam ali drugim represivnim organizacijam. Europol in Eurojust sicer na tem področju poskušata postati izjemi in tako težita tudi k čim večjemu vplivu na izvajanje operativnih nalog. Pri tem so glavne značilnosti vseh zgoraj naštetih organizacij predvsem teženje k poenotenju pojmov oz. definicij pojavnih oblik kriminalitete, poenotenju izvajanja operativnih preiskav, prikritih preiskovalnih ukrepov, zasegov protipravno pridobljenih premoženjskih koristi, usposabljanj in logistične opremljenosti nacionalnih policij ali drugih represivnih organizacij, ki se ukvarjajo z obravnavano problematiko.

Z brisanjem mej v EU in zagotovljeno svobodo gibanja raste potreba po novih, prožnejših ukrepih, ki bodo skrajnežem na internetu preprečili nadaljnje izkoriščanje razlik v pravni ureditvi držav članic. Bolj kot kadarkoli prej je treba pospešiti usklajevanje zakonodaje na področju preprečevanja, odkrivanja in preganjanja storilcev ekstremističnih dejanj ter sodelovanje na policijskem in pravosodnem področju.

Schengenski sporazum uveljavlja primarno načelo, da je notranje državne meje držav pristopnic povsod mogoče prestopiti brez mejnega nadzora. To velja za vse osebe, ne glede na državljanstvo, tako za državljane držav podpisnic, držav Evropske unije ali drugih držav. Pri tem se v okviru Schengenskega sporazuma krepi sodelovanje na političnem, strokovnem in operativnem povezovanju in sodelovanju, še posebej na področjih skupnega čezmejnega nadzora, skupnega čezmejnega pregona, skupne informacijske mreže, v sklopu katere deluje tudi informacijski sistem Schengen (SIS), in skupnih predstavnikov nacionalnih policij za povezavo oz. za operativno sodelovanje (oficirji za zvezo).

V letu 1998 je stopila v veljavo konvencija o Europolu, ki so jo vse države članice ratificirale še istega leta. Evropska unija želi s pomočjo Europola izboljšati predvsem učinkovitost policij posameznih držav članic, zato so med temeljnimi nalogami Europola:

- pospeševanje izmenjave informacij med državami članicami,
- pridobivanje in analiziranje informacij in obveščevalnih podatkov,
- pravočasno posredovanje informacij pristojnim organom držav članic,
- pomoč državam članic pri preiskovanjih kaznivih dejanj,
- vzdrževanje računalniško podprtega informacijskega sistema (Čurin 2003, 26).

7.7 VLOGA EUROPOLA

»Europolova osnovna naloga predstavlja podporo učinkovitejšemu sodelovanju med pristojnimi organi držav članic Evropske unije pri odkrivanju, preiskovanju, preprečevanju ter analiziranju najhujših oblik mednarodnega organiziranega kriminala na območju Evropske unije. V osnovi je namenjen izmenjavi podatkov in podpori nacionalnim organom s policijskimi pooblastili, katerih dejavnost je usmerjena v preprečevanje in odkrivanje organizirane kriminalitete. Med tovrstne organe sodijo predvsem policija, carina, žandarmerija, migracijski organi in službe za preprečevanje pranja denarja« (Farič 2004, 13).

Vsaka država članica Evropske unije mora ustanoviti oziroma določiti nacionalno enoto, ki bo skrbela za izvajanje temeljnih nalog in povezovanje med Europolom in pristojnimi organi v državah članicah. Vsaka nacionalna enota napoti na sedež Europola najmanj enega ''oficirja za zvezo'', ki ga posebej usposobi za uresničevanje njenih interesov znotraj Europola. Vsi podatki v informacijskem sistemu so neposredno dostopni nacionalnim enotam, oficirjem za zvezo, direktorju in njegovim pomočnikom ter izbranim uradnikom Europola. Naloge nacionalnih enot so:

- tekoče oskrbovanje Europola z informacijami in podatki, potrebnimi za nemoteno izvajanje njegovih nalog,
- posredovanje informacij in podatkov, ki jih zahteva Europol,
- shranjevanje informacij in podatkov do določenega obdobja,
- vrednotenje informacij in podatkov z vidika nacionalne zakonodaje in njihovo posredovanje pristojnim organom,

- posredovanje zahtev Europolu za svetovanje, informacije, podatke in analize,
- posredovanje informacij in podatkov Europolu za njegov informacijski sistem,
- zagotavljanje skladnosti posredovanja vseh informacij in podatkov med nacionalnimi enotami in Europolom z nacionalno zakonodajo.

Na podlagi navedenega je razvidno, da organi Evropske unije sprejemajo zavezujoče politične odločitve v smeri harmonizacije kazenske zakonodaje in vzpostavitve pravnega sistema, ki pomeni temelj skupni strategiji policijskih dejavnosti in organizacije. Na tem področju so ključni trije pomembni in med seboj povezani procesi:

- države izgubljajo monopol na področju kazenskega pregona, del odgovornosti in dejavnosti prenašajo na raven nadnacionalnih in medvladnih struktur Evropske unije,
- od transnacionalnega sodelovanja na področju kazenskega pregona pričakujejo praktične rezultate,
- čeprav je težnja po globalizaciji na področju kazenskega pregona jasno razvidna, ostaja večina stikov med policijami na področju prehajanja državne meje na bilateralni in zgolj informativni ravni (Čurin 2003, 26–28).

Preko Europola, kot tudi preko ostalih ustanov Evropske unije, se poskuša tako na nacionalne pravne rede in policijske organizacije držav članic vplivati na določenih področjih, ki lahko pomembno prispevajo k učinkovitejšemu boju proti organiziranemu kriminalu ter s tem povezanemu ekstremizmu. Ta področja so zlasti:

- poenotena opredelitev organiziranega kriminala,
- zaseg in hramba zaseženega premoženja,
- poenotenje izvajanja in uporabe posebnih metod in sredstev ter
- zaščita prič in skesancev (Čurin 2003, 65).

