UNIVERZA V LJUBLJANI
FAKULTETA ZA DRUŽBENE VEDE

MATJAŽ VIDIC

UPORABA INTERNETA V TERORISTIČNE NAMENE

DIPLOMSKO DELO

LJUBLJANA, *2008*

UNIVERZA V LJUBLJANI
FAKULTETA ZA DRUŽBENE VEDE

MATJAŽ VIDIC

Mentor: doc. dr. Iztok PREZELJ

Somentor: asist. dr. Uroš SVETE

UPORABA INTERNETA V TERORISTIČNE NAMENE

DIPLOMSKO DELO

LJUBLJANA, *2008*

Iskreno se zahvaljujem mentorju Iztoku Prezlju za vse ideje in vzpodbude pri pisanju naloge,

ter somentorju Urošu Svetetu za vodenje v pravo smer.

Sodelavcem, ki so me podpirali, pomagali in svetovali.

Nataši za lektoriranje.

Posebna zahvala pa gre moji družini, Ani in Jolandi!

UPORABA INTERNETA V TERORISTIČNE NAMENE

V diplomskem delu je opisana uporaba interneta kot pripomoček pri izvajanju terorističnih napadov. Z razvojem informacijske družbe in naše odvisnosti od računalnikov, informacijskih sistemov in hitrih povezav se odpira dodaten poligon za terorizem. Internetni terorizem. Tehnološki napredek je tudi terorističnim skupinam omogočil dostop do skoraj vseh vrst orožja. Kljub temu so se teroristi začeli posluževati internetnega prostora. Gre predvsem za širjenje informacij in globalno povezanost celic terorističnih skupin. Internet se uporablja predvsem kot medij za prenos informacij. Za teroristične skupine informacija pomeni moč. Z učinkovito uporabo medijev lahko teroristične skupine vplivajo na javnost. Internet, s svojimi značilnostmi omogoča terorističnim organizacijam širjenje novodobnih groženj. Ponuja jim takojšnjo svetovno razširjenost, možnost promoviranja svojih organizacij in rekrutacijo "borcev". Pri internetnem terorizmu gre torej za napade na računalniške sisteme z namenom prizadejati škodo posameznikom in ne računalnikom. Države s povečano varnostno problematiko so že sprejele vrsto zakonskih določil s katerim so omejile internetni kriminal in terorizem.

Ključne besede: Internet, terorizem, tehnologija, varnost, grožnja

A USE OF INTERNET FOR TERRORIST PURPOSES

A diploma gives a description of use of Internet as a tool for terrorist attacks. Development of informational society and our dependence of computers, informational systems and quick links open an additional polygon for terrorism. Cyber terrorism. Technological progress has allowed an access to almost all kind of weapon to terrorist groups. Never the less terrorists started to use a cyber space. Above all it's about spreading information and global connection between terrorist groups cells. Internet is primarily used as a media for information deliverance. Information represents a power for terrorist groups. With effective use of media terrorist groups can affect on a public. Internet, with its characteristics, makes spreading of new age threats possible for terrorist organizations. It offers them immediate global spread, possibility of their organizations promotion and recruitment of "fighters". Internet terrorism is first of all about attacks on computer systems with a purpose of harming individuals and not computers. Countries with high security issues have already accepted several legal regulations to restrict Internet crime and terrorism.

Key words: Internet, terrorism, technology, security, threat

SEZNAM KRATIC

AWF	Analitic Work File – analitična delovna datoteka
CVC	*Canal Voice of Kalifat (Program Glas Kalifata*)
EU	Evropska unija
FBI	Federal Bureau of Investigation
GIMF	The Global Islamic Media Front
GPU	Generalna policijska uprava
IMC	The Islamic Media Center
IRA	Irska republikanska armada
IKT	Informacijsko-komunikacijska tehnologija
OVS	Obveščevalno-varnostna služba Ministrstva za obrambo
PWGT	Police Working Group on Terrorism
RS	Republika Slovenija
RAF	Rote Armee Fraktion
SNAV	Svet za nacionalno varnost
SOVA	Slovenska varnostno-obveščevalna agencija
SECI	South Eastern Cooperative Initiative
TWG	Terrorism Working Group
UKP	Uprava kriminalistične policije
ZKP	Zakon o kazenskem postopku
ZSOVA	Zakon o Slovenski obveščevalno-varnostni agenciji
ZDA	Združene države Amerike

1 UVOD

Ali je mogoče na preprosto vprašanje, zakaj se bojimo internetnega terorizma, ponuditi enako preprost odgovor? Veliko je bilo že pojasnjenega, veliko napisanega, veliko prebranega, vendar pa ravno pri internetnem terorizmu veliko stvari ostaja neznanih v ozadju. Kaj sploh lahko štejemo za internetni terorizem. Z razvojem informacijske družbe in naše odvisnosti od računalnikov, informacijskih sistemov in hitrih povezav internetni terorizem odpira dodaten poligon za terorizem. Internetni terorizem[1]. Ali je onemogočen dostop do vladnih spletnih strani terorizem ali hekerstvo? Verjetno hekerstvo, lahko pa o internetnem terorizmu govorimo v primeru, ko bi s pomočjo vdora v računalniški sistem kontrole letenja na mednarodnem letališču nadzor nad letalskim prometom prevzela kakšna teroristična skupina.

Nov izziv za globalno varnostno okolje pa predstavlja tudi *novodobni terorizem*. Terorizem z novim obrazom, novimi sporočili človeštvu, ki jih sporoča skozi grožnjo, ki jo predstavljajo novodobni izzivi, kot so biološki terorizem, kemični terorizem, jedrski in nuklearni terorizem in ne nazadnje internetni terorizem.

Center za strateške in mednarodne študije iz Washingtona v študiji o internetnem terorizmu navaja, da je to bolj ekonomsko kot teroristično orožje. Čeprav teroristične skupine, kot je Al Kaida, uporabljajo internet in računalniško tehnologijo kot pomoč pri komunikaciji, zbiranju denarja in propagandi, je bolj malo verjetno, da bi bili zadovoljni samo z učinki internetnega terorizma. Cilj terorističnih skupin je povzročiti psihološki strah in materialno škodo, z namenom doseganja političnih ali socialnih sprememb.

Napačno in nevarno je razmišljati, da lahko z vojaško navzočnostjo spremenimo in dokončno zbrišemo radikalno ideologijo različnih fundamentalistov (skrajnežev). Samomorilski napadi, podstavljene bombe ali ugrabitve so klasični načini opozarjanja terorističnih skupin na njihove ideje. Klasični načini kratkoročno dosežejo velik učinek, po preteku določenega časa dejavnost varnostnih organov popusti, razmere pa se do novega napada umirijo. Takšna umiritev razmer ne more veljati za izvajanje internetnega terorizma. Preži povsod, uporaba računalniških mrež je prisotna povsod in v vsakem trenutku. Za preprečevanje internetnega terorizma ni pomembna vojaška moč z najnatančnejšimi izstrelki, temveč potrebujemo

[1] V literaturi se uporabljajo različni izrazi: cyberterrorism, kiber terorizem, IP-terorizem. V diplomski nalogi bom uporabljal izraz internetni terorizem.

računalniške strokovnjake in učinkovit način nadzora spletnih strani ter ne nazadnje prilagoditev zakonodaje.

Tehnološki napredek je tudi terorističnim skupinam omogočil dostop do skoraj vseh vrst orožja. Kljub temu so teroristi začeli uporabljati internetni prostor. Gre predvsem za širjenje informacij in globalno povezanost celic terorističnih skupin. Različne radikalne skupine imajo z razvojem interneta možnost pridobiti informacije za izdelavo različnega orožja, predvsem različnih vrst eksplozivnih naprav. Na srečo, kljub črnogledim napovedim pred leti, predvsem po terorističnih napadih na ZDA, ni prišlo do uporabe orožja za množično uničevanje, s katerim bi teroristične skupine napadle civilno prebivalstvo v zahodnih državah. Bolj verjetna je uporaba komunikacijskih sredstev, kot so računalniki ali satelitski telefoni, s katerimi se poveča učinkovitost klasičnih terorističnih napadov.

Internet se uporablja predvsem kot medij za prenos informacij. Za teroristične skupine informacija pomeni moč. Mediji poročajo predvsem o dramatičnih dogodkih. Vsak poskus ali dejanski teroristični napad mediji obravnavajo kot »glavno novico«, kar radikalne skupine uporabljajo za pridobitev publicitete. Dramatičen dogodek je priložnost za javno predstavitev svojega obstoja ali pridobitev širše javne podpore.

Z učinkovito uporabo medijev lahko teroristične skupine vplivajo na javnost. Javno mnenje in razpoloženje obrnejo proti vladi in lahko celo omogočijo popuščanje njihovim zahtevam. Novice na internetu v hipu obkrožijo svet. Z objavami različnih terorističnih skupin si spletni mediji povečujejo število bralcev in uporabnikov, s tem pa se je oblikovalo okolje, kjer si mediji želijo pridobiti teroristična sporočila za objavo. Namenska uporaba nasilja, ki jo lahko obravnavamo kot obliko psihološkega bojevanja, ima danes s pomočjo množičnih medijev in njihove prodornosti enake ali celo večje učinke kot orožje za množično uničevanje. Gre predvsem za vplivanje na posameznikovo zavest (Gus 2003).

Internet je že zdavnaj zabrisal državne meje. Z brisanjem mej v EU in zagotovljeno svobodo gibanja raste potreba po novih, prožnejših ukrepih, ki bodo teroristom 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.

Sodobni terorizem brez dvoma napada samo bistvo načel in vrednot, na katerih temeljijo liberalne demokratične družbe: življenje, svobodo, dostojanstvo, varnost. Nihče, ki se zaveda razsežnosti napadov v New Yorku, Londonu, na Baliju pa vse do Bagdada, ne more več dvomiti v resnost in drugačnost te sodobne grožnje ter v nujnost odločnega odgovora. Internet pri tem igra pomembno vlogo medija za pridobivanja znanja za radikalne skupine in iskanja širše publicitete ter iskanja enako mislečih novih teroristov.

Brez vsakega dvoma terorizem ogroža demokracijo kot družbeni sistem in pravno državo kot njen pravni izraz. Zato je razumljivo, da mora imeti demokratična in na vladavini prava temelječa država pravico, da se pred terorizmom brani oziroma (za)varuje. Odločilno pri varstvu pred terorizmom pa je merilo, da ti ukrepi ne smejo biti taki, da bi posegli v dva temelja družbenega obstoja – v demokratično ureditev in pravno državo (Šelih 2003). Izjema ni niti preprečevanje internetnega terorizma. Država mora braniti svoje državljane, pri tem pa zelo paziti, da s tem ne krši pravic posameznika – npr. pravice do svobode govora na različnih spletnih straneh, kjer lahko vsakdo izrazi svoje mnenje.

2 METODOLOŠKO - HIPOTETIČNI OKVIR

2.1 OPREDELITEV PREDMETA IN CILJEV PROUČEVANJA

Predmet proučevanja v diplomski nalogi je uporaba interneta v teroristične namene. S prodiranjem informacijske tehnologije v skoraj vse pore življenja postaja ta infrastruktura vedno pogostejša in priljubljenejša tarča internetnih kriminalcev in tudi teroristov. Internet s svojimi značilnostmi terorističnim organizacijam omogoča širjenje novodobnih groženj. Ponuja jim takojšnjo svetovno razširjenost, možnost promoviranja njihovih organizacij in rekrutacijo "borcev". Mimogrede pa pobirajo celo dobrodelne prispevke. Grožnje, obglavljanja zahodnih talcev, pozivi k umorom – vse to se z veliko hitrostjo prek spleta širi med internetnimi uporabniki.

Cilji diplomskega dela so predvsem naslednji:

1. Predstavitve definicij izrazov, uporabljenih v diplomskem delu, opredelitev temeljnih pojmov, kot so terorizem in varnost, in opis značilnosti in razvoja internetnega terorizma.
2. Opis razsežnosti kibernetskega prostora, načina njegove uporabe za izvajanje računalniške kriminalitete in povezav z internetnim terorizmom, razsežnosti in možnosti elektronskega komunikacijskega okolja.
3. Predstavitev zakonskih možnosti preprečevanja kaznivih dejanj prek interneta. Države s povečano varnostno problematiko so že sprejele vrsto zakonskih določil, s katerimi so omejile internetni kriminal in terorizem. Nekaj možnosti nadzora je uvedenih tudi v Sloveniji, čeprav kazenska zakonodaja zaostaja za tehnološkim razvojem.
4. Opis terorističnih dejavnosti v internetnem prostoru (rekrutiranje, obveščanje, priprava na džihad ipd.), opis elektronskega komuniciranja med pripadniki terorističnih skupin in uporabnosti interneta v teroristične namene.
5. Predstavitev dela varnostnih organov v tujini in Republiki Sloveniji, ki se ukvarjajo s preprečevanjem terorizma.

2.2 HIPOTEZE

Hipoteza 1 **Mednarodne teroristične skupine uporabljajo internet kot propagandni pripomoček in za pridobivanje novih članov (rekrutacija).**

Hipoteza 2 **S pomočjo interneta se je spremenilo komuniciranje med teroristi. Omogoča jim komunikacijo in dajanje napotkov razpršenim celicam organizacij.**

Hipoteza 3 **Države EU so ustrezno zakonsko spremenile strategije varnostnih organov za preprečevanje internetnega terorizma.**

2.3 UPORABLJENA METODOLOGIJA

Prva metoda je bila zbiranje informacij, virov in relevantne literature za oblikovanje postavljenih hipotez pri proučevanju internetnega terorizma. Za pregled izbrane tematike sem uporabil tako primarne vire (dokumenti, poročila, zapisniki) kot sekundarne (dostopne v akademskem okolju, in sicer monografske publikacije in strokovne članke)[2].

Uporabljene so bile naslednje metode:

- **analiza besedil, ki so relevantna za to področje**: pregled javnih virov in literature (sekundarna analiza); za spoznavanje problema sem proučil in analiziral ustrezno literaturo, članke na omenjeno temo v tiskanih medijih in na internetu;
- **razgovor s strokovnjaki – intervju**: za potrebe diplomske naloge sem opravil razgovor s tujimi in domačimi strokovnjaki s področja preprečevanja internetnega terorizma;
- **pregled rešenih primerov izvajanja internetnega terorizma po svetu**;
- **lastne izkušnje**: v policiji sem zaposlen 20 let, zadnjih 6 let opravljam naloge v Oddelku za terorizem in ekstremno nasilje na UKP GPU; sodelujem v več domačih in mednarodnih delovnih skupinah za preprečevanje terorizma, tako da so mi bile lastne izkušnje pri izdelavi diplomske naloge v veliko pomoč.

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

3 OPREDELITEV TEMELJNIH POJMOV IN DEFINICIJE

3.1 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 lahko terorizem upravičen. V okvirih mednarodnega kazenskega prava obstajajo sicer vse številčnejši dokumenti, posebej posvečeni terorizmu, vključno z lepim številom večstranskih (multilateralnih) pogodb, vendar se ti definicije terorizma bodisi sploh ne lotevajo bodisi jo podajajo zgolj kot kakšno specialno pojavno obliko (Bavcon in Korošec 2003: 80).

V zadnjih letih se stopnjujejo 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).

Po Prezlju (2006: 177) je terorizem »načrtovanje, organiziranje, izvajanje in podpiranje nasilnih dejavnosti večinoma proti nedolžnim ciljem za doseganje političnih ciljev«. Doda, da k terorizmu sodijo tudi podporne dejavnosti, kot so financiranje, rekrutiranje, skrivanje teroristov, usposabljanje, tihotapljenje ipd., k terorizmu šteje tudi grožnjo s terorizmom. Definicija je pomembna, ker terorizem opredeli kot kompleksni proces, in ne samo kot dejanje. Poznavanje procesa pa omogoča lažje razumevanje, odkrivanje in preprečevanje terorističnih dejanj. Prezelj pravi, da terorizem v sodobnem svetu predstavlja eno od ključnih groženj nacionalni in mednarodni varnosti, predvsem zaradi neposrednih posledic, kot so človeške žrtve, trpljenje in strah, spodkopavanje načel pravne države in drugih načel, na katerih temeljijo sodobne demokracije, ogrožanja družbene povezanosti in politične stabilnosti, ter posrednih posledic, kot je povečevanje poseganja varnostnih organov v

človekove pravice. Terorizem zaradi številnih razlogov, metod in posledic uvršča med kompleksne ogrožajoče pojave.

Na ravni EU je z vidika opredelitve terorizma pomemben okvirni sklep Sveta z dne 13. junija 2002 o boju proti terorizmu[3]. Sklep je nastal po terorističnih napadih v New Yorku leta 2001 in pomeni korak naprej v odnosu EU do tovrstne problematike. Za opredelitev terorizma je zlasti pomemben 1. člen, ki se glasi:

Teroristična kazniva dejanja in temeljne pravice in načela
1. Vsaka država članica sprejme vse potrebne ukrepe, ki zagotavljajo, da se namerna dejanja, na katera se nanašajo spodnje točke (a) do (i) in ki so po nacionalni zakonodaji določena kot kazniva dejanja, ki lahko zaradi svojega značaja ali vsebine hudo škodujejo državi ali mednarodni organizaciji, kadar so storjena z namenom:

- *da bi resno zastraševala prebivalstvo ali*
- *nezakonito izsiljevala vlado ali mednarodno organizacijo, da izvede ali opusti kakršno koli dejanje, ali*
- *da bi resno rušila ali uničevala temeljne politične, ustavne, gospodarske ali socialne strukture države ali mednarodne organizacije,*

šteje za teroristična kazniva dejanja:

(a) napadi na človekovo življenje, ki lahko povzročijo smrt;
(b) napadi na fizično integriteto človeka;
(c) ugrabitev ali zajetje talcev;
(d) znatno uničevanje vladnih ali javnih objektov, transportnega sistema, infrastrukture, vključno z informacijskim sistemom, pričvrščenih ploščadi, ki se nahajajo na epikontinentalnem pasu, javnega kraja ali zasebne lastnine, ki lahko ogrozi človekovo življenje ali povzroči večjo gospodarsko izgubo;
(e) ugrabitev letal, ladij ali drugih sredstev javnega ali tovornega transporta;
(f) proizvodnja, posedovanje, nakup, prevoz, dobava ali uporaba orožja, razstreliv ali jedrskega, biološkega ali kemičnega orožja, kot tudi raziskave in razvijanje biološkega in kemičnega orožja;
(g) spuščanje nevarnih snovi ali povzročanje požarov, poplav ali eksplozij, ki lahko ogrozijo človekovo življenje;

[3] Council Framework decision of 13 June 2002 on Combating Terrorism.

(h) motnje ali prekinitve oskrbe z vodo, elektriko ali drugimi osnovnimi naravnimi viri, ki lahko ogrozijo človekovo življenje;

(i) grožnja, da se bo izvršilo katero od dejanj, naštetih v točkah (a) do (h).

2. Ta okvirni sklep ne spreminja dolžnosti do spoštovanja temeljnih pravic in temeljnih pravnih načel, kot je zapisano v členu 6 Pogodbe o Evropski uniji.

Etimološko beseda terorizem izhaja iz besede teror, ki je latinskega izvora in pomeni nasilje, strahovlado, izzivanje strahu z nasilnim delovanjem, za katerim stojijo politični cilji. Kot politični termin se prvič pojavi v času francoske revolucije (jakobinski teror). Kot reakcija na teror državne oblasti se konec 19. stoletja pojavi teror od »spodaj«, terorizem, ki postane v 20. stoletju tudi del strategije različnih narodnoosvobodilnih ter gverilskih gibanj (npr. IRA) in ideoloških skupin (RAF, Rdeče brigade itd.). Državni organizirani terorizem je bistvena značilnost totalitarnih sistemov 20. stoletja (fašizem, stalinizem) (Dolinar 1988: 1078).

Ena od dveh poglavitnih pojavnih oblik terorizma je državni oziroma vladni terorizem. Gre za množične raznovrstne hude kršitve človekovih pravic, ki jih državna oblast izvaja nad nemočnim prebivalstvom z namenom, da bi ostala na oblasti. Pojem zajema takšne kršitve tako v miru kot v okoliščinah oboroženih spopadov in naperjene proti lastnemu ali tujemu prebivalstvu. V tem pogledu ne gre le za problematiko, ki je stara toliko kot organizirana človeška družba, ampak se soočamo zlasti s problematiko varstva vseh mednarodno priznanih človekovih pravic ter s celotno paleto raznovrstnih kaznivih dejanj po mednarodnem kazenskem pravu, vključno s pravom oboroženih spopadov in t. i. humanitarnim pravom – od mučenja do posebno grobih kršitev procesnih pravic obdolžencev v kaznovalnih postopkih, genocida in vojnih hudodelstev (Bavcon in Korošec 2003: 80).

Na drugi strani pa govorimo o nedržavnem oz. nevladnem terorizmu, ki je pravzaprav težka klasična nasilna kriminaliteta (zlasti zoper življenje in telo, zdravje, prostost, premoženje in splošno varnost) z nekaterimi posebnostmi na strani storilčevega motiva. Kot zelo standarden element definicije terorizma, ki temelji na motivu storilca, sodobni teoretiki mednarodnega kazenskega prava navajajo povzročanje strahu v družbi. Podobno »povzročanje strahu v splošni javnosti, v skupini oseb ali pri posameznih osebah« najdemo tudi v definiciji terorizma v pozitivnem mednarodnem pravu, in sicer v deklaraciji Generalne skupščine ZN št. 49/60 iz leta 1994 o ukrepih za odpravo mednarodnega terorizma. O strahu – kot razlogu za

dejanja teroristov – izrecno govori tudi člen 2/I(b) Mednarodne konvencije o zatiranju financiranja terorizma iz leta 1999[4].

Pri tem je tako v teoriji kot v pozitivnem pravu jasno, da so posamezne konkretne žrtve terorizma, njihovo življenje, telesna celovitost, zdravje, prostost, premoženje, občutek varnosti ipd. le sredstvo za širjenje strahu med drugimi, praviloma širšimi skupinami. Prav zato naj bi značilna sredstva terorističnih napadov učinkovala dramatično, z vidnim neposrednim ali vsaj posrednim učinkom: razstreliva in t. i. sredstva za množično uničevanje (kemijsko, biološko in jedrsko orožje), ugrabitve zračnih in vodnih plovil s pobijanjem talcev ter ugrabitve in usmrtitve posameznih, še posebej družbeno izpostavljenih oseb (Bavcon in Korošec 2003: 80).

3.2 INTERNET

Po definiciji ameriškega Kongresa, ki jo je ta uzakonil v predpisu Communications Decency Act, je internet mednarodna mreža medsebojno povezanih računalnikov. Hkrati je internet tudi edinstven interaktivni medij za globalno komuniciranje, ki uporabnikom omogoča ne le izmenjavo mnenj (internet kot komunikacijski kanal) po elektronski pošti, diskusijskih listah, v klepetalnicah, prek oglasnih desk (Bulletin Board) in na svetovnem spletu (World Wide Web), ampak je tudi sredstvo za pridobivanje in objavljanje informacij v obliki elektronskih časopisov, novic, spletnih portalov in drugih objav, izvrstno orodje in vir za izobraževanje, globalni trg, kjer se srečujeta ponudba in povpraševanje z vsemi vrstami produktov in storitev, vir neskončne zabave, sredstvo države za komuniciranje s svojimi državljani ter tudi sredstvo državljanov za sodelovanje pri upravljanju javnih zadev. V končni posledici lahko internet v prihodnjih letih olajša in omogoči večjo vključenost posameznikov v kibernetsko in realno družbo ter tako pripomore k njeni večji demokratizaciji[5]. Za razliko od tradicionalnih medijev, kot so časopisi, radijski in televizijski programi, kjer ima povprečni bralec, poslušalec ali gledalec razmeroma majhno možnost objavljanja in vplivanja na vsebino posredovanih sporočil, je internet edinstven interaktivni medij, pri katerem posameznik zlahka postane sam svoj založnik, prav tako pa tudi žrtev grobih posegov v svoje osebnostne

[4] International Convention for the Suppression of the Financing of Terrorism, New York, 1999. Konvencija je začela veljati 10. aprila 2002, RS jo je podpisala 10. nov. 2001 in jo ratificirala leta 2004.
[5] Naj kot primer omenim spletne strani http://www.e-participacija.si/, kjer lahko vsakdo sodeluje v razpravi o aktualnih zadevah ter poda svoje mnenje o predlogih podzakonskih aktov.

pravice z nedovoljenim zbiranjem osebnih podatkov in dejanji zoper čast in dobro ime ter drugih kršitev (Velikonja 2001).

Po tragičnem 11. septembru 2001 se zdi, da želijo nekatere države iz varnostnih razlogov sistematično spremljati komunikacijo prek interneta, zagovorniki človekovih pravic pa temu nasprotujejo. Ravnotežje med "varnim" in "svobodnim" internetom pa je tudi eno od osnovnih vprašanj elektronskega poslovanja in interneta nasploh: ali omogočiti svobodno izmenjavo informacij in s tem povezano relativno anonimno in nenadzorovano uporabo interneta ali pa naj se vzpostavi sistem "velikega sita", v katerem bo državam, predvsem pa tržnikom, omogočen pregled nad tem, kaj ljudje počnejo v svetovnem spletu (Možina 2002).

3.3 KIBERNETSKI PROSTOR[6]

Izraz kibernetski prostor (Cyberspace) je skoval pisatelj znanstvene fantastike William Gibson. V svojih delih ga je uporabil za oznako sveta, analognega virtualni resničnosti, kjer poteka interakcija človeških misli[7] (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 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

[6] V literaturi se uporablja tudi beseda kibernetski prostor, pogosto pa se uporablja kar angleški izraz cyberspace.

[7] 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."

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 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)?

Zaradi "nekrajevne" narave interneta je eno najzahtevnejših vprašanj, kako neko sporno elektronsko dejavnost povezati z območjem določenega sodišča (pri tem gre lahko tudi za notranjedržavno 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 1997)?

3.4 INTERNETNI TERORIZEM

Standardne definicije internetnega terorizma ni, ameriški preiskovalni urad FBI, ki se največ ukvarja s tem problemom, pa ga definira kot naklepno politično motiviran napad na informacijski oziroma računalniški sistem, programsko opremo in podatke posamezne ali več držav.

Termin internetni terorizem, ki se nanaša na zbliževanje kibernetskega prostora in terorizma, je v 80. letih prvi uporabil Barry Collin, starejši raziskovalni sodelavec Inštituta za varnost in obveščanje v Kaliforniji (Institute for Security and Intelligence in California) (Denning 1999).

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).

Na splošno lahko internetni terorizem definiramo kot združitev terorizma in kibernetskega prostora. To so nezakonite grožnje ali napadi 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. Napadi, ki uničijo nebistvene službe ali povzročijo predvsem finančno škodo, niso dejanja informacijskega terorizma (Denning 2000 in 2001).

Uporaba informacijsko-komunikacijske tehnologije (IKT) teroristom omogoča številne prednosti, najpomembnejše pa so naslednje:

- IKT je močno zmanjšala čas prenosa informacij, kar omogoča medsebojno povezanost s hitro zunanjo in notranjo komunikacijo in koordinacijo.
- Uporaba kibernetskega prostora omogoča prikrito komunikacijo in anonimnost.
- Nove informacijsko-komunikacijske tehnologije so močno pocenile komunikacijo (npr. uporaba interneta je relativno poceni).
- IKT deluje kot ojačevalec moči, zato se danes vse pogosteje izpostavljata informacijska moč in prostor kot novi področji geopolitike.
- Povezovanje računalništva in komunikacije je bistveno povečalo obseg in zapletenost informacij.
- IKT teroristom omogoča, da dosežejo ciljno občinstvo tudi, kadar drugi mediji niso učinkoviti, hkrati pa na ta način dosežejo tudi novo občinstvo (mlade in izobražene) (Whine 1999 in Edwards in Zanini 2001).