Pri preiskovanju kriminalitete, pri kateri se kot pripomoček uporablja internet, je zelo pomembno tudi mednarodno sodelovanje (Projekt Check the Web). Pri tem ima pomembno vlogo Europol, ki poleg hitre in neovirane izmenjave potrebnih informacij državam članicam s svojim analitičnim računalniškim sistemom in veliko bazo podatkov v njem zagotavlja tudi operativno analitično oporo pri preiskovanju konkretnih primerov in

z analizo določenih pojavnih oblik kaznivih dejanj išče najboljše preiskovalne prakse ter s tem pripomore k poenotenju preiskovalnih tehnik v državah članicah (Potparič 2006).

7.7.1 PROJEKT CHECK THE WEB

Projekt "Check the Web" je nastal na pobudo Nemčije, sprejela ga je delovna skupina za terorizem v okviru Sveta EU (Terrorism Working Group – TWG). V pobudi je poudarjen pomen medsebojnega sodelovanja držav članic v boju proti uporabi interneta v teroristične namene[45].

Glavne smernice pobude so:
1. Internet ima zelo pomembno vlogo pri komunikacijskem, logističnem in operativnem povezovanju terorističnih organizacij. Teroristi ga ne uporabljajo zgolj kot medij za komuniciranje in propagando, ampak tudi za radikalizacijo, novačenje in urjenje teroristov, širjenje navodil za storitev specifičnih kaznivih dejanj, prenos informacij ter za namene financiranja teroristov.

Eden izmed glavnih ciljev EU je spoprijeti se z internetom kot nosilcem radikalizacije in novačenja teroristov. Preprečitev radikalizacije in novačenja morebitnih teroristov je eden izmed temeljnih stebrov boja proti terorizmu. Temu ustrezno so v strategiji in akcijskem načrtu za boj proti radikalizaciji in novačenju za terorizem (dokument 14781/1/05 in dokument 14782/05) predvideni ukrepi za boj proti uporabi interneta v teroristične namene.

Cilj pobude "Check the Web" je okrepiti sodelovanje in delitev nalog spremljanja in ocenjevanja odprtih internetnih virov na prostovoljni bazi. Na področju usklajenega spremljanja in ocene islamskih terorističnih spletnih strani v okviru projekta "Check the Web" je izvedenih že vrsta uspešnih preiskav. Informacijski portal Europola je ključnega pomena za medsebojno sodelovanje držav članic.

[45] Projekt Check the Web je opredeljen v dokumentih EU številka 9496/06 ENFOPOL 96 JAI 261 in 16532/1/06 ENFOPOL 219 in 8457/3/07 REV 3.

Europol gradi informacijski portal kot tehnično platformo za izmenjavo informacij med državami članicami. Vsebuje naslednje module, za katere bodo države članice zagotavljale podatke in do katerih bodo imele dostop vse države članice:

- kontaktne osebe za krepitev mreže strokovnjakov; seznami povezav za spremljanje spletnih mest za medsebojno informiranje;
- dodatne informacije (posebno znanje jezikov v posameznih državah članicah, tehnično znanje, možnosti uporabe pravnih sredstev zoper teroristična spletna mesta), da se omogoči delitev virov;
- seznam sporočil terorističnih organizacij za lažje združevanje virov;
- rezultati ocen, da se izognemo podvajanju dela.

Z vzpostavitvijo informacijskega portala se je znatno povečala kakovost medsebojnega sodelovanja držav članic pri spremljanju in ocenjevanju islamskih terorističnih spletnih strani. Portal zagotavlja platformo, kjer si države članice izmenjujejo informacije in tako zbirajo znanje v okviru EU. Države članice bodo imele neposreden in hiter dostop do informacij o delu drugih držav članic in njihovih rezultatov. V nujnih primerih se lahko vzpostavi neposredni stik, sodelovanje pa se uskladi prek seznama nacionalnih kontaktnih oseb. Poleg tega so bili storjeni že prvi koraki za okrepitev prostovoljnega sodelovanja po načelu delitve dela med zainteresiranimi državami članicami.

Sodelovanje prek informacijskega portala dopolnjujejo redna srečanja strokovnjakov. Države članice so začele izvajati skupne projekte. Nekatere države članice pod vodilno vlogo nemških varnostnih organov skupaj analizirajo Al Kaidin oddelek za medije, "As-Sahab".

7.8 DELOVANJE DRUGIH EVROPSKIH INŠTITUCIJ

»Dejavnost evropskih policij konec 20. stoletja je bila podrejena zlasti združevanju v enotno tvorbo. Smisel tovrstnega povezovanja je bil v doseganju enakopravnega položaja v primerjavi z organiziranim kriminalom, čigar povezave presegajo nacionalne okvire« (Pečar 1994, 104).

Maastrichtski sporazum ali pogodba o Evropski uniji, podpisana februarja leta 1992, je zaznamovala novo obdobje v procesu oblikovanja vse tesnejše zveze med državami

Evropske unije in s tem naredila korak k oblikovanju Evropske unije kot politične tvorbe. Na podlagi omenjene pogodbe si je Evropska unija kot enega od ciljev zastavila tudi razvijanje tesnega sodelovanja na področju pravosodja in notranjih zadev. Države članice so si enotne, da so določena področja pravosodja in notranjih zadev obravnavana kot zadeve skupnega interesa. Nadaljnji korak k oblikovanju skupne evropske varnostne politike se odraža v Amsterdamski pogodbi, podpisani leta 1997, uveljavljeni leta 1999, ki vnaša obsežne vsebinske in formalnopravne spremembe pogodb, na katerih temelji Evropska unija. V Amsterdamsko pogodbo sta s protokoli vključena tudi Schengenski sporazum in Konvencija o izpeljavi Schengenskega sporazuma, kar pomeni, da je Schengenski sporazum postal del pravnega reda Evropske unije. Policijsko in sodno sodelovanje v kazenskih zadevah naj bi kot drugi del tretjega stebra postala bolj učinkovita. V ospredju je predvsem preprečevanje in boj proti organiziranemu kriminalu, terorizmu, trgovini z ljudmi, boj proti trgovini s prepovedanimi drogami in orožjem, podkupovanjem in goljufijami. Podlaga je intenzivnejše sodelovanje med policijo, carino, pravosodjem in drugimi pristojnimi organi držav članic, posebna pooblastila pa so podeljena Europolu. Prav tako so razširjene pristojnosti Evropskega sodišča, v večji meri se v odločitve vključujeta Evropski parlament in Evropska komisija. Sporazum, sklenjen v Nici decembra leta 2000, posega v urejanje odnosov, predvsem na institucionalni ravni. Ti niso bili doseženi z Amsterdamsko pogodbo, ampak so se morali urediti s procesom širitve Evropske unije (Čurin 2003, 22–25).