3.5 VARNOST

Po Grizoldu je varnost stanje, v katerem je zagotovljen uravnotežen, fizični, duhovni, duševni ter gmotni obstoj posameznika in družbene skupnosti v razmerju do drugih posameznikov, družbenih skupnosti in narave (Anžič 1997).

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.

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.

4 KIBERNETSKI PROSTOR

4.1 ZGODOVINSKI RAZVOJ POJMA RAČUNALNIŠKE KRIMINALITETE

Korenine pojma računalniški kriminal segajo v leto 1960, ko so bili v javnem tisku in strokovni literaturi objavljeni prvi članki o t. i. računalniškem kriminalu. Primarno so ti primeri vključevali računalniško manipulacijo, računalniško sabotažo, računalniško »špijonažo« oziroma vohunstvo in nelegalno uporabo računalniških sistemov. V sredini 70. let so bile o računalniškem kriminalu narejene prve empirične raziskave, ki so se sklicevale na znanstveno-kriminološke preiskave. Pogled javnosti in znanosti nanj pa se je drastično spremenil v 80. letih, ko so v tisku objavil osupljive primere o hekerjih, računalniških virusih in črvih. Ranljivost informacijske družbe je širši javnosti razkril val programskega piratstva, manipulacij delitve denarja in zlorabe telekomunikacijskih sredstev (Seiber 1998: 19).

Zaradi vedno novih in novih oblik računalniškega kriminala se je pojavila potreba po definiciji. Tako je že leta 1983 skupina strokovnjakov OECD (Organisation for Economic Co-operation and Development – Organizacija za ekonomsko sodelovanje in razvoj) definirala termin »računalniški kriminal« kot »*vsako ilegalno, neetično ali neavtorizirano vedenje, ki zajema avtomatsko obdelavo podatkov in/ali prenos podatkov*« (Seiber 1998: 20). Kasnejše razlage pojma pa so šle še dlje, z razvojem obsežnejšega pojma »*podatkovni in/ali informacijski kriminal*« (Seiber 1998: 21).

4.2 RAČUNALNIŠKA KRIMINALITETA

Ne glede na prvotni namen računalništva (znanstveni in raziskovalni), je svojo priložnost v njem kaj hitro našel tudi kriminal. Njegov interes po izrabi zmogljivosti računalniške tehnologije, njegove povezave s komunikacijskim okoljem in vedno bolj imaginarnim spletnim okoljem postaja vedno večji (Thackrah 2004).

Čeprav je večina razlag pojma kibernetske kriminalitete oziroma kriminalitete, povezane z računalniki, dokaj splošnih, pa je verjetno prav v njihovi splošnosti mogoče najti širok spekter kriminalnih dejanj, ki jih ta pojem obsega. Tako David Wall v svoji konceptualizaciji kibernetske kriminalitete pravi, da je to pojem, ki obsega škodljivo vedenje, ki je na nek način povezano z računalnikom (Wall 2001: 2). Armstrong in Forde pa za kibernetski kriminal pravita, da je to »kriminal, ki je zagrešen s pomočjo interneta« (Armstrong in Forde 2003:

209). Grabosky in Smith računalniško kriminaliteto definirata kot t. i. digitalni kriminal, to pa je kriminal, ki obsega informacijske sisteme kot sredstva ali tarče nezakonitega delovanja (Wall 2001: 29).

Nekoliko bolj natančno je ta pojem definiral Brvar, ki je kriminaliteto v zvezi z računalniki definiral »kot kazniva dejanja, v katerih računalnik nastopa kot sredstvo (orodje), predmet ali objekt napada, za izvršitev ali poskus izvršitve kaznivega dejanja pa je potrebno določeno znanje iz računalništva in informatike« (v Martonosi 1993: 498).

Danes organizirana kriminaliteta in nekatere druge vrste kriminalitete, kot so področje goljufij, bančnih prevar, kraj avtorskih pravic, kriminalitete z obeležjem diskriminacije, tatvin patentov ipd., da pornografske industrije, zlorab otrok, otroške pornografije sploh ne omenjamo, verjetno ne bi obstajale v vsem svojem obsegu, če ne bi pri svoji kriminalni dejavnosti uporabljale računalniške tehnologije in kibernetskega prostora. Organizirane kriminalne združbe in posamezniki z različnimi interesi internet izrabljajo za širjenje internetnega vandalizma, razširjanje virusov in črvov, povzročanje enormnih materialnih škod z uničevanjem podatkovnih baz, z vsem tem pa povzročajo pravi tehnološki kaos.

Obstajajo torej različne definicije kriminala, storjenega v kibernetskem prostoru. Nekateri (npr. Brvar) mu pravijo kriminal v zvezi z računalniki, drugi digitalni in informacijski kriminal (npr. Grabosky in Smith), ne nazadnje pa se je splošno uveljavil pojem kibernetska kriminaliteta (»cybercrime«). Zanj Littlejohn Shinder (2002: 5) pravi, da je podkategorija računalniškega kriminala in se nanaša na kriminalna dejanja, storjena s pomočjo uporabe interneta ali kakega drugega računalniškega omrežja. Računalniki in računalniška omrežja so lahko uporabljeni za kriminalna dejanja na različne načine. Računalnik ali računalniško omrežje je lahko:

- orodje za izvedbo kriminalnega dejanja,
- tarča kriminalnega dejanja (torej žrtev kriminala),
- vmesnik pri povezavi s kriminalnim dejanjem (npr. za shranjevanje ilegalnih vsebin ali prodajo ilegalnih drog) (Littlejohn Shinder 2002: 5).

Poskusi področij, kot so psihologija, politika in ekonomija, poskušajo združiti napore v prizadevanjih, da bi se družba osvestila in spoznala pretečo nevarnost v njenem pravem obsegu. Izražata se predvsem dva vidika, psihološki in tehnološki; prvi, naključnost izbire

ciljne skupine žrtve, ki povzroča nenehno stanje negotovosti, in drugi, za izvršitev uporabljena tehnološka dognanja (Weimann 2004).

Ne glede na vložke javnega in zasebnega sektorja v razvoj tehnologije, ki bi pomagala zaščiti t. i. virtualni svet in omogočila nemoteno delovanje ter s tem izpad dobička, se je praktično nemogoče izogniti nenehnim vpadom v računalniške sisteme iz takšnih ali drugačnih razlogov. Center za raziskavo računalniške kriminalitete (Computer Crime Research Center) je v letu 2002 poročal, da je kar 90 % obravnavanih uporabnikov, ki so bili zajeti v študiji, zaznalo poskus nedovoljenega dostopa v sistem. V drugi nedavni spletni raziskavi so ugotovili, da je bilo kar 92 % zasebnih podjetij v zadnjem letu predmet poskusov neavtoriziranih vstopov v računalniške sisteme (Coleman 2005).

Ocenjujejo, da bi samo enodnevni izpad spletnega medmrežja v ZDA povzročil izpad 6,5 milijard Dolarjev prometa. Blagovni promet skozi spletno medmrežje, IT-komunikacije, bančne komunikacije in finančne transakcije, sistem avtorizacije kreditnih kartic ipd. predstavljajo osnovno gonilo ekonomije. Pomembnost informacij in s tem dostopa do njih je nepredstavljiva, njihova pomembnost pa skokovito narašča. Te potrebe narekujejo nenehen razvoj tehnologije, ki omogoča hitrejšo in bolj učinkovito uporabo računalniške infrastrukture, s tem pa se povečuje tudi njena ranljivost. Ob finančnem vidiku ob tem ne smemo pozabiti na psihološki učinek, ki ga predstavlja nenehen strah, da bo uporabnik zlorabljen (Coleman 2005).

Ker gre v primeru virtualnega sveta in kibernetskega okolja, ki bi lahko potencialno deloval v njem ali proti njemu, za zelo kompleksno področje, kjer se prepletajo različna področja elektronskih tehnologij, je treba opredeliti tudi komplementarne sisteme, preko katerih deluje računalniška kriminaliteta oz. terorizem. S tem se ukvarja t. i. Communication Intelligence. Gre za zelo delikatno področje, ki ima bogato tradicijo v pretekli zgodovini nekaterih totalitarnih sistemov, ki so na ta način nadzirali vsak korak svojih državljanov, pa tudi v različnih kriznih obdobjih, kot je npr. hladna vojna, ko je bilo za nacionalno varnost ključnega pomena prestrezanje informacij, ki so jih vsebovala diplomatska sporočila (Černigoj).

Ker gre za občutljivo področje obveščevalne dejavnosti in zasebnega varovanja, ki prikrito nudi usluge prestrezanja sporočil za državne strukture, je to seveda povezano z grobimi posegi v posameznikovo zasebnost.

Kršenje človekovih pravic in svoboščin trči ob t. i. višje državne, politične in gospodarske interese, za katerimi se skriva fenomen državne varnosti, v najnovejšem času pa tudi varnosti posameznih regij, celotnih skupnosti, kot je npr. EU, ipd.

Za prenos elektronskih sporočil v največji meri skrbijo mednarodni telekomunikacijski sistemi, ki so največkrat v lasti posameznih državnih ali mešanih družb, nekaj manj pa družb, ki so v celoti v zasebni lasti. Prestrezanje in spremljanje elektronskih sporočil, ki ima skoraj 90-letno tradicijo, je osredotočeno na področja, kot so visokofrekvenčni radijski signali, mikrovalovne frekvence, podvodni telekomunikacijski vodi, satelitski prenosi, digitalna telekomunikacijska tehnologija idr. (http://www.cyber-rights.org/interception/stoa/ic2kreport.htm#Report).

5 ZAKONODAJA

Boj proti mednarodnemu terorizmu ni le boj za varnost, temveč tudi boj za temeljne vrednote in svoboščine, ki gradijo temeljno identiteto demokratičnih družb in ki jih terorizem sistematično ogroža. Prav zato je treba v tem boju dosledno spoštovati tako notranje ustavno pravo kot mednarodno pravo človekovih pravic, saj predstavlja pripravljenost razgraditi lastne zakone, namenjene zaščiti pravic vsakogar, prav takšno, če ne celo večjo grožnjo demokratični družbi (Švarc 2006: 135).

Kljub temu da so bile posledice terorističnega napada v Londonu 7. julija na prvi pogled mnogo manj obsežne kot po 11. septembru v New Yorku in po 11. marcu v Madridu, je žalovala vsa Velika Britanija. Nekaj dni po napadu se je za 86 odstotkov spremenilo javno mnenje v korist večjih pooblastil policistom pri iskanju osumljencev za teroristična dejanja. Posledice spremembe zakonodaje in povečanja pooblastil varnostnim organom pa bo čutiti tudi na področju internetnega terorizma, kar naj bi pomagalo pri boju proti terorizmu in povzročilo večji občutek varnosti (Grosek 2005).

Terorizem je v okviru mednarodnega prava predmet cele palete aktov, ki se jim pridružujejo še pravila na državni ravni. Samo pod okriljem OZN obstaja približno 150 aktov, nobeden pa nima enotne univerzalne definicije terorizma kot mednarodno prepovedanega dejanja. Jedro omenjenega normativnega okvira je dvanajst veljavnih mednarodnih konvencij in protokolov:

- Konvencija o kaznivih dejanjih in nekaterih drugih dejanjih, storjenih na letalih (1963),
- Konvencija o zatiranju nezakonite ugrabitve zrakoplovov (1970),
- Konvencija o zatiranju nezakonitih dejanj zoper varnost civilnega zrakoplovstva (1971),
- Konvencija o preprečevanju in kaznovanju kaznivih dejanj zoper osebe pod zaščito, vštevši diplomatske agente (1973),
- Mednarodna konvencija proti jemanju talcev (1979),
- Konvencija o fizičnem varovanju jedrskega materiala (1980),
- Protokol o zatiranju nezakonitih dejanj na letališčih za mednarodno civilno zrakoplovstvo, s katerim se dopolni Konvencija o zatiranju nezakonitih dejanj zoper varnost civilnega zrakoplovstva (1988),
- Konvencija za preprečevanje nezakonitih dejanj zoper varnost pomorske plovbe (1988),

- Protokol za preprečevanje nezakonitih dejanj zoper varnost ploščadi, postavljenih na epikontinentalnem pasu (1988),
- Konvencija o označevanju plastičnih razstreliv zaradi njihovega odkrivanja (1991),
- Mednarodna konvencija o zatiranju terorističnih bombnih napadov (1997) in
- Mednarodna konvencija o zatiranju financiranja terorizma (1999).

Mnoge od teh pogodb so bile sprejete kot odziv na večje teroristične incidente (Konvencija o kaznivih dejanjih in nekaterih drugih dejanjih, storjenih na letalih, Konvencija o zatiranju nezakonitih dejanj zoper varnost civilnega zrakoplovstva in Konvencija o zatiranju nezakonite ugrabitve zrakoplovov, denimo, kot odgovor na številne ugrabitve in sabotaže civilnih letal v šestdesetih in sedemdesetih letih 20. stoletja; podobno je bila Konvencija za preprečevanje nezakonitih dejanj zoper varnost pomorske plovbe sprejeta kmalu po ugrabitvi italijanske križarke Achille Lauro) (Hohler 2005: 6).

Kot trinajsta v vrsti specialnih konvencij je bila leta 2005 sprejeta Konvencija o zatiranju dejanj jedrskega terorizma (International Convention for the Suppression of Acts of Nuclear Terrorism).