S postopnim uveljavljanjem temeljnih načel Evropske unije, ki se odražajo v zahtevah po pretoku blaga, storitev in kapitala ter svobodi gibanja ljudi, se nedvomno spreminja značaj družbenih okolij – oblikovanje globalne družbe, ki pa žal s seboj prinaša tudi slabosti. Ta določila enotnega trga in ukinitev nadzora na državnih mejah odpirajo pot raznoterim oblikam kriminalitete. Širi se kriminalna dejavnost, ki prestopa regionalne ali nacionalne okvire, nastajajo transnacionalne kriminalne organizacije, ki obvladujejo različna področja kriminalnih dejavnosti, s tem pa "varnostno ogrožajo" države članice Evropske unije. To je spodbudilo ukrepe za oblikovanje različnih delovnih skupin in pripravo posameznih projektov ter sporazumov, ki naj bi zavrli ali preprečili potencialne oblike ogrožanja skupnosti, v nadaljnjem procesu izgradnje skupne varnostne politike pa

so postali sestavina pravnega reda Evropske unije na področju pravosodja in notranjih zadev (Jeglič 2001, 28–29).

Glede na to, da je Slovenija polnopravna članica Evropske unije, je kot taka tudi del evropskega varnostnega sistema. Evropski pravni sistem se v okviru evropske varnostne politike določa in izvaja deloma preko evropskih institucij, deloma pa preko nacionalnih varnostnih politik in ustanov ter organov vseh držav članic Evropske unije. Kot pomembnejše oblike izvajanja evropske varnostne politike lahko omenimo uvedbo in vzdrževanje t. i. schengenskega območja prostega gibanja oseb, blaga in storitev ter s tem povezanih varnostnih ukrepov, izvajanje skupne evropske obrambne in zunanje politike ter na področju terorizma izvajanje Strategije EU za boj proti terorizmu.

7.8.1 STRATEGIJA BOJA PROTI TERORIZMU

Strategija pomeni strateško zavezo bojevati se proti terorizmu na svetovni ravni in obenem spoštovati človekove pravice in napraviti Evropo varnejšo, s čimer bi državljanom omogočili, da živijo v svobodi, varnosti in pravici.

- Terorizem je grožnja vsem državam in vsem narodom. Z nepremišljenim napadanjem nedolžnih ljudi resno ogroža našo varnost, vrednote naših demokratičnih družb ter pravice in svoboščine naših državljanov. Terorizem je kaznivo dejanje in pod nobenim pogojem ni upravičen.
- Evropska skupnost je območje naraščajoče odprtosti, kjer sta notranji in zunanji vidik varnosti tesno povezana. Je območje naraščajoče soodvisnosti, ki omogoča prosti pretok oseb, idej, tehnologije in virov. To je okolje, ki ga teroristi za dosego svojih ciljev zlorabljajo. V tem smislu je usklajeno in enotno evropsko ukrepanje v boju proti terorizmu nujno.
- Štirje stebri strategije EU za boj proti terorizmu – preprečevanje, zaščita, onemogočanje, odzivanje – predstavljajo celovit in sorazmeren odziv na mednarodno teroristično grožnjo. Strategija zahteva delo na nacionalni in evropski ravni, da bi zmanjšali grožnjo terorizma in našo ranljivost za napad. Strategija določa naše cilje, da bi preprečili novačenje k terorizmu; bolje zaščitili

morebitne tarče; onemogočili obstoječe mreže in izboljšali našo sposobnost, da se odzovemo na posledice terorističnih napadov in z njimi upravljamo.

- Skupna značilnost vseh štirih stebrov strategije Unije je vloga Unije v svetu. Z zunanjimi ukrepi Evropska unija prevzema odgovornost, da prispeva k globalni varnosti in gradi varnejši svet. S pomočjo Združenih narodov in v sodelovanju z njimi ter drugimi mednarodnimi in regionalnimi organizacijami bo skušala EU doseči mednarodno soglasje in spodbuditi mednarodne standarde za boj proti terorizmu. Dialog s ključnimi državami partnericami, vključno z ZDA, bo prav tako osrednji del evropskega pristopa. Glede na to, da sedanja mednarodna teroristična grožnja preti in izvira v veliko delih sveta zunaj EU, je sodelovanje s tretjimi državami, ki se obravnavajo prednostno – vključno s severno Afriko, Bližnjim vzhodom in jugovzhodno Azijo – ključnega pomena; enako tudi zagotavljanje pomoči tem državam. Ne nazadnje so reševanje sporov in spodbujanje dobrega vodenja in demokracije ključni elementi strategije, da bi lahko obravnavali motivacijske in strukturne dejavnike podkrepljene radikalizacije.

Strategija EU za boj proti terorizmu obsega štiri osi dejavnosti, ki spadajo pod isto strateško zavezo:

7.9 FILTRIRANJE INTERNETA

Hiter razvoj interneta je bil presenečenje tako za pravo kot za etiko. Pomanjkljivo in neprilagojeno regulacijo so nadomeščala tehnična pravila in odločitve gospodarjev informacijskih sistemov (državna uprava, vojska in korporacijski menedžment). Tudi očetje interneta so bili prepričani, da ga bodo vselej lahko urejali le s tehničnimi pravili. Toda problemi so se kopičili in postalo je očitno, da jih brez ustreznega normiranja ne bo mogoče razrešiti (Pivec 2004, 162).

Uporabniki interneta so bili v preteklosti prepričani, da je internet zaradi svojih lastnosti že po svoji naravi odporen proti nadzorovanju države, danes ga različne zakonodaje obvladujejo čedalje bolj, državni organi in podjetja pa odkrivajo privlačnost nadzorovanja po internetu. Popolna neregulacija s strani države bi dopuščala možnost večjih zlorab, ki so se pojavile z računalniškim kriminalom.