5.1 UREDITEV V REPUBLIKI SLOVENIJI

Preprečevanje terorističnih napadov v Sloveniji so opravila varnostnih organov, ki večini prebivalcev niso vidna, niti niso poznana. Večina Slovencev se ne počuti ogroženih zaradi delovanja različnih mednarodnih terorističnih skupin, niti se ne ukvarja z vprašanji o teroristični ogroženosti po svetu[8]. Kljub temu se zakonodaja prilagaja in se pripravlja, da bi se lahko uspešno uprli morebitnemu ogrožanju Slovenije.

Kazenski zakonik iz leta 1995 (spremenjen in dopolnjen v letih 1999, 2004 in 2008)[9] med kaznivimi dejanji, povezanimi s problematiko terorizma, opredeljuje zlasti kazniva dejanja iz 33. in 35. poglavja, in sicer kazniva dejanja zoper varnost Slovenije in njeno ustavno ureditev ter kazniva dejanja zoper človečnost in mednarodno pravo. Za varstvo ustavne ureditve je pomembna ugotovitev, da je večina v nadaljevanju navedenih kaznivih dejanj povezana z ogrožanjem ustavne ureditve oziroma varnosti Slovenije. V kazenski zakonodaji so

[8] Podatki iz Obramboslovnega raziskovalnega centra – SJM, 2005, SJM, 2003, SJM, 2001 in SJM, 1999).
[9] Ur. l. RS, št. 63/94, 70/94, 23/99, 40/2004, 55/2008.

nedvoumne povezave med terorizmom, mednarodnim terorizmom, diverzijo in drugimi dejanji ter problematiko varstva ustavne ureditve. Ključni kaznivi dejanji, določeni v Kazenskem zakoniku RS z obravnavanega področja, sta: 355. člen – Terorizem in 388. člen – Mednarodni terorizem. Z zadnjo novelo kazenskega zakonika[10] pa je dodan nov člen, in sicer člen 388/a. – Financiranje terorističnih dejanj.

Terorizem danes v svetu zaradi svoje globalnosti vzbuja skrb zaradi ogrožanja temeljnih družbenih vrednot. Pri iskanju rešitev se države in mednarodne organizacije zatekajo k novim oblikam delovanja, tako da se medsebojno povezujejo na dvostranski ali večstranski ravni z doslednim upoštevanjem mednarodnega prava. V posameznih primerih pa nekatere države v boju proti terorizmu kot protiukrep uporabljajo tudi državni terorizem. Praksa kaže, da nobena od rešitev ne zagotavlja dovolj učinkovitosti in kot taka ne pomeni dokončne rešitve problema terorizma. Teroristi se namreč vedno znova prilagajajo mednarodnim ukrepom in se tako uspešno izogibajo pravnemu nadzoru (Kečanovič 1994, str. 1).

Za učinkovito preprečevanje terorizma in uspešno izvedbo kazenskega postopka pri tovrstnih kaznivih dejanjih so, zaradi izjemno velike družbene nevarnosti, potrebne tudi posebne kazenskoprocesne in upravno-administrativne norme. Za ustrezno preprečevanje kaznivih dejanj, povezanih s terorizmom, bi morali urediti tudi uporabo nekaterih določil Zakona o kazenskem postopku, ki urejajo uporabo posebnih metod in ukrepov, s katerimi je mogoče preprečiti delovanje teroristov in zbrati dovolj dokazov za njihovo namero že v fazi priprave na izvršitev posameznega kaznivega dejanja. Sedanja zakonodaja namreč omogoča izvajanje teh ukrepov zoper določeno, na podlagi podatkov znano osebo. V današnjem času mobilne telefonije (predplačniški sistem brez znanih podatkov o naročniku) in anonimne uporabe internetnih storitev pa identifikacija storilcev prav gotovo predstavlja resen problem (glej Kečanovič 1995: 5).

5.1.1 Pravna ureditev internetne kriminalitete v Republiki Sloveniji

Svet ministrov Evropske unije je 8. 11. 2001 sprejel besedilo Konvencije o kibernetski kriminaliteti (Convention on Cybercrime) in poročilo »Explanatory Report«, v katerem med drugim razlaga posamezne pojme, ki jih konvencija vsebuje. Republika Slovenija je ratificirala

[10] Zakon o spremembah kazenskega zakonika, Ur. list RS, št. 40-1662/2004.

konvencijo in pripadajoče dokumente, Državni zbor pa je sprejel novo dikcijo kaznivega dejanja »Neupravičen vstop v informacijski sistem« po členu 225 KZ.

Poročilo konvencije navaja, da je prestrezanje računalniških podatkov izenačeno s prisluhom telefonskega pogovora med subjekti in je kot tako grob poseg v človekove pravice in svoboščine. Pravica do zasebnosti je ena temeljnih človekovih pravic, zato so avtorji konvencije to pravico uporabili kot vodilo pri določitvi neupravičenega elektronskega prestrezanja podatkov, ki so lahko preneseni po telefonu, faksu, elektronski pošti ali z navadnim prenosom računalniških podatkov. Prestrezana komunikacija se lahko dogaja v enem računalniškem, dveh računalniških sistemih, ki pripadata isti osebi, dveh računalniških sistemih, ki komunicirata med seboj, ali med računalniškim sistemom in človekom (npr. vnos znakov preko tipkovnice). Med prestrezanje podatkov se po tem členu šteje tudi prestrezanje elektronske emisije, na podlagi katere se da rekonstruirati računalniške podatke (sevanje računalniških zaslonov).

Konvencija je eden redkih mednarodnih aktov, ki so posegli v zapleteno področje kibernetskega oziroma internetnega kriminala, njen namen pa je zagotoviti čim učinkovitejši boj proti temu pojavu na nacionalnih in na mednarodni ravni.

Konvencija o kibernetski kriminaliteti vsebuje vrsto ukrepov, ki jih je treba v boju proti kibernetskemu kriminalu sprejeti na državni ravni. Glede kazenskega materialnega prava konvencija zavezuje države podpisnice, da v svojem notranjem pravu kot kazniva dejanja opredelijo nekatere hujše zlorabe, povezane z računalniki. Zato Konvencija kazniva dejanja deli v štiri skupine.

Prva skupina: kazniva dejanja zoper zaupnost, celovitost in dostopnost računalniških podatkov in sistemov. Sem sodijo:

- protipravni dostop;
- protipravno prestrezanje;
- motenje podatkov;
- motenje sistemov ter
- zloraba naprav.

Druga skupina: kazniva dejanja, povezana z računalnikom. Sem sodita:

- računalniško ponarejanje in

- računalniška goljufija.

Tretja skupina: kazniva dejanja, povezana z vsebino digitalnega zapisa. Sem sodijo:

- kazniva dejanja, povezana z otroško pornografijo;
- v to skupino pa je mogoče uvrstiti tudi kazniva dejanja razširjanja rasističnega in ksenofobičnega gradiva v računalniških sistemih, rasistične in ksenofobične grožnje, rasistične in ksenofobične žalitve ter zanikanja, hujša zmanjševanja pomena, odobravanja ali zagovarjanja genocida ali hudodelstev zoper človečnost, glede katerih obveznost inkriminacije za države podpisnice ne izhaja iz Konvencije, ampak iz dodatnega protokola k tej konvenciji.

Četrta skupina: kazniva dejanja, povezana s kršitvijo avtorske in sorodnih pravic. Sem sodijo:

- kazniva dejana, povezana s kršitvijo avtorske in sorodnih pravic (Selinšek 2005).

Države podpisnice morajo za navedena kazniva dejanja zagotoviti tudi odgovornost pravnih oseb, in sicer za primere, ko fizična oseba izvrši kaznivo dejanje v korist pravne osebe. Fizična oseba lahko pri tem deluje samostojno ali pa v imenu pravne osebe, v kateri ima vodilni položaj (torej ima pravico do zastopanja pravne osebe, pristojnost za sprejemanje odločitev v imenu pravne osebe ali pristojnost opravljati notranji nadzor v pravni osebi).

Slovenija na področju internetnega kriminala spada med relativno urejene države. Materialna kazenska zakonodaja vsebuje večino kaznivih dejanj, ki jih pozna konvencija, relativno dobro pa so urejeni tudi nekateri instituti kazenskega procesnega prava. Primerjalno je konvencija sicer širša od naših nacionalnih določb, kar pomeni, da bodo potrebne spremembe v nekaterih zakonih (kazenski zakonik, zakon o kazenskem postopku, zakon o telekomunikacijah). Slovenska primerjalna prednost je tudi v tem, da spadamo v ne ravno veliko skupino držav, ki ima v organizacijski strukturi policije posebno enoto za boj proti računalniški kriminaliteti, ki deluje tudi v resnici, in ne samo na papirju (Rupnik 2002).

Ustrezna zakonodaja je osnova in prvi pogoj za uspešen pregon, posredovanje ter sankcioniranje kriminala, ki se odvija preko interneta. Internet pa zaradi lastniške dileme ne sodi pod nikogaršnjo pravno priznano pristojnost, zato je težko postavljati zakone v prostoru, ki je povsod in nikjer, kar pa izkoriščajo tudi teroristične skupine ali posamezniki, ki širijo različne ekstremistične propagande.

6 TERORISTIČNA DEJAVNOST V SPLETNEM OKOLJU

Teroristi informacijsko tehnologijo za svojo dejavnost uporabljajo na dva načina. Pri prvem gre za zlorabo informacijske tehnologije (svetovni splet in elektronska pošta na internetu) 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 delovanje, pri tem pa nudi anonimnost v različnih operacijah (Weiman 2004).

Druga oblika zlorabe informacijske tehnologije je uporaba tovrstne tehnologije za napade in vdore v informacijske sisteme različnih organizacij, varnostnih služb in vladnih organizacij, ki se borijo proti terorizmu. V tem primeru se informacijska tehnologija uporablja kot teroristično orožje ali kot objekt terorističnega napada. Poleg klasičnega napada na informacijske sisteme (uničevanje infrastrukture sistemov) teroristične skupine načrtujejo tudi informacijski napad z uporabo računalniških virusov, trojanskih konjev in logičnih bomb. Na tak način pri vdoru v informacijski sistem poskušajo uničiti čim več podatkov v kibernetskem prostoru in tako onemogočiti nemoteno funkcioniranje dejanskega sveta. Tovrstna oblika napada gotovo pomeni veliko nevarnost v primeru, da bi prišlo do kaosa v informacijskem sistemu, ki ureja zračni ali železniški promet predvsem v trenutku, ko je varnost v veliki meri odvisna od informacijske tehnologije (vodenje letal v času pristanka, radarska zaznava letenja, usmerjanje prometa potniških vlakov …). Tarča tovrstnega terorizma pa so tudi poskusi blokad finančnih transakcij, bančnih sistemov in povzročanje zmede na svetovnih borzah (Černigoj 2007).

Grožnjo predstavlja predvsem možnost napada ali vdora v državno infrastrukturo, ki je podprta z računalniško tehnologijo, posledice tega pa bi bile:

- ogrožanje človeških življenj,
- onesposobitev vojaških varnostnih sistemov,
- onesposobitev urgentnih zdravstvenih storitev,
- dezorganiziranost v transportu,
- motene telekomunikacijske povezave ter
- ustvarjanje kaosa z napadom na bančne in finančne zmogljivosti.

Samo ZDA[11] so v preteklih nekaj letih zaznale številne poskuse vdorov v računalniške sisteme ministrstva za obrambo in vladnih ustanov. V letu 1998 so zaznali 11 vdorov v ministrstvo za obrambo, v letu 2005 pa v povprečju beležijo okoli 60 poskusov vdorov oz. napadov tedensko. Seveda gre v večini primerov za visoko usposobljene nadobudneže, kjer ni v ozadju terorizem ali kriminalna dejavnost, temveč osebni izziv ali lastna promocija. Je pa dovolj veliko opozorilo, da je treba računati tudi s t. i. informacijskim spopadom/napadom (*Information Warfare*), ki ga lahko izvedejo teroristi ali posamezne države (http://www.adl.org/terror/focus/16_focus_a2.asp, 28. april 2006).

6.1 INTERNETNI TERORIZEM

Pri internetnem terorizmu gre za napade na računalniške sisteme, z namenom povzročiti škodo posameznikom, in ne računalnikom. Njegova značilnosti je velika učinkovitost v družbah, kjer računalniški sistemi nadzorujejo večino vidikov posameznikovega življenja. To pomeni, da gre za nadzor nad različnimi državnimi podsistemi (zdravstvo, izobraževanje, poslovanje, sodni pozivi). Zloraba oziroma pridobitev takšnih podatkov bi lahko imela hude posledice (Libicki 1995).

Kot pojav internetnega terorizma se v evropskem prostoru pojavljajo različne spletne strani z radikalno islamistično propagando. Največja težava za preiskovalce je, da so po večini pisane v arabščini, v različnih narečjih, in bi za popolno analizo potrebovali več različnih prevajalcev. Spletne strani vsebujejo podatke o izvajanju nalog islamističnih ekstremistov v različnih državah, ki se borijo proti »zahodni nadvladi«, ki predstavlja največjo nevarnost za širitev islama. Spletne strani vsebujejo pozive za različne donacije med muslimani v evropskih državah in spletne forume, kjer se izražajo mnenja tudi med muslimani v Evropi.

Thomas tako loči devet možnih načinov delovanja terorističnih organizacij na internetu:

[11] Zanimivo je, da ZDA, ki so eden od največjih promotorjev grožnje kibernetskega terorizma, niso zaznale »pravih« terorističnih dejavnosti na tem področju. Za primerjavo lahko navedemo nekatere druge države. Leta 1997 je t. i. skupina Internet Black Tigers (ena od opcij organizacije The Liberation Tigers of Tamil Eelam) prevzela odgovornost za napade na misije Šrilanke v tujini. Tu so še napadi neimenovanih skupin na Jedrski raziskovalni inštitut v Indiji leta 1998, začasna onesposobitev kitajskega satelita leta 1997, s strani oporečnikov, ki opozarjajo na nestrinjane z vlaganji zahodnega kapitala na Kitajskem, ipd. V evropskem prostoru lahko kot primer navedemo sabotažo desno opredeljene stranke, in sicer uničenje njihove spletne strani med volilno kampanjo.

- zbiranje občutljivih podatkov o tarčah,
- zbiranje finančne podpore,
- povezovanje različnih skupin,
- izsiljevanje,
- propaganda,
- globalna svoboda,
- psihološki vplivi,
- goljufije in
- prikrite operacije (Thomas 2002).

Podobno tudi Belič v informacijskem pomenu loči štiri oblike delovanja terorističnih organizacij:

- medsebojne komunikacije,
- propagandna dejanja,
- zbiranje informacij,
- teroristični napadi z uporabo informacijskih orodij – orožij.

Prve tri oblike niso nujno uvod v informacijsko izveden teroristični napad, lahko so le pripravljalne stopnje v klasično teroristično dejanje. Pri terorističnih napadih z informacijskimi orodji – orožji pa je nujen jasen cilj napada (npr. Elektroenergetski sistem, prometni sistem, borza ...). Osnovni cilj takšnega napada je onesposobitev ciljnega informacijskega sistema (Belič 2001: 263).

6.2 SPLETNE STRANI TERORISTIČNIH ORGANIZACIJ

Teroristične, separatistične in različne ekstremistične skupine že od sredine 90. let prejšnjega stoletja uporabljajo internet in informacijsko tehnologijo za predstavitev svojih idej in ciljev. Izjema niso niti radikalne islamistične skupine. Na začetku razvoja interneta so islamistične skupine internet označevale kot »mašinerijo« za širjenje neislamske kulture, kasneje pa se je internet razvil v glavno orodje za širjenje islamističnih idej.

Danes je na radikalnih islamističnih straneh mogoče najti zelo obširno literaturo islamističnih ideologov, strokovnjakov in učiteljev. V besedilih iščejo povezavo med teologijo in nasiljem, opisujejo dolgoročne politične strategije, taktiko gverilskega bojevanja, opisujejo načine

izdelave improviziranih eksplozivnih sredstev ali izognitve morebitnemu nadzorovanju varnostnih služb.

Islamistične spletne strani pogosto objavljajo pisne, avdio ali video posnetke, s katerimi obveščajo javnost o džihadističnih bojih v Afganistanu in Iraku. Veliko strani ima na voljo spletne forume, bloge in klepetalnice. V nadaljevanju bom predstavil nekaj najbolj znanih spletnih strani z radikalno islamsko vsebino in pozivi na vodenje džihada. Podatke sem pridobil z udeležbo na več predavanjih dr. Brynjar Lie, predstavnice organizacije »Norwegian Defense Research Establishment«, ki jih je imela v več mednarodnih delovnih skupinah, ki se ukvarjajo s preprečevanjem terorizma.

6.2.1 The Islamic Media Center – Islamski medijski center

Islamski medijski center (IMC) je verjetno med najstarejšimi ustvarjalci džihaditskih spletnih strani. V izjavi, odkriti leta 2005, pravijo:
»IMC je bil ustanovljen pred 14 leti. Predstavil je čudovite stvari spletnemu svetu v obliki tečajev, publikacij in filmov, in to v času, ko je bi splet še nekaj novega …«

IMC je tudi največji ustvarjalec spletnih priročnikov. Bil je na primer pomemben soustvarjalec *Enciklopedije priprave za džihad*, znane tudi kot *Enciklopedija džihada*. Zdi se, da je material prišel iz različnih virov. Lahko ga je napisalo osebje IMC, po vsebini sodeč, je bilo prevedeno iz NATO-vih in ameriških terenskih priročnikov ali pa izdelano na osnovi »zapisov z bojišča«.

Njihovi priročniki za treninge in slike treningov obravnavajo različne teme, od načrtovanja eksplozivnih naprav do rabe konvencionalnega orožja, izdelave in uporabe strupov in strupenih plinov za teroristična dejanja, varnostnih priporočil za borce džihada, gverilskega bojevanja in vojaške taktike ipd.

Glede druge medijske produkcije pa se zdi, da je IMC deloval bolj kot distributer kot ustvarjalec. V svojem imenu so distribuirali več filmov, vključno s starimi filmi iz arabsko-afganistanske vojne, pa tudi filme iz Eritreje, Kašmirja in Iraka.

Zdi se, da IMC od leta 2005 ne deluje več, ali pa so morali spremeniti ime in naslov spletne strani, potem ko so vdrli na njihovo spletno stran in v račune elektronske pošte. Obstaja pa tudi možnost, da so se združili z ostalimi džihadskimi medijskimi podjetji.

IMC je bil poskus, kako narediti gradivo za džihadistično urjenje, ki so ga združili iz različnih virov, predvsem iz različnih urjenj v Afganistanu. Njihove organizacijske povezave niso znane.

6.2.2 Al-Sahab Institute for Media Production – Inštitut za medijsko produkcijo Al Sahab

Al Sahab je najbližje pojmu uradnega podjetja Al Kaide za medijsko produkcijo. Zaradi tega predstavlja njihovo ime močno tržno znamko glasu Al Kaide. Imajo ekskluzivni dostop do dveh vodij Al Kaide. Od leta 2001 je to edina agencija, ki je imela medijske intervjuje z Osamo bin Ladnom in Ajmanom Al Zavahirijem. Zaradi tega so precej skrivnostni, tako glede svoje organiziranosti kot glede osebja.

Njihov glavni produkt so avdio in video intervjuji. Prav tako so ponovno natisnili knjige Ajmana Al Zavahirija.

V preteklosti so bili Al Sahabovi video filmi največkrat poslani v pisarno Al Džazire v Islamabadu, nekaj pa tudi v njihove druge poslovalnice. Od leta 2005 se vse večkrat odločajo, da propagandne filme objavijo na spletu.

Celo Al Sahab občasno kreira spletne strani za distribucijo svojih izdelkov, povpraševanje pa je tako veliko, da se njihovi filmi hitro širijo po spletu tudi na drugih naslovih.

Večina Al Sahabove produkcije je iz Afganistana, vendar so objavili tudi dva filma o delovanju Al Kaide na Arabskem polotoku. Prvi Al Sahabov video je bila reportaža o bombardiranju ameriškega rušilca USS Cole sredi oktobra 2000. Od takrat je njihova produkcija stalno naraščala. V letu 2006 so ustvarili kar 58 videov, kar je kar trikrat več kot leto pred tem. V zadnjih letih je Al Sahab v svojih video filmih začel uporabljati angleške podnapise in celo angleški jezik. Nedavno pa se je pojavil tudi video z nemškimi podnapisi.

6.2.3 Al-Furqan Institute for Media Production – Inštitut za medijsko produkcijo Al Furkan

Medtem ko je Al Sahab uradni medijski proizvajalec vodstva Al Kaide, so pripadniki njene veje v Iraku in njeni koalicijski partnerji, ki se imenujejo »Islamska država v Iraku«, ustanovili svoj ekvivalent Al Sahaba. To medijsko podjetje se imenuje Inštitut za medijsko produkcijo Al Furkan. Ustanovljen je bil konec oktobra 2006 kmalu po ustanovitvi »Islamske

države v Iraku«. Snemajo predvsem avdiovizualni material Islamske države v Iraku in ne služijo nobeni drugi skupini.

6.2.4 The Labbayk Institute for Media Production – Inštitut za medijsko produkcijo Labbaik

Organizacija za medijsko produkcijo Labbaik je prav tako relativno mlado medijsko podjetje. Zdi se, da je podjetje za medijsko produkcijo za talibane, četudi večkrat prikazujejo arabske mudžahedine, še posebej Abuja Faradža Al Libija in Abuja Naserja Al Kahtanija, kot same talibane. Njihova prva dela so se pojavila konec leta 2005, nedolgo za tem, ko sta Abu Faradž Al Libi in Abu Naser Al Kahtani pobegnila iz vojaške baze Bagram, kar ju je zelo proslavilo v skupnosti džihadistov.

Produkcijo Labbaika sestavljajo večinoma video posnetki iz Afganistana, v katerih prikazujejo usposabljanja, ideološke govore, ugrabitve in usmrtitve. Veliko posnetkov je v arabskem jeziku, nekateri novejši pa tudi v paštunskem jeziku. Najvišji voditelji Al Kaide se v njihovi produkciji ne pojavljajo, kar sproža namigovanja o rivalstvu in tekmovanju med Al Sahabom in Labbaikom.

Zadnji dve medijski podjetji, ki ju bom predstavil, se precej razlikujeta od prejšnjih, vendar sta verjetno eni najbolj zanimivih. Prvo je nekakšna organizacija z odprtim članstvom in brez posebne organizacijske strukture. Drugo pa je mednarodna agencija za novice, ki služi kot glasnik mnogih skupin džihadistov.

6.2.5 The Global Islamic Media Front (GIMF) – Globalna islamska medijska fronta

Globalna islamska medijska fronta je ena največjih in najbolj profilirana proizvajalka in distributerka džihadskega spletnega gradiva, četudi so njene zveze z vodstvom Al Kaide zelo šibke. Nikoli jim ni uspelo intervjuvati Bin Ladna. V tem smislu se precej razlikuje od Al Sahaba in je veliko bolj podobna gibanju oziroma mreži simpatizerjev. Ker imajo manj vprašanj glede varnosti kot Al Sahab, se GIMF odprto reklamira na džihadskih spletnih straneh z namenom pridobiti nove prostovoljce. GIMF je veliko bolj javen kot Al Sahab in njihovo vodstvo objavlja izjave o različnih vprašanjih.

Ker je GIMF koalicija prostovoljcev, se zdi, da ne izvaja centraliziranega nadzora nad raznolikostjo publikacij; včasih člani GIMF objavijo svoje lastne izjave.

GIMH vodi različne projekte, vključno z internetno televizijo in spletnim časopisom. Ima več serij publikacij, v katerih ponovno objavlja strokovnjake in stratege pomembnih ideologij džihada. GIMF je tudi edino džihadsko medijsko podjetje, ki izdeluje video posnetke z navodili za uporabo orožja. Tako rekoč vsi dosegljivi video posnetki usposabljanj na džihadskih spletnih straneh so sposojeni od Hezbolaha ali stranke Hizb Al Lat (džihadisti jo imenujejo hudičeva stranka) ali od drugih.

Verjetno pa je njihov najprestižnejši medij *Kanal Glas Kalifata* (CVC), džihadska spletna televizija. Občasno je začela oddajati že v drugi polovici leta 2005 z 20-minutnimi tedenskimi novicami. 20. januarja 2007 so začeli oddajati tudi video produkcijo.

Zdi se, da je Globalna islamska medijska fronta zrasla iz *Globalnega islamskega medija*, popularne skupine Yahoo! in Message board. Hitro je postala ključna spletna stran za vse gradivo, povezano z Al Kaido. Globalni islamski medij je verjetno najbolj znan zaradi objave iraškega dokumenta Al Džihad, pomembnega strateškega dokumenta, ki je priporočal teroristične napade v Španiji pred volitvami marca 2004. Dokument je v analizi napadov naveden kot možen navdih za napadalce v Madridu.

GIMF je nastal kot rezultat združitve več džihadskih medijskih skupin, ko se je oktobra 2004 Globalni islamski medijski center združil s skupino Faruk News Pulpit, direktorjem Meshavir in skupino Haqaik News Network. Kasneje je GIMF še naprej prevzemal tekmece. Na primer, nedolgo zatem ko je Firdaws Forum začel z oddajanjem spletne televizije *The Firdaws InterVision*, je bila objavljena nova združitev z GIMF-ovim Kanalom Glas Kalifata.

Če želite direktno dostopati do GIMF, vas ta oskrbi s spletno stranjo in orodji, ki omogočajo džihadskih simpatizerjem, da bi ostali anonimni.

6.2.6 Al-Fajr media Center – Medijski center Al Fajr

Vse od začetka leta 2006 se je Medijski center Al Fajr postopno uveljavil kot vrsta mednarodne džihadske tiskovne agencije, ki distribuira gradivo širokega spektra džihadskih skupin. Zdi se, da več džihadskih skupin, pa tudi druga džihadska medijska podjetja uporabljajo Medijski center Al Fajr za distribucijo svojih uradnih sporočil na džihadskem spletu. Al Fajr kot kanal novic uporablja tudi več džihadskih medijskih podjetij, vključno z Al Sahabom, Labbaikom in Al Furkanom. Pomembnost Al Fajra na džihadskem spletu je v tem,

da služi kot »dokaz avtentičnosti«. Organizacija »Islamska država v Iraku« je na primer izjavila, da uporabljajo Al Fajr izključno za distribucijo svojih uradnih sporočil.

Lastna produkcija Al Fajra je skromna. Posneli so relativno malo video posnetkov. Objavljajo časopis »Tehnični mudžahid«, ki se ukvarja z IT-vsebinami, kot je »umetnost skrivanja datotek«. Do zdaj smo videli le eno izdajo. Prav tako imajo na spletu »Interaktivne intervjuje«, kjer obiskovalci foruma postavljajo vprašanja pomembnim predstavnikom džihada. Al Fajr obljublja, da bodo poslali njihove odgovore v obliki avdiovizualnega gradiva. Včasih pa spregovorijo o lastnih stališčih. Objavili so na primer izjavo, v kateri obsojajo papežev govor o Preroku.

6.2.7 Angar

Spletna stran www.angar.com (december 2006) je objavljena v francoskem jeziku, urejajo pa jo pripadniki islamskih skupin, ki živijo v Franciji. Posodablja se večkrat dnevno, vsebuje pa podatke o dogajanju v Iraku, predvsem o trpljenju otrok in žensk. Zelo močno izstopa sovražnost do nemuslimanov in celotnega Zahoda. Zanimiva so tudi dogajanja na forumu, kjer na vprašanja na različnih spletnih straneh odgovarjajo osebe po večini z istim vzdevkom (ko si na forumu registriran, lahko dostopaš tudi do zaprtih strani, vedno pa se ob odgovoru ali podajanju mnenja izpiše vzdevek).