Internet omogoča posamezniku, da dobi informacijo o istem dogodku iz več različnih virov. Posameznik lahko zbira in analizira informacije, ki sicer v njegovem okolju niso zaznane. Za določene svetovne voditelje to pomeni, da lahko uporabniki računalniških

komunikacijskih sistemov javno izpostavljajo vsakodnevne probleme humanosti, kot so na primer človekove pravice in svoboščine, onesnaževanje okolja ipd. Ravno zaradi svobodne internetne komunikacije se nekaterim zaprtim političnim sistemom zdi smiselno cenzurirati internet ali zbirati podatke, katere spletne strani obiskujejo posamezniki.

Danes obstaja kar nekaj držav, ki z elektronskimi ovirami omejujejo dostop do nekaterih spletnih strani. Najpogosteje se omenja Kitajsko, Uzbekistan, Egipt, Tunizijo, Libijo, Jemen, Iran, Severno Korejo in Vietnam. Gre za kršenje svobodnega pretoka informacij, ker preprečujejo ljudem dostop do delov svetovnih omrežij. Države, ki omejujejo dostop do interneta, niso deležne nikakršnih sankcij, razen obsodb drugih držav, ker proti cenzuriranju sankcije niso nikjer opredeljene.

Zanimiv je primer iz Turčije. Leta 2007 je turški parlament sprejel široko zakonodajo, ki je sodiščem omogočala blokado katerekoli spletne strani, pri kateri je obstajal "zadosten sum", da se je zgodilo kaznivo dejanje širjenja otroške pornografije, iger na srečo, prostitucije ali "zločina zoper Ataturka". Na podlagi zakona je v času med letoma 2007 in 2010 Turčija uvedla blokado dostopa do spletne strani YouTube. Prepoved strani je bila uvedena zaradi objavljanja vsebin, ki naj bi žalile ustanovitelja države, Mustafo Kemala Ataturka. Posnetke, ki so povzročili prepoved, so objavili Grški uporabniki in naj bi Ataturka in Turke označevali za homoseksualce.

Nekatere države, denimo Nemčija, so uvedle blokado spletnih strani, ki vsebujejo otroško pornografijo. V skladu z dogovorom se je pet najmočnejših ponudnikov interneta v Nemčiji – Deutsche Telekom, Vodafone/Arcor, Hanse Net, Telefonica O2 in Kabel Deutschland – zavezalo, da bodo svojim strankam onemogočili dostop do spletnih strani, ki vsebujejo otroško pornografijo. Osvežene sezname spornih strani naj bi podjetjem redno posredoval nemški zvezni urad za boj proti kriminalu (BKA).

8 ZAKLJUČEK IN VERIFIKACIJA TRDITEV

Ekstremistične skupine sicer uporabljajo internet kot podporo tradicionalnim oblikam ekstremizma. Vzpostavljajo spletne strani, ki širijo njihove politične ali družbene cilje, pridobivajo nove člane, med seboj komunicirajo ipd. Internet uporabljajo kot orodje za dostop do množičnih medijev. Z internetom pridobivajo simpatizerje in s tem širši izbor posameznikov, ki so pripravljeni tudi na izvajanje ekstremističnih dejanj.

Preiskovanje internetnega kriminala in ekstremizma je povezano s številnimi problemi. Prvi problem je ravnanje z računalniškimi sistemi in računalniško opremo. Kompleksnost te vrste orodij laikom in tudi preiskovalcem, ki niso strokovno usposobljeni, z računalniško tehniko in programi onemogoča spopadanje s to vrsto kriminala in terorizma. Spremljati in ocenjevati je treba številne spletne strani v različnih jezikih, za kar so potrebna zajetna tehnična sredstva in človeški viri. Zaradi ogromnega števila spletnih strani prihaja tako na nacionalni kot na mednarodni ravni do težav glede količine in kakovosti preiskovalcev, zlasti v zvezi s potrebnim znanjem jezikov. Preiskovalci v posamezni državi skorajda ne morejo spremljati vseh sumljivih in z ekstremizmom povezanih dejavnosti na internetu. Spremljanje in ocenjevanje interneta bi bilo torej treba okrepiti tako, da bi pri tej nalogi sodelovali na mednarodni ravni, pri tem pa upoštevali posebne jezikovne in strokovne usposobljenosti varnostnih agencij posameznih držav. Poleg izmenjave informacij prek Europola se lahko države članice odločijo, da si bodo prostovoljno razdelile delo in tako dosegle čim bolj učinkovito uporabo virov.

Če preprečevanje računalniškega kriminala na mednarodni ravni ne bo usklajeno in ratificirano z nacionalnimi zakoni, bodo še vedno prisotne ovire za odkrivanje računalniških kriminalcev in vse to bo vodilo k nastajanju skrivališč računalniških kriminalcev, v katerih bodo ti nad zakonom in imuni na kakršnokoli kaznovanje. Na nacionalni ravni je nujno treba utrditi osnove zaščite v skladu z mednarodnimi standardi in smernicami.

Internet omogoča anonimnost posameznika, kar otežuje identifikacijo storilca. Internetni kriminal postaja pereč problem zaradi decentralizirane narave interneta, anonimnosti

nadlegovalcev, množice osebnih podatkov o nekem posamezniku na spletnih straneh, neustrezne zakonodaje, ki povečini ni dovolj natančna na tem področju nima univerzalno veljavne definicije tega pojma. Vse to istočasno otežuje odkrivanje in kazensko preganjanje storilca tovrstnega kriminalnega dejanja.

Z razvojem interneta je svoboda izražanja dobila nov, širši pomen. Zaradi enostavne uporabe in široke dostopnosti je internet idealen medij za vzpostavitev večje komunikacijske svobode, tako pri sporočanju med dvema osebama kot tudi v komuniciranju z najširšo svetovno javnostjo, kar na žalost izkoriščajo tudi teroristične organizacije.

Prvo hipotezo lahko potrdim: **Internet vpliva na razvoj ekstremističnih idej pri posameznikih, ki s pomočjo interneta iščejo somišljenike. Ekstremistične skupine internet uporabljajo predvsem za predstavitev svojih ciljev, financiranje in pridobivanje novega članstva, in ne za napade na internetno infrastrukturo**. Ekstremistične skupine lahko zelo učinkovito uporabljajo internet za dostop do množičnih medijev. To je njihov način, da s skromnim znanjem, cenovno dostopno in minimalno informacijsko tehnologijo same pošljejo sporočila v javnost. Število sporočil na internetu se stalno povečuje. Ekstremisti uporabljajo vse prednosti, ki jih internet ponuja: takojšnjo svetovno razširjenost, anonimnost pošiljatelja in možnost promoviranja svojih organizacij, kar je pripeljalo k vedno večji rekrutaciji "borcev". Preko spleta zbirajo tudi dobrodelne prispevke. Pozivi separatističnih skupin, grožnje terorističnih skupin, kraj in način demonstracij levih ekstremističnih skupin ter parole desnih ekstremističnih skupin – vse to se z bliskovito hitrostjo prek spleta širi med internetnimi uporabniki.