6.3 ZNAČILNOSTI RADIKALNIH ISLAMISTIČNIH SPLETNIH STRANI

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. Veliko spletnih strani zelo natančno in sproti spremlja vojno v Iraku, predvsem prikazujejo zločine proti Iračanom.

Teroristične skupine po drugi strani internet uporabljajo, da preko strani za druženje (facebook) iščejo podatke o zavezniških vojakih v Iraku. Vojaki si med seboj ali s svojimi družinami izmenjujejo podatke o krajih nastanitve, udeležbah v bojih, številu mrtvih vojakov, številu mrtvih sovražnikov in ocene o taktiki in dolžini njihovih bitk ipd. Terorističnim skupinam tovrstne informacije omogočajo lažjo izbiro gverilske taktike (http://www.finance.si/208119).

Zaradi širše dostopnosti različne teroristične skupine v zadnjem času objavljajo tudi besedila v angleškem jeziku. Širijo veliko propagande za vojno proti zahodnim državam, objavljajo priročnike o ravnanju z orožjem, načinih vojskovanja, načinih vojaškega urjenja ipd. Pri opisovanju različnih vrst orožja so na mnogih ekstremističnih spletnih straneh objavili povezave z uradnimi stranmi proizvajalcev orožja, kjer so ponavadi natančno opisani izdelki.

6.4 SPLETNO OKOLJE, UPORABNOST IN PRILOŽNOSTI

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[12]:

- komunikacijo,
- načrtovanje napadov,
- pripravljalna dejanja.

[12] 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.

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).

Pri tem je treba izpostaviti predvsem prikritost delovanja, ki jo omogoča spletno okolje, nesledljivost zaradi množice komunikacij in prepletenosti z drugimi vrstami digitalne komunikacijske tehnike. Zaskrbljujoča je prav tako možnost širjenja diskriminatornih vsebin, ki pozivajo k nestrpnosti in netolerantnosti. Tu pa se seveda srečamo s področjem nasilne radikalizacije in rekrutiranja (Gelbart 2007).

Spletno okolje s svojo dostopnostjo, uporabnostjo in prilagodljivostjo omogoča informacijsko disperzijo za iskanje novih rekrutirancev, nasilno radikalizacijo, omogoča jim dostop do informacij, ki jim omogočajo dostop do sredstev, potrebnih za izvršitev, in ne nazadnje si na ta način lahko pridobijo pomoč strokovnjakov s posameznih področij, npr. izdelovanje eksplozivnih naprav ipd., ter se s tem izognejo dodatnemu tveganju, ki ga predstavlja tovrstno usposabljanje (Černigoj in Gelbart 2007).

Druga povezava pa predstavlja spletno okolje kot sredstvo za izvršitev napada oz. cilj napada, kot smo to opisali v predstavitvenih poglavjih. Prvenstveno gre za dostop do podatkovnih baz ali njihovo uničenje, onesposobitev sistemov za upravljanje kritične infrastrukture, upravljanje s sistemi za izvršitev napada ipd. (Černigoj in Gelbart 2007).

Seveda je trenutno prvih primerov bistveno več. Ameriška vlada je identificirala 12 od 30 terorističnih skupin, ki vzdržujejo svoje spletne strani za konkretne namene. Takšni primeri so bili v preteklosti npr. teroristično dejanje perujske skupine Tupac Amaru v primeru napada na japonsko predstavništvo. Ne samo da je bila na njenih spletnih straneh objavljena vsebina z ideološko in politično propagando, temveč so varnostni organi takoj po napadih v ZDA in Kanadi odkrili še več spletnih strani različnih *simpatizerjev;* na eni od teh strani so našli tudi načrt napada na japonsko rezidenco (http://www.adl.org/terror/focus/16_focus_a.asp, 2. maj 2006).

Nedvomno so južnoameriška gverilska gibanja ena od najbolje tehnološko opremljenih ekstremističnih opcij[13], dokaz za to so skupine Zapatista v Mehiki, The Revolutionary Armed Forces of Colombia (FARC) v Kolumbiji ali pa npr. Shining Path (http://www.adl.org/terror/focus/16_focus_a.asp, 2. maj 2006).

Skrajne islamistične opcije spletno okolje trenutno uporabljajo za širjenje protipropagande, upravljanje z organizacijskimi strukturami, kot npr. to počne Hamas, Hizb Ut Tahrir, radikalna islamistična skupina, ki deluje v Veliki Britaniji, spletno okolje uporablja za širjenje radikalnih idej, in s tem posredno zagotavlja nasilno radikalizacijo in rekrutiranje novih simpatizerjev, ipd. Kot zelo uporabno sredstvo za uveljavljanje skrajnih idej se kaže spletno okolje tudi pri zagotavljanju finančnih sredstev (http://www.adl.org/terror/focus/16_focus_a.asp, 2. maj 2006).

Obstaja še veliko drugih skrajnih skupin, ki na ta način promovirajo radikalne ideje, širijo večvrednostne ideje, pozivajo k nepokorščini in spodbujajo k nasilnemu sprevračanju obstoječih politik ali družbeno sprejemljivih in uveljavljenih sistemov. Zanimivo pri tem je, da ima večina teh strani vzpostavljene aktivne povezave s stranmi[14], katerih vsebina se nanaša na orožje, eksplozive. Vsebina mnogih med njimi je sporna, nedovoljena ali celo prepovedana. Skladno z veljavno regulativo, ki je v različnih državah različna, bi se sicer takšna stran morala ukiniti. Nekatere od teh strani delujejo le kratek, lahko tudi za dogovorjen čas. Po ukinitvi strani se njihova vsebina objavi na drugi strani, pod drugim skrbnikom (Černigoj in Gelbart 2007).

Največjo skrb danes vzbuja tudi poskus teroristov za pridobitev gradiva in tehnologije za izdelavo orožja za množično uničevanje (jedrskega, kemičnega, biološkega, radiološkega). Sestavine in način izdelave poskušajo dobiti preko ponudnikov na spletnih straneh, kjer je mogoče dobiti veliko navodil za samo izdelavo umazane bombe[15]. Zato je še posebej

[13] Za primerjavo: Maja 1997 so npr. kolumbijskemu kartelu zasegli komunikacijsko tehnično opremo v vrednosti 10 mio. dolarjev.
[14] Za primer lahko navedemo "Terrorist's Handbook" ali "The Anarchist Cookbook".

[15] V novejšem času se vse pogosteje omenja možna ogroženost zaradi uporabe radiološke disperzivne naprave oziroma umazane bombe. Ta bi razpršila radioaktivne snovi po širši okolici.

pomemben nadzor nad spletnimi stranmi, ki ponujajo različne sestavine za izdelavo nevarnega orožja.

6.5 HEKERJI

Internetne teroriste zaradi nevednosti pogosto menjavajo s hekerji ali crekerji. Nekaj splošnih definicij, povzetih po članku »Hackers guide to protect your Internet Network« (Hekerjev vodič za zaščito interneta), nam pomaga ločiti te pojme.

Heker je oseba, ki se intenzivno zanima za skrivnosti in zapleteno delovanje računalniškega operacijskega sistema. Hekerji so najpogosteje tudi programerji. Zaradi lastnih interesov želijo pridobiti poglobljeno znanje o operacijskih sistemih in programskih jezikih. Večinoma poznajo varnostne luknje znotraj sistemov in vzroke zanje. Stalno iščejo nove izzive in znanja, svoje pridobljeno znanje pa naprej delijo z ostalimi in nikoli namenoma ne povzročajo škode (www.ods.com.ua/win/eng/security/max_security, 26. februar 2007).

Britanske varnostne službe so skozi prakso, ki je v Veliki Britaniji na tem kriminalnem področju zelo bogata, ugotovile nekakšen osebnostni vzorec storilcev tovrstnih kaznivih dejanj. Po laičnem in nekako splošnem prepričanju, ki vlada med ljudmi, naj bi bili to mlajši ljudje, stari med 14 in 16 let, zelo inteligentni, posmehovali naj bi se računalniškim varnostnim sistemom ipd. V resnici pa so ti storilci oz. "hekerji" ljudje, stari med 15 in 35 let, večinoma moški, belci, ne pretirano inteligentni – povprečno inteligentni, zanemarjeni, neurejeni ipd. Motivi, zaradi katerih se običajno lotevajo vdorov v računalniški sistem, so:

- vohunstvo,
- finančni motivi,
- trgovinske informacije (gospodarsko vohunstvo),
- občutek moči, zadovoljstvo ob pisanju o njihovem vdoru v medijih ipd. (Markovič 1997).

Hekerji v tuje računalniške sisteme vdirajo z ugibanjem gesla. Do njega prihajajo na različne načine, tudi zelo neobičajne. Tako je npr. v Angliji znan primer, da so ponoči hekerji iskali geslo (password) v košu za smeti, kamor ga je lahko skupaj s kakšnim nepomembnim lističem odvrgel uporabnik računalnika. Poleg tega se hekerji poslužujejo tudi prevar po telefonu, ko se uporabniku računalnika predstavijo za nekakšnega serviserja ali vzdrževalca računalniške mreže in tako od uporabnika izvedo njegovo geslo. Obstajajo pa tudi posebni

računalniški programi, ki hekerju omogočijo, da sam najde geslo. Ti programi izvedejo "craking" tako, da v bistvu ugibajo 200.000 besed v sekundi. Pred tem pa lahko heker sam ugiba geslo tako, da vnaša imena bližnjih sorodnikov uporabnika računalnika, kar je najbolj običajna izbira gesla med uporabniki (Markovič 1997).

Za razliko od hekerjev, ki imajo celo svoj manifest, pa crackerji vdirajo v oddaljeni računalnik ali kako drugače zlonamerno ogrožajo njegovo integriteto. Crackerji, ki pridobijo nepooblaščen dostop, uničujejo vitalne podatke, preprečujejo legitimne uporabniške storitve ali v osnovi povzročajo težave njihovim tarčam. Crackerji so z lahkoto prepoznavni zaradi svoje zlonamernosti. Ponavadi so to posamezniki ali manjše skupine, ki se želijo dokazovati. Pogosto napadajo telekomunikacijske sisteme in komunikacijska vozlišča.

Razlika med hekerji in teroristi je v tem, da imajo običajni hekerji in hektivisti znanje, sposobnosti in orodja, da bi takšen napad izvedli, vendar nimajo v sebi motivacije, da bi povzročili nasilje, hudo ekonomsko ali družbeno škodo. Po drugi strani pa teroristi, ki to motivacijo imajo, nimajo sposobnosti ali motivacije, da bi takšno škodo povzročili v kibernetskem prostoru (Denning 2000).

Izpeljano iz teh definicij bi internetnega terorista lahko definirali kot pripadnika določene teroristične skupine, ki za doseganje političnih ciljev uporablja strokovno računalniško znanje z namenom povzročiti strah, škodo ali smrt (Černigoj, Gelbart in Blažina 2007).

Nova generacija teroristov odrašča in že živi v digitalnem svetu, zato razpolaga z večjim hekerskim znanjem in veščinami in s še močnejšimi ter lažje uporabljivimi hekerskimi orodji. Novodobni teroristi bodo lahko videli večji potencial za internetni terorizem kot današnji teroristi. Lahko pričakujemo, da se bosta v prihodnje resnični in virtualni svet zelo zbližala z velikim številom naprav, priključenih na internet, in takrat bo internetni terorizem postal bolj privlačen (Denning 2001).

V zadnjem času se pojavlja vse več t. i. "usmerjenih napadov" (angl. targeted attacks) na podjetja in posameznike. To pomeni, da napadalec izdela trojanskega konja, namenjenega napadu samo na določeno spletno stran, in za uspešno obrambo ne ostane prav veliko možnosti. Delavci v javni upravi v današnjem času komunicirajo v večini primerov v Wordovih dokumentih. Uporabniki so torej navajeni, da odprejo Wordov dokument, če prihaja od znanega pošiljatelja (prijatelj, sodelavec, partnersko podjetje); naslove pošiljatelja

je dokaj enostavno ponarediti! Ko uporabnik takšen Wordov dokument odpre, se poleg dokumenta izvede tudi trojanska funkcija, ki ima vedno vključene tudi nekatere sposobnosti skrivanja pred protivirusnimi programi. Takšnega "trojanskega" dokumenta ne bo odkril noben protivirusni program, saj protivirusna podjetja sploh ne bodo vedela zanj, ker je za programe neviden (http://www.varnostne-novice.com/index.php?option=com_content&task=view&id=710).

Do zdaj največji poskus ohromitve celotnega interneta so februarja 2008 poskušali izvesti južnokorejski hekerji. Tarča napada so bili glavni strežniki, ki usmerjajo internetne povezave do spletnih strani. V torek so bili napadeni vsaj trije izmed trinajstih glavnih usmerjevalnih strežnikov. Hekerji so v tako imenovanih napadih DDos (prenatrpanje strežnikov) poskušali preobremeniti strežnike s pošiljanjem ogromnih količin podatkov v upanju, da bodo pod nenormalno količino podatkov popustili in odpovedali. Vsakega izmed treh napadenih strežnikov posebej upravljajo ameriška služba za obrambo, ICANN (organizacija za nadzor interneta) ter Ultra DNS, ki upravlja domene .org. Direktor ICANN Paul Levins je sporočil, da končni uporabniki niso opazili napada, za kar naj bi bila zaslužna dobro razpršena mreža strežnikov in homogeno sodelovanje več sto strežniških upravljavcev po celem svetu, ki so ubranili napad. Večurni napad tako ni napravil posebne škode. Če bi omenjeni strežniki popustili in odpovedali, bi to pomenilo nedelovanje ogromnega števila spletnih strani po celem svetu. Prav tako pa ne bi bila mogoča dostava elektronske pošte (Finance, 2008, http://www.finance.si/174603/Globalni_hekerski_napad_na_internet 15.december 2007).