Tudi drugo hipotezo lahko potrdim: **Slovenska zakonodaja zagotavlja pogoje, ki omogočajo preiskovanje kaznivih dejanj, storjenih s pomočjo interneta. Pretekle izkušnje so pripomogle k nadgradnji izvajanja preiskav, preiskovalci so pridobili nova tehnična znanja in začeli uporabljati nova tehnična sredstva. Slovenska zakonodaja se ustrezno prilagaja novim trendom izvrševanja kaznivih dejanj preko interneta.**

Tudi slovenska kazenska zakonodaja se odziva na kibernetsko kriminaliteto kot eno izmed perečih novodobnih oblik kriminala. Ratifikacija Konvencije o kibernetski kriminaliteti je našo državo zavezala k izrecni inkriminaciji nekaterih dejanj s področja kibernetskega kriminala ter k sprejetju nekaterih ukrepov, ki olajšujejo odkrivanje kibernetskih kaznivih dejanj, torej kaznivih dejanj, ki so storjena z zlorabo interneta in/ali računalniške tehnologije.

Ugotovimo lahko, da je tudi pravna ureditev preiskovanja kaznivih dejanj z elementi ekstremizma v Sloveniji kakovostno primerljiva s standardi, ki jih priporoča Evropska unija. Slovenija je ratificirala večino pomembnejših mednarodnih dokumentov. S sklenitvijo bilateralnih sporazumov in reformo kazenske zakonodaje, ki je prinesla modernejše oblike boja proti storilcem najhujših kaznivih dejanj, je Slovenija naredila nove korake k učinkovitemu izvajanju teh mednarodnih dokumentov. Slovenska zakonodaja je naredila velik napredek pri omogočanju pogojev za učinkovit razvoj preiskovanja kaznivih dejanj ekstremizmov na internetu. Predvsem gre za preiskovanje sovražnega govora. V tem delu ji sodna praksa še ni sledila; sovražni govor na internetu sicer razume, ne zna pa ga ustrezno sankcionirati.

Preiskovalni organi, tožilstva, sodišča in zakonodaja morajo zastaviti strategije za reševanje in preiskovanje ekstremizmov na internetu. Čeprav so države glede tovrstne problematike že zelo veliko naredile, pa kljub napredku veljavna zakonodaja ne more slediti tehnološkemu razvoju, prav tako pa ne more v korak z ekstremizmi, ki so lahko povzročeni preko interneta.

9 LITERATURA

1. Alkalaj, Mišo. 2008. Kdo je pravi terorist?. *Mladina*. Dostopno prek: http://www.mladina.si/tednik/200203/clanek/rogue/index.print.html-l2. (22. novembra 2009)
2. Alter, Peter. 1991. Kaj je nacionalizem? Zbornik: *Študije o etnonacionalizmu*. Narodna in univerzitetna knjižnica Ljubljana.
3. Anžič, Andrej. 1997. *Varnostni sistem Republike Slovenije*. Ljubljana: Časopisni zavod Uradni list RS.
4. Banovič, Zoran. 2007. Stopiti na prste kiberkriminalcem. *Moj Mikro*. Dostopno prek: http://www.mojmikro.si/preziveti/varnost/stopiti_na_prste_kiber_ kriminalcem (15. novembra 2010).
5. Barrett, Shawn. 1998. Investigation Computer Crime. *The Police Chief, May*: 28–35.
6. Baylis, John. 2008. Mednarodna in globalna varnost. V *Globalizacija svetovne politike*, ur. John Baylis, Steve Smith in Patricia Owens, 24–15. Ljubljana: FDV.
7. Berners-Lee, Tim. 2000. *Weaving the web: The Original Design and Ultimate Destiny of the World Wide Web*. HarperCollins Publishers.
8. Blanchard, Christoper. 2004. *Al Qaeda: statement and Evolving Ideology. Foreighn Affairs, defense, and Trade Division*. Dostopno prek: http://www.fas.org/irp/crs/RS21973.pdf. (10. januarja 2011).
9. Blažina, Bruno, intervju z avtorjem. Ljubljana 24. decembra 2010.
10. Bogataj Jančič, Maja, Boštjan Makarovič, Janez Toplišek, Goran Klemenčič, Klemen Tičar. 2007. *Pravni vodnik po internetu*. Ur. Boštjan Makarovič in Janez Toplišek. Ljubljana: GV Založba.
11. Borum, Randy. 2007. *Psychology of terrorism*. Tampa: University of South Florida. Dostopno prek: http//www.ncjrs.gov/pdffiles1/nij/grants/208552.pdf (16. decembra 2010)
12. Boyd, Danah in Nicole Ellison. 2007. Social network sites: Definition, hystory and scholarship. Journalof Computer-Mediated Communication 13 (1). Dostopno prek: http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html (4. aprila 2011).

13. Brand, Urlich in Joachim Hirsch. 2004. In search of Emancipatory Politics: The resonances of Zapatism in West Europe. *Antipode* 36 (3): 371–382.
14. Buzan, Barry. 1991. *People, States, and Fear: An Agenda for International Security Studies in the Post-Cold War Era*. New York, London, Toronto, Sydnes, Tokyo, Singapore: Harvester Wheatsheaf.
15. Celar, Branko. 1996. *Mednarodno policijsko sodelovanje v luči evropskih integracijskih procesov*. Ministrstvo za notranje zadeve Republike Slovenije, Ljubljana.
16. Ceresa, Alessia. 2005. The Imapct of »new tehnology« on the Red Brigades Italian Terrorist organisation: Thre progressive modernisation of a terrorists movement active in Italy since 1970. *European Journal on a Criminal Policy and Research* 11 (2): 193–222.
17. Cralley, William in Andrew Garfield. 2004*. Lessons of the Past – Indicator for the Future*. Alexandria: Institute For defence Analyses.
18. Černigoj, Albert, intervju z avtorjem. Ljubljana 24. decembra 2010.
19. Čurin, Sandi. 2003. Obvladovanje sprememb na področju »pravosodja in notranjih zadev – organiziran kriminal«. P*ridružitveni proces Slovenije k Evropski uniji*. Univerza v Ljubljani, Ekonomska fakulteta, Ljubljana, 2003.
20. Dalghern, Peter. 1991: Communication and Citizenship. *Journalism and the Public Sphere, Introduction*: 1–24.
21. Day, J. F. Richard. 2005. *Gramschi is Dead: Anarchist Currents in the Newest Social Movements*. London: Pluto Press.
22. Dobovšek, Bojan. 2007. Organizirana kriminaliteta, prepovedane droge in narkoterorizem. *Poročilo s področja prepovedanih drog v Republiki Sloveniji*, Inštitut za varovanje zdravja, Ljubljana.
23. Dolinar, Ksenija. 1998. *LEKSIKON Cankarjeve založbe – dopolnjena 5. izdaja,* 1078. Ljubljana: Cankarjeva založba.
24. Dovč, Danica. 2005. *Uporaba oblik informacijskega bojevanja v sodobnem terorizmu: primer teroristične organizacije PKK*. Ljubljana: Fakulteta za družbene vede.
25. Erjavec, Karmen in Melita Poler Kovačič. 2007. *Kritična diskurzivna analiza novinarskih prispevkov*. Ljubljana: Fakulteta za družbene vede.

26. Erten, Nejc. 2009. *Prikrite preiskave in zasebnost*. Ljubljana: Fakulteta za varnostne vede
27. Europol. 2003. High Tech Crimes Center: *Computer – related Crime within the EU: Old Crimes new tools, new Crimes new Tools*. e. Europol
28. Europol. 2007. High Tech Crimes Within the EU: *Old Crimes new tools, new Crimes new Tools*. Threat Assesment 2007. High Tech Crime Centre. Europol
29. Farič, Marjan. 2004. Slovenija, polnopravna članica Europola. *Varnost* 4, 16–17, Ministrstvo za notranje zadeve Republike Slovenije, Ljubljana.
30. Gatlung, Johan. 2002. On Causes of Terrorism and their Removal. V *Enciclopaedia of International Terrorism 1 – Terrorism: hystory and development*. Ur. Verinder Grover, 37–48. Deep & Deep Publications, New Delhi.
31. Gelbart, Ivan, intervju z avtorjem. Deen Haag, 15. septembra 2010.
32. Graboski, Peter in Russel SMITH. 1998. *Crime in the Digital Age*. New Jersey: Transaction Publishers.
33. Graeber, David. 2002. The New Anarchists. *New Left Rewiew* 13. dostopno prek: http://www.newleftreview.org/?page=article&view=2368 (15. novembra 2010)
34. Grandič, Dejan. 2007. *Sorazmernost pri prikritih preiskovalnih ukrepih*. Fakulteta za podiplomske državne in evropske študije, Brdo pri Kranju.
35. Grizold, Anton. 1998. Institucionalizacija zagotavljanja mednarodne varnosti. V *Perspektive sodobne varnosti*, ur. Anton Grizold, 1–15. Ljubljana: FDV.
36. Gustains, Justin. 2002. Ku Klux Klan. *Find Articles*. Dostopno prek: http://findarticles.com/p/articles/mi_g1epc/is_tov/ai_2419100688/ (10. januarja 2011)
37. Hohler, Beti. 2005. Problem definicije terorizma, *Pravna praksa* 33, 6–15.
38. Jakopič, Kaja. 2005. *Boj proti sovraštvu na medmrežju ali boj z mlini na veter*. Dostopno prek: http://mediawatch.mirovni–institut.si/bilten/seznam/24/watch/ (10. maja 2010).
39. Jakša, Urban. 2009. Izumljene tradicije zamišljenih skupnosti. *V Ustroj nacionalizem*, ur. Samo Bohak. Maribor: Zofijini ljubimci – društvo za razvoj humanistike. Dostopno prek: http://www.zofijini.net/Ustroj7.pdf.

40. Jakulin, Vid. 1996. *Kazenskopravni vidiki računalniškega piratstva*. Ljubljana: Podjetje in delo.
41. Jeglič, Peter. 2001. Skupni evropski prostor svobode, varnosti in zakonitosti. *Slovenska uprava*. 2001, let. 1, št. 1, Ministrstvo za notranje zadeve Republike Slovenije, Ljubljana, str. 27–29.
42. Jones, Steven G. 1995. 'Understanding community in the information age.' Pp. 10-35 V *Cybersociety: Computer Mediated Communication and Community*, edited by S. G. Jones. Thousand Oaks, CA: Sage.
43. Juris, S. Keffrey. 2005. The new Digital Media and Activism Networking within Anti- Corporative Globalization Movements. *The Annals of the American Academy of Political and Social Science*. 597 (1): 189–208.
44. Kastelic, Toni. 2005. *Elektronsko poslovanje in računalniški kriminal*. Diplomsko delo. Ekonomsko – poslovna fakulteta, Maribor.
45. Kastelic, Toni. Računalniški kriminal v Sloveniji. Kiberpipa. Dostopno prek: http://video.kiberpipa.org/media/POT_Racunalniski_kriminal_v_Sloveniji/play.html. (17. oktobra. 2010).
46. Kastelic, Toni, intervju z avtorjem. Ljubljana, 17. decembra 2010.
47. Karakaš, Aleksander. 2000. Uporaba posebnih (preiskovalnih) metod in sredstev v kazenskem postopku. V *Uveljavljanje novih institutov kazenskega materialnega in procesnega prava*, ur. Ljubo Bavcon, 261–279. Uradni list, Ljubljana, str. 261.
48. *Kazenski zakonik Slovenije*. Ur. list RS, 63/94, 70/94, 23/99, 40/2004, 55/2008, 77/09.
49. Kiš, Danilo. 1978 *Čas anatomije*. Beograd: Nolit.
50. Klemenčič, Goran. 2001. Temeljne pravice: Veliki Brat na vašem računalniku. *Pravna praksa* 32: 11.
51. Klemenčič, Goran. 2007. *Nekateri pravni vidiki zaščite zasebnosti uporabnikov informacijskih sistemov*. Fakulteta za policijsko-varnostne vede, Ljubljana.
52. Knight, Alan in Kasun Ubayasiri. 2005. *E-Terror: Journalism, Terrorism and the Internet.* Dostopno prek: http://ejournalist.com.au/v2n1/alkas.pdf (10. januarja 2011)