6.6 RAČUNALNIŠKI VIRUSI

Virus predstavlja posebno vrsto računalniškega programa, napisanega z namenom, da uničuje podatke v osebnem računalniku oziroma otežuje delo s programsko opremo, ki je nameščena na osebnem računalniku. Poimenovanje "virus" izhaja iz dejstva, da je virus po tem, ko je okužil magnetni medij, težko odkriti, saj lahko preteče nekaj časa od okužbe do trenutka, ko virus začne povzročati težave (virusi, ki se zaženejo na določen datum) (http://ro.zrsss.si/ 21. marec 2007).

Z razvojem interneta pa se virusi danes prenašajo in okužujejo računalnike – magnetne medije s pomočjo elektronskih sporočil, ki imajo pripete viruse v obliki priloženih datotek, oziroma z drugimi načini izmenjave podatkov (http://ro.zrsss.si/ 21. marec 2007).

Kibernetski prostor je stalno napadan. Kibernetski vohuni, tatovi, saboterji in drugi hekerji vdirajo v računalniške sisteme, kradejo osebne podatke in poslovne skrivnosti, vandalizirajo spletne strani, sabotirajo podatke in sisteme, razpošiljajo viruse, goljufajo in nadlegujejo posameznike in podjetja (Denning 2000).

Večina teh napadov povzroči resne ekonomske posledice. Pred nekaj leti je virus ILOVEYOU povzročil škodo, ki je doletela več kot deset tisoč uporabnikov, stroški pa so bili ocenjeni na več milijard dolarjev. Napadi z virusi, zaradi katerih so bile nedostopne spletne strani internetnih podjetij Yahoo, CNN, eBay in podobnih, je povzročil več milijonov dolarjev izgube. Neposredno pa se je zaradi napada zmanjšalo zaupanje drugih podjetij in posameznikov v e-trgovanje. Zato se je zmanjšalo vlaganje v ta podjetja, cene delnic so padle (Denning 2000).

6.7 KRITIČNA INFRASTRUKTURA KOT CILJNA PRIORITETA

Kritična infrastruktura[16] skrbi za zagotavljanje osnovnih pogojev, potrebnih za nemoteno vsakodnevno življenje, je del tega sistema. Čeprav se zavedamo nevarnosti, ugotavljajo, da je 95 % vse infrastrukture, ki skrbi za zagotavljanje nemotene dobave in razpolaganje s plinom, elektriko, vodo in telekomunikacijami, neustrezno zaščitenih (Ashenden 2002).

Fred Cohen (2003) deli primarno ogrožena področja kritične infrastrukture na:

- elektro sisteme – prekinitev ali motnje v oskrbi z električno energijo, v krajšem ali daljšem časovnem obdobju je tak napad veliko bolj verjeten kot nočna mora, ki jo predstavlja direkten napad na elektrarno, katere proizvodnja energije bi ušla izpod nadzora; odgovor se skriva v tehnični rešitvi, saj so sistemi distribucije in generiranja popolnoma fizično ločeni;
- sisteme za oskrbo z vodo – računalniško nadzorovan sistem kontrole kakovosti vode, čiščenje, sistem prečiščevanja, bi zlahka postal cilj, in sicer tako, da bi s pomočjo informacijske tehnologije ponastavili parametre vsebnosti kemičnih snovi;
- zemeljski plin, naftne derivate in maziva – v večini primerov se preigravajo scenariji izpustitve, motenj v črpanju, distribuciji, požari in eksplozije …;
- sisteme kriznega reševanja – ob vzporedno scenirani nesreči bi onesposobili sistem kriznega reševanja, ki temelji na IKT in računalniški tehnologiji;

[16] Kritična infrastruktura je mreža podjetij in ustanov/javnih zavodov in drugih institucij, ki opravljajo dejavnost višjega družbenega pomena.

- finančne sisteme – po vsej verjetnosti bi bile še najhujše posledice ob napadu na pomembnejše finančne ustanove;
- sisteme javne uprave – napad na medmrežje javne uprave med volitvami ipd.

Telekomunikacije in spletno okolje – odvisnost od IKT in svetovnega spleta ali pa lokalnih računalniških mrež je nepredstavljiva. Izpad večje računalniške mreže ali spleta zaradi disperzije virusa, ki bi prodrl globoko v posamezne *intranete*, bi imel za posledico večtedenske izpade, nekateri sistemi bi bili lahko za vedno uničeni.

Niso pa omenjena npr. področja transporta, raziskovalnih inštitutov in laboratorijev, medicinske oskrbe ipd., ki jih v Sloveniji uvrščamo med kritično infrastrukturo.

Informacijsko-komunikacijske tehnologije so dobesedno prepredle svet, saj jih je mogoče najti povsod: v spalnici, v šoli, v pisarni, na ulici. "Moderne države, multinacionalne korporacije, vojaška moč, državni aparat za vzdrževanje blaginje, satelitski sistemi, politični procesi, oblikovanje naših predstav, sistemi za nadzor dela, medicinsko izdelovanje naših teles, komercialna pornografija, mednarodna delitev dela in religiozni evangelizem so tesno povezani z elektroniko" (Haraway 1999: 266).

Sodobne tehnologije s svojo vseprisotnostjo omogočajo preseganje nekoč prevladujoče hierarhične oblike družbene organizacije, saj jih uporabljajo za vzpostavljanje mrežnih oziroma rizomatičnih odnosov, kjer "komunikacija poteka od enega do kateregakoli drugega soseda, kjer stebla ali kanali ne preeksistirajo, kjer so vsi posamezniki zamenljivi , se definirajo prek nekega stanja, v nekem trenutku tako, da se lokalne operacije koordinirajo in da se končni globalni rezultat sinhronizira, neodvisno od neke središčne instance" (Deleuze in Guattari 2000: 36).

Sodobna družba deluje na način ravno takšne razsrediščenosti, fleksibilnosti in nestalnosti, kar pa predstavlja zelo ploden teren tudi za delovanje in ohranjanje sodobnega političnega in gospodarskega sistema. Sodobna oblast ni več skoncentrirana v eni točki, temveč je mrežna, razpršena in tudi s pomočjo informacijsko-komunikacijske tehnologije povsod prisotna (Foucault 2000: 99). Vsekakor ne trdim, da ni mogoče identificirati ključnih oziroma osrednjih protagonistov sodobne vladavine. Želim poudariti, da je s tem, ko ni enega vrhovnega suverena, ko je glavno gonilo družbe gospodarska rast in optimizacija produkcijskih faktorjev, ko je čut za socialna vprašanja zamenjal grob in neusmiljen boj za dobiček, rast ter

napredek, in s tem, ko neoliberalna globalizacija (re)producira nove modele neenakosti na globalni ravni, ustvarjeno izjemno negotovo in odprto polje sil kot prostor za produkcijo konstantne (globalne) ogroženosti, nevarnosti in vojne. Tukaj je tudi prostor za t. i. terorizem. V skladu z zgornjimi spremembami na družbeno-politični ravni pa se je spremenilo tudi delovanje in razumevanje vojne.

Kritične infrastrukture, to so vojaške, letalske, medicinske, energetske itd., so ranljive do neke mere. Sami računalniški sistemi so zelo ranljivi, še posebej zaradi vzajemne odvisnosti in medsebojne povezanosti (Denning 2000), tako da obstaja možnost napada. Vsi računalniški sistemi pa imajo nadzornika; vedno je prisoten človek, ki bi v primeru napada ukrepal. Dokler bo v procesih kontrole vpletenih dovolj ljudi, kibernetski terorizem ne bo resna grožnja (Pollit 1997).

6.7.1 Modus delovanja

Internetni terorizem pri napadu na kritično infrastrukturo poskuša:

- delno, v celoti, začasno ali stalno onesposobiti določen oskrbovalen sistem,
- uničiti del sistema, ki skrbi za nemoteno oskrbovanje,
- povzročiti stalne ali občasne motnje v delovanju.

Ker gre za delovanje v virtualnem okolju s posebnimi zakonitostmi ter proti ciljem, ki so lahko povezani v globalno celoto oz. zagotavljajo oskrbo tudi na globalni ravni, so lahko posledice nepredstavljive (Ashenden 2002).

6.7.2 Kdo so potencialni storilci

Vprašanje je torej, kdo bi lahko bil internetni terorist. Medtem ko si večina še vedno zatiska oči pred resnico in zanika možnost katastrof, povzročenih v sklopu internetnega terorizma, dejanska nevarnost in možnost uporabe skokovito narašča. Trenutne ocene kažejo, da se tovrstna grožnja uporablja le za izvajanje pritiska na posamezne vlade (ne toliko zaradi cilja, da bi državo popolnoma ohromili) in s tem povzročanje posebnih stanj med množicami, ki se počutijo ob tem nelagodno, povzročajo strah med ljudmi, nezaupanje v programsko in strojno opremo, nezaupanje v delovanje sistemov ipd. (Černigoj 2007).

Globalno gledano, preseki stanj in ocene tveganja kažejo, da velja kot prioriteto obravnavati potencialne uporabnike, kot so marginalne skupine, ki jih v takšno dejavnost vodijo užaljenost ali za širše množice nerazumljiva ideološka prepričanja, npr. protikapitalistične

skupine, skrajne opcije protiglobalističnih gibanj, okoljevarstveniki, zaščitniki pravic različnih manjšinskih skupnosti ipd. Tovrstne ciljne skupine imajo največkrat omejeno kvoto tako ustreznega kadra kot tudi potrebne ITT-tehnologije, zato se predvidoma raje odločajo za napad na bolj ranljive in nezaščitene cilje (Černigoj 2007).

Glede na to, da gre za množične, nedolžne žrtve, je medijski učinek še vedno dovolj velik, da omogoča *pogajalska* izhodišča izvršiteljem (Ashenden 2002).

6.7.3 Predvidevanja

Pretekle izkušnje, obveščevalni podatki in ocene tveganja kažejo, da so teroristične skupine spoznale, da lahko na takšen način izvajajo prisilo in teror na širše množice brez smrtnih žrtev. To jim omogoča bistveno prednost, saj ne izgubijo, vsaj ne v tolikšni meri, simpatije okolja. Seveda ne smemo zanemariti ocene tveganja in presekov stanj, ki npr. za območje EU pristojnim telesom še naprej nalagajo večjo skrb za zaščito kritične infrastrukture[17].

Po predvidevanjih bo do leta 2010, ko naj bi globalno internetno omrežje doseglo svoj vrh in bo kritična infrastruktura dejansko povezana v optimalnem obsegu, grožnja z uporabo računalniške kriminalitete v teroristične namene občutno narasla in postala resničnost (Ashenden 2002).

Če vzamemo pod drobnogled le območje EU, kjer trenutno potekajo napori po iskanju konsenza, ki bi omogočal vzpostavitev in vzdrževanje sistemov zgodnjega obveščanja, zagotavljanje takojšnje pomoči ob naravnih in drugih nesrečah, vzpostavitev različnih mrež in povezav za zagotavljanje zgodnjega obveščanja, zagotavljanje takojšnje pomoči v primeru katastrof ipd., vidimo, da je samo na tem področju kar nekaj ciljnih točk, ki bi lahko postale primerno ranljive tarče.

Poleg tega velja omeniti oskrbo z vedno bolj omejenimi naravnimi viri, kot so zemeljski plin in nafta, kmalu pa bo to postala tudi voda. Napad na infrastrukturo, ki omogoča nemoteno oskrbo z že tako nezadostnimi kapacitetami, bi pomenil hud udarec na globalni ravni, in ne le znotraj države ali regije. Vdor v sistem nadzora transportne infrastrukture bi lahko vodil v stanje kaosa (Gelbart in Černigoj 2007).

[17] Glej vsebino dokumenta The European Union Counter-Terrorism Strategy (14469/4/05).

Teroristi sicer uporabljajo internet kot podporo tradicionalnim oblikam terorizma, kot je na primer iskanje načinov izdelave eksplozivnih teles ali izvrševanje terorističnih napadov z njimi. Internet izkoriščajo tudi za vzpostavljanje spletnih strani, ki širijo njihove politične ali družbene cilje, pridobivajo nove člane, med seboj komunicirajo in koordinirajo napade.

Verjamem, da bo vloga interneta za radikalne islamistične skupine postala še pomembnejša. Glavni razlog je v tem, da internet postaja vodilni svetovni medij. Člani terorističnih skupin se zavedajo, da novica sama po sebi ne pomeni dovolj, če ni primerno, pompozno predstavljena.

Po drugi strani pa internet izkoriščajo tudi kot sredstvo napada, ko storilci na različne načine onemogočijo dostop do spletnih strani, bodisi državnih ustanov ali bank bodisi drugih pomembnih spletnih strani. Napadov, ki so bili opredeljeni kot internetni terorizem ali pa jih preiskovalci ali posamezne vlade niso opredelile kot terorizem, temveč kot hekerstvo, se je v zadnjem letu zgodilo kar nekaj.

6.8 INTERNETNI NAPAD NA VLADNE SPLETNE STRANI V ESTONIJI

Do zdaj edini primer internetnega terorističnega napada, ki je bil tudi pravno preganjan in storilec obsojen, se je zgodil v Estoniji.

V Estoniji je po odločitvi vlade, da bodo iz središča Talina umaknili bronasti kip vojaka Rdeče armade, prišlo do niza internetnih napadov na vladne spletne strani. Za napade so takoj obtožili ruske obveščevalne službe, vendar so uradne ruske strani vpletenost v napade takoj zanikale. Ruski varnostni organi so tudi pomagali pri preiskavi. Napadi na spletne strani ministrstev, bank in drugih javnih ustanov so trajali dva tedna. Uporabljali so program, ki je popolnoma prenatrpal strežnik in s tem onemogočil dostop do strani.

Zaradi posledic v estonskem gospodarstvu je bil za posredovanje zaprošen tudi NATO, od koder so v Estonijo poslali svoje strokovnjake za informacijsko varnost, ki so poskušali omejiti napade. Estonske banke so npr. blokirale ves internetni promet, ki je do njih prihajal iz tujine, tako da so lahko do spletnih bank dostopali samo računalniki znotraj Estonije. Napadenih je bilo več tisoč spletnih strani, pri čemer so imele nekatere promet tudi po 1000 obiskov na sekundo (prej so imele npr. 1000 obiskov na dan).