53. Korošec, Damjan in Ljubo BAVCON. 2003. *Mednarodno kazensko pravo – Posebni del.* Ljubljana: Pravna fakulteta.
54. Kovačič, Blaž. 2001. Pravni vidiki sovražnega govora. V *Poročilo skupine za spremljanje nestrpnosti* 01, ur. Brankica Petkovič, 177–198. Ljubljana: Mirovni inštitut.
55. Kovačič, Matej. 2006. Tehnične rešitve za zaščito posameznika na internetu. V *Računalniška/kibernetična kriminaliteta v Sloveniji,* ur. Nina PERŠAK, 241–254. Ljubljana: Inštitut za pravno kriminologijo pri Pravni fakulteti v Ljubljani.
56. Križanič, Rastko. 2010. *WEB 2.0*. Dostopno prek: http://www.rastko.cc/?p=81 (4. februarja 2011).
57. Kučić, Lenart. 2010. Konec skrivnosti. *Delo, Sobotna priloga*. (3. julij).
58. Laudon, C. Kenneth in Jane Price Laudon. 2006. Management Information Systems. *Managing the digital firm*. Ninth edition. New Yersey: Prentice Hall.
59. Lassen, Helena. 2008. *Nacionalizem in kultura. Primer filma Emirja Kusturice*. Ljubljana: Fakulteta za družbene vede.
60. Leigh, David. 2010. *Iraq War Logs: An Introduction*. Dostopno prek: http:// www.guardian.co.uk/world/2010/oct/22/iraq-war-logs-introduction (5.aprila 2011)
61. Leskošek, Vesna. 2005. Sovražni govor kot dejanje nasilja. V *Mi in oni: nestrpnost na Slovenskem*, ur. Vesna Leskošek, 81–95. Ljubljana: Mirovni inštitut.
62. Linstroth, John. 2002. *The Basque Conflict Globally Speaking. Media and Basque Identity in the Wider World*. London: Carfax Publishing. Oxford Development Studies.
63. Macmaster, Neil. 2004. *Racism: a »mutating bacillus« - islamphobia, antisemitism and »cultural« racism as new challenges in our societes*. Strasbourg: ECRI.
64. Martin, Gus. 2003. *Understanding Terrorism: Challenges, Perspectives, and Issues*. Thousand Oaks: Sage Publications. Inc.
65. Medosch, Amin. 2002. Hacktivism – political Activism on the Net or: Why we have to protect the net as a public sphere. *Transnational Radical Party*. Dostopno prek:

http://servizi.radicalparty.org/documents/index.php?func=detail&par=54 (27. novembra 2010).

66. *Mednarodna konvencija za preprečevanje financiranja terorizma*. Ur. list RS 21/2004.
67. *Microsoft*. 2004. Kaj morate vedeti o Pishingu. Dostopno prek: http://www.microsoft.com/slovenija/doma/varnost/spam/phishing.mspx (3. januarja 2011).
68. Oddelek za protiteroristično dejavnost in ekstremno nasilje GPU UKP (2005). *Organiziranost in dejavnost Oddelka za terorizem in ekstremno nasilje*. Arhiv GPU UKP.
69. Oberstar, Jože. 2001. Boj proti nezakoniti trgovini z mamili in terorizmu: temeljni dokumenti in njihov pomen za policijsko delo. *Pravna praksa – priloga*. let. 20, št. 7, GV založba, Ljubljana, str. 1–32.
70. Oblak, Tanja. 1997. *Družbeni kontekst komunikacijskih tehnologij: podobe »kibernetske družbe« v znanstvenem in popularnem diskurzu*. Magistrska naloga. Ljubljana: FDV.
71. Paolo Alto, Calif. 2010. Wikileaks, Julian Assange, and the dark side of Internet freedom. *The Christian Science Monitor*. Dostopno prek: http://www.csmonitor.com/Commentary/Global-Viewpoint/2010/1207/WikiLeaks-Julian-Assange-and-the-dark-side-of-Internet-freedom. (9. januarja 2011).
72. Pečar, Janez. 1994. Kriminaliteta in Europol. *Revija za kriminalistiko in kriminologijo.* 1994, let. 45, št. 2, Ministrstvo za notranje zadeve Republike Slovenije, Ljubljana, str. 103–112.
73. Peršak, Nina. 2006. Pravno in sistemsko odzivanje na računalniško in kibernetično kriminaliteto. V: PERŠAK, Nina (ur.*). Računalniška/kibernetična kriminaliteta v Sloveniji*. Ljubljana: Inštitut za pravno kriminologijo pri Pravni fakulteti v Ljubljani.
74. Petrovec, Dragan. 2003. Mediji in nasilje: *Obseg in vpliv nasilja v medijih v Sloveniji*. Ljubljana: Mirovni inštitut.
75. Pivec, Franci. 2004. *Informacijska družba*. Maribor: Subkulturni azil.

76. Podjet, Dejan. 2008. *Računalniški kriminal*. Magistrsko delo. Univerza v Ljubljani, Fakulteta za upravo.
77. Podpečan, Mitja. 2007. Vas ta trenutek preiskujejo? *Pravna praksa* 8: 18.
78. Prezelj, Iztok. 2006. *Teroristično ogrožanje nacionalne varnosti Republike Slovenije*. Dostopno na http://www.sos112.si/slo/tdocs/ujma/2006/prezelj.pdf (17. novembra 2010).
79. Prezelj, Iztok. 2002. Konceptualizacija nacionalnih varnostnih interesov. *Teorija in Praksa* 39 (4): 621–637. Dostopno prek: http://dk.fdv.uni-lj.si/tip/tip20024Prezelj.PDF (4. septembra 2010).
80. Radetič, Goran. 2006. *Pomen varnostne politike v elektronskem poslovanju na primeru banke Koper*. Diplomsko delo. Ekonomska fakulteta v Ljubljani.
81. Ramet, Sabrina Petra. 1999. *The Radical Right in Central and Eastern Europe since 1989*. Penn Stare Press, University Park, Pensylvania.
82. Robi Ribič, intervju z avtorjem. Ljubljana, 28. februarja 2011.
83. Rupnik, Janko, Rafael Cijan, Božo Grafenauer. 1996. *Ustavno pravo Republike Slovenije, posebni del*. Pravna fakulteta Univerze v Mariboru.
84. Ryan, Damian in Calvin Jones. 2009. *Understanding Digital Marketing: Marketing Strategies for Enganging the digital generation*. London: Kogan Page, Ltd.
85. Safe.si. 2011. *Varna uporaba interneta*. Dostopno na http://www.safe.si/ (3. januarja 2011).
86. Sherman, Mark. 2000. Introduction to Cyber Crime. *Federal Judicial Center: Special Needs Offenders Bulletin*, št. 5, str. 5–6.
87. Slevin, James. 2000. *The Internet and the Society*. Boston: Polity Press.
88. Sluga, Andrej. 2000. *Policija v Republiki Sloveniji*. Diplomsko delo. Pravna fakulteta v Mariboru, Maribor.
89. Smrkolj, Sebastjan. 2000. *Računalniška kriminaliteta (Oblike in preiskovanja)*. Magistrsko delo. Visoka policijsko-varnostna šola, Ljubljana.
90. Svete, Uroš. 2005. *Varnost v informacijski družbi*. Ljubljana:FDV.
91. Svete, Uroš 2007. *Informacijske razsežnosti sodobnega terorizma – teoretična vprašanja in praktični vidiki*. Dostopno na http://www.sos112.si/slo/tdocs/ujma/2007/124.pdf (4. aprila 2011).

92. Šabec, Ksenija. 2006. Lahi so sodrga in vi, njihova manjšina, imete to v genih. V *Poročilo skupine za spremljanje nestrpnosti 05*, ur. Sabina Autor in Roman Kuhar, 162–190. Ljubljana: Mirovni inštitut.
93. Šajatovič, Tatjana. 1998. *Virtualna realnost – VR: boljša kot resničnost ali slepa ulica civilizacije*. Diplomska naloga. Ljubljana: FDV.
94. Šebenik, Špela. 2002. *Poročanje medijev o proglobalizacijskih protestih*. Diplomsko delo. Fakulteta za družbene vede, Ljubljana. Dostopno prek: http://dk.fdv.uni-lj.si/dela/Sebenik-Spela.PDF
95. Škrt, Radoš. 2005. Pharming napadi. Dostopno prek: http://www.nasvet.com/pharming-napadi/ (15. Novembra 2010).
96. Tankel, Stephen. 2008. *Toward a synthesis view*. Dostopno na http://www.ewi.info/pdf/attachments131.pdf (4. maja 2009).
97. Taylor, Max in Ethel Quale. 2003. *Child Pornography: An Internet Crime*. Bruner – Routledge. New York.
98. Tipton, Harold in Micki Krause. 2008. *Information Security Management handbook*. Boca Raton: Auerbach Publications.
99. Tonnevold, Camilla. 2009. The Intzernet in the Paris Riots of 2005. V *The Public*, ur. Slavko Splichal, 87–100. Ljubljana: Univerza v Ljubljani.
100. Toplišek, Janez. 1998. *Elektronsko poslovanje*. Ljubljana: Založba Atlantis.
101. Trček, Franc in Matej Kovačič. 2000. Kiberseks in pornografija na internetu. Teorija in praksa 37 (št. 6): 1069–1081.
102. Turnšek, Tit. 2008. Terorizem razširjena verzija. *Marija Drofelnik*, Dostopno prek: http://www.marija-drofenik.net/files/TERORIZEM.doc. (23. februarja 2008).
103. Turban, Efraim. 2003. *Electronic Commerce*. A Managerial Perspective. Prentice-Hall, New York.
104. Ulčar, Matjaž. 2001.: Mednarodna pristojnost in kiberprostor. *Pravna praksa* 2001 (8), 21–34.
105. Ustava Slovenije, *Ur. list RS*, št. 33/91-I; 42/1997, 66/2000;
106. Valenčič, Erik. 2009. Samoorganiziranje dela muslimanske mladine. *Mladina*. Dostopno prek: http://www.mladina.si/tednik/201004/islamski_aktivizem (11. januarja 2010).

107. Valenčič, Erik. 2010. Koalicija sovraštva. *Mladina*. Dostopno prek: http://www.mladina.si/tednik/201016/koalicija_sovrastva (10. januarja 2010).
108. Vodušek, Mojca. 1992. Računalniški kriminal. *Varnost – strokovni bilten* 1992 (12), 27-39.
109. Waterman, Peter. 1998. *Globalization, social Movements, and the new Internatinalism*. London: Mansell.
110. Weimann, Gabriel. 2004. *Cyberterrorism: How Real Is the Threat?* Dostopno na http://www.usip.org/pubs/specialreports/sr119.html (25. novembra 2010).
111. Whitman, Michael in Hebert Mattord. 2007. *Principles of Information Security*. Boston: Cengage Lerning EMEA.
112. Ye'or, Bat. 1996. *The decline of eastern Christianity under Islam*. Cranbury, NJ. Fairleigh Dickinson University Press. Dostopno prek: http://www.aspu.edu/oconnort/34003400lect04a.htm. (16. decembra 2010).
113. *Zakon o kazenskem postopku.* Ur. list RS 63/94, 70/94, 72/98, 55/2003.
114. Zakon o policiji, *Ur. list RS*, 210/94, 43/2004, 2303/2004 in 54/2004.
115. Založnik, Pika. 2007. Konstrukcija kiberterorirzma. *Memefest*. Dostopno prek: http=www.memefest.org/2004/si/?meme=gallery&submeme=1. (29. aprila 2010).
116. Zupančič, Maja. 1997. Kriminaliteta v globalni komunikacijski mreži (internet). *Revija za kriminalistiko in kriminologijo* 48 (2), 23–36.
117. Žibert, Anja. 2007. *Teroristična ogroženost Kraljevine Španije*. Fakulteta za družbene vede. Ljubljana.