Kljub omenjenim ukrepom so se Estonci morali za nekaj časa posloviti od spletnega bančništva, spletnih nakupov, obiskovanja svetovnega spleta in prebiranja pošte.

S pomočjo ruskih varnostnih organov so prijeli storilca, študenta Dmitrija Galuškeviča, ki je v znak protesta zaradi odstranitve spomenikov iz dobe sovjetske okupacije iz svojega računalnika sprožil internetne napade na estonske spletne strani iz računalnikov po celem svetu.

Dmitrij Galuškevič je bil prva oseba, ki je bila obsojena zaradi udeleževanja v tako imenovani "cyber vojni" proti Estoniji, obsojen je bil na denarno kazen v višini 17.500 estonskih kron ali nekaj manj kot 1000 evrov (Varnostne novice).

6.9 HEKERSKI NAPAD NA PENTAGON

Junija 2007 je neznanemu hekerju uspelo vdreti v e-poštni sistem ameriškega ministrstva za obrambo, zaradi česar so bili v Pentagonu prisiljeni onemogočiti 1.500 e-poštnih računov. Pentagon je sicer vsak dan tarča nekaj sto hekerskih napadov, ki pa so redko uspešni. Običajno gre za napade "rekreacijskih hekerjev, namišljenih kibernetskih odpadnikov ter različnih nacionalističnih ali ideologističnih skupin".

Sprva so predstavniki Pentagona močno zmanjšali pomen napada, češ da je prizadel samo nerazvrščena elektronska sporočila ministrove pisarne in da ne pričakujejo škodljivega vpliva na delo ministrstva. Kasneje se je izkazalo, da je bil škodljivi vpliv junijskega napada veliko večji, kot so domnevali, saj so si hekerji prisvojili podatke iz elektronskih sporočil zaposlenih.

Vdor so na Pentagonu odkrili med rednimi vzdrževalnimi deli na informacijskem sistemu. Do takrat je bila škodljiva koda v računalniškem sistemu nameščena že vsaj dva meseca, pri razširjanju pa je izkoriščala znano varnostno luknjo v Microsoftovem operacijskem sistemu Windows. Črv se je razmnoževal s pomočjo elektronske pošte iz enega sistema na mreži v drugega. Sporočila so bila sleparska, videti pa so bila kot sporočila enega od sodelavcev. Ko je prejemnik okuženo elektronsko pošto odprl, je črv v domačo bazo poslal geslo in uporabniško ime prejemnika.

6.10 HEKERSKI VDOR V SPLETNI SISTEM DRŽAVNEGA IZPITNEGA CENTRA

Tudi slovenski internetni prostor ni imun na hekerske napade. Poleti 2007 so do zdaj neznane osebe vdrle v spletni sistem Državnega izpitnega centra. Z napadom so hekerji odprli nekatere strani, ki so sicer dostopne le z geslom. Hekerji z vdorom niso mogli dostopati do baze s podatki o učencih, saj naj bi bila za to potrebna posebna gesla. Lahko so le pregledovali ankete o številu ustnih izpitov ter seznam maturantskih seminarskih nalog.

Državni izpitni center je doživel dva hekerska napada. Prvi je trajal kar 12 ur, med napadom pa je bilo zabeleženih 2500 dostopov v sistem. Drugi je bil krajši, trajal je štiri ure. V preiskavi so identificirali IP-naslove napadalcev, ki so prihajali iz tujine.

Napad je pokazal slab sistem varovanja osebnih podatkov. Sicer je sistem zaprt za vpisovanje podatkov, tako da se teh ne da spreminjati. Pomanjkljivosti sistema se kažejo predvsem v primerih, ko uporabnik izgubi geslo. Novega je namreč mogoče pridobiti preko elektronske pošte, pri čemer je treba navesti osebne podatke ravnatelja šole.

Seveda v tem primeru nikakor ne moremo govoriti o terorizmu, je pa meja med hekerji in teroristi zelo tanka. Glavna razlika je le v motivu in ideologiji. Na žalost je na podoben način kot sistem Državnega izpitnega centra zaščitenih še veliko zaprtih spletnih sistemov v Sloveniji, ki vsebujejo osebne podatke. Če jih je napad na Državni izpitni center opozoril na nevarnost in so svoje sisteme varnostno posodobili, do podobnih napadov v Sloveniji ne more priti. Konec koncev gre vedno za to, koliko so skrbniki zaprtih spletnih sistemov pripravljeni vložiti v varovanje svojih sistemov, tako finančno kot strokovno. Na žalost jih k sodobnim varnostnim posodobitvam nihče ne more prisiliti.

7 DELOVANJE VARNOSTNIH ORGANOV

Preiskovanje internetnega kriminala in terorizma 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. Spopad pomeni predvsem veliko mero strokovnega znanja s področja računalništva in informatike in tudi psihoanalitične metode (izdelava psiholoških profilov storilcev), potrebne za odkrivanje storilcev tovrstnih dejanj. Ravno zato je na tem področju najpomembnejše usposabljanje, predvsem v smeri uporabe določene računalniške opreme in računalniških programov za pridobitev znanja o informacijskih sistemih. Preiskovalci morajo biti zelo iznajdljivi – slediti morajo iznajdljivosti storilcev. Računalniška kriminaliteta se širi bliskovito, zato so usposabljanja nujna. Še pred nekaj leti je bil problem, kako pravilno zaseči in uskladiščiti dokazno računalniško opremo. Vsaj takih problemov preiskovalci danes nimamo več. Zaradi tehnične narave te vrste kriminalitete in terorizma so potrebne policijske enote, specializirane za odkrivanje tovrstnih zlorab. Nujno je tudi mednarodno policijsko sodelovanje in sodelovanje z računalniškimi strokovnjaki (Vodušek 1992 in Zupančič 1997).

Zavedati se moramo, da je večina radikalnih islamističnih strani, ki širijo teroristično propagando, dostopnih le kratek čas. Spletni naslov in s tem možnost dostopa in zavarovanja dokazov se spreminja zelo hitro. Mnogo lažje je slediti propagandi tradicionalnih spletnih strani, ki besedila objavljajo že dlje časa, tako poznamo matično spletno stran, ki si je teroristi niti ne želijo spreminjati, in po ključnih besedah lahko spremljamo tudi »stranske spletne strani«, na katerih so objavljeni konkretni pozivi, ki so dostopne le nekaj ur.

Globalizacija zahteva okrepitev skupnega mednarodnega boja proti terorizmu na vseh ravneh. Izjema ni niti skupni boj proti internetnemu terorizmu. Skoraj ni več države, ki je ne bi (ne)posredno ogrožali napadi, usmerjeni v zastraševanje prebivalstva in institucij, z namenom spremeniti ali uničiti sedanje politične, ekonomske ali socialne strukture. Sodobni teroristi delujejo nadnacionalno in so organizirani v sofisticirano koordinirane mreže, ki izkoriščajo geografske meje odkrivanja in preiskovanja ter prednosti močne logistične in finančne podpore iz različnih virov (Švarc 2004).

Terorizem v zadnjih letih postaja največja varnostna grožnja. Priča smo velikim spremembam tako v delovanju kot organizaciji terorističnih skupin; ena glavnih značilnosti sodobnega terorizma nasploh pa je njegova mednarodna oziroma globalna komponenta ter

nepredvidljivost, kar otežuje učinkovit boj proti njemu. Sodobni teroristi pri organizaciji napadov uporabljajo najsodobnejše tehnologije. Da bi dosegli določene cilje ali samo zaradi svoje ideološke usmerjenosti pa se t. i. novodobni teroristi vse pogosteje povezujejo tudi z mednarodnimi kriminalnimi združbami.

Zaradi vseh nevarnosti mednarodnega kriminala in terorizma je nujno mednarodno sodelovanje policij pri odkrivanju in zatiranju tovrstne kriminalitete. Zakonodaje držav so glede na stopnjo njihovega ekonomskega, družbenega in pravnega razvoja zelo različne, kljub temu pa je na mednarodnopravnem področju mogoče najti nekaj skupnih kazalnikov, katera so tista kazniva dejanja, ki so – zaradi nevarnosti, ki jo pomenijo – deležna največje pozornosti tako teoretikov kot praktikov. Brez dvoma so to terorizem, kazniva dejanja organizirane kriminalitete ter korupcija, goljufije in pranje denarja.

Na podlagi sodelovanja si države izmenjujejo svoje znanje in podatke o načrtovanih ali storjenih terorističnih akcijah, vanje vpletenih osebah in o načinih izvedbe in tehničnih sredstvih, uporabljenih v takšnih dejanjih. Prav tako si izmenjujejo znanje in podatke o terorističnih skupinah in njihovih članih, ki načrtujejo ali so izvedli svoja dejanja na območju države članice Evropske Unije, njeno škodo in proti njenim interesom, pri čemer bodo takšne informacije koristile za boj proti terorizmu in preprečevanje nasilnih kaznivih dejanj.

Po sklepu Sveta EU o posredovanju informacij, ki izhajajo iz dejavnosti varnostnih in obveščevalnih služb v zvezi s kaznivimi dejanji terorizma, je terorizem postal mednarodna nevarnost, ki je nobena država članica ne more reševati sama. EU razvija protiteroristično politiko, s katero se države članice skupaj borijo proti terorizmu, z enako odločnostjo, zavzetostjo in spoštovanjem človekovih pravic in temeljnih svoboščin. Sprejeti so bili pomembni zakonski ukrepi in politike za pomoč Evropski uniji pri preprečevanju terorizma in boju proti njemu. Zlasti pomembno je, da je Evropski svet sprejel akcijski načrt EU za boj proti terorizmu. Opravljen je bil tudi medsebojni pregled ureditev po vsej EU za boj proti terorizmu v vsaki državi članici.

Na teroristične napade na ozemlju EU in po svetu ter na povečano aktivnost mednarodnih terorističnih združb se je EU odzvala s sprejetjem Okvirnega sklepa o boju zoper terorizem z dne 13. junija 2002. Okvirni sklep je določil usklajeno definicijo terorističnih kaznivih dejanj, vendar pa se je pozneje izkazalo, da je treba njegove določbe nujno dopolniti, zlasti zaradi pojava novih oblik teroristične dejavnosti oziroma dejavnosti, ki so s terorizmom neposredno

povezane. Gre predvsem za tiste oblike, ki jih omogoča internet. Preko sodobnih komunikacijskih sredstev je namreč mogoče na lahko dostopen način, ki doseže katerokoli območje zemeljske oble, širiti propagandne dejavnosti za promocijo terorističnih dejanj, novačenje novih privržencev terorističnih dejavnosti, s tem povezano dajanje ustreznih navodil za usposabljanje, planiranje in izvajanje terorističnih dejanj. Na ta način se torej lahko širi in krepi teroristična indoktrinacija in pridobiva nove člane oziroma pripadnike mednarodnih terorističnih organizacij[18].

Pri zakonodajni oblasti v večini pravno urejenih držav se pogosto pojavlja vprašanje, do kolikšne mere lahko policija zakonito nadzoruje računalniška omrežja. Pogosto razumevanje večine držav je, da se lahko policisti vedejo tako, kot se vedejo državljani, ko vstopajo v kibernetski prostor ter v njem raziskujejo in nato shranjujejo različne informacije, ki jih najdejo. V primeru, da policisti preiskujejo kazniva dejanja na internetu, morajo za to imeti ustrezna dovoljenja sodišča. Seveda morajo predlog za poseg v zasebnost posameznika ustrezno utemeljiti pristojnemu državnemu tožilcu, ta pa pristojnemu preiskovalnemu sodniku (določila ZKP). Običajno s pridobivanjem dovoljenj v RS ni težav. Imamo storilca, ki izvaja kazniva dejanja v Sloveniji, materialna škoda je nastala v Sloveniji, tako da je utemeljitev za uporabo določil ZKP dovolj. Poseben problem pa nastane, ko gre za transnacionalni kriminal ali terorizem, ker se zakonodaja od države do države razlikuje, preiskovalne prakse, ki so v eni državi ustaljene, so v drugi po njihovi zakonodaji nesprejemljive. Predvsem zaradi kršitev osebnih podatkov. V takih primerih pa ima ključno vlogo za izmenjavo podatkov v mednarodnem prostoru Europol (Sieber 1998).

7.1 UREDITEV PREISKOVANJA INTERNETNEGA KRIMINALA V REPUBLIKI SLOVENIJI

V sodobnem varnostnem okolju si je težko zamisliti skrb za nacionalno varnost le s samostojnim prizadevanjem državnih služb. Varnost ni več omejena samo na posamezne države, temveč vse bolj presega meje držav. Države se vse bolj povezujejo, sklepajo različna multilateralna in bilateralna sodelovanja na področju zagotavljanja varnosti, tudi na področju policijskega sodelovanja.

[18] Dokument je bil obravnavan v okviru delovne skupine TWG v okviru Sveta EU med slovenskim predsedovanjem EU.

Slovenska policija aktivno sodeluje v številnih pomembnih mednarodnih organizacijah in ustanovah, kot so:

- PWGT (Police Working Group on Terrorism),
- INTERPOL,
- EUROPOL,
- SECI Center (South Eastern Cooperative Initiative),
- TWG (delovna skupina za terorizem v okviru Sveta EU).

Pri mednarodnem sodelovanju se pojavljajo ovire zaradi različnih nacionalnih pravnih redov, ki ščitijo osebne podatke in njihovo izmenjavo z ostalimi članicami, ter pri različnih sistemskih ureditvah boja proti terorizmu (pri nekaterih državah je npr. mogoč t. i. predhodni postopek, pri katerem policija pod vodstvom tožilstva že izvaja prikrite preiskovalne ukrepe kljub obstoju le »suma« terorizma – pri nas je za to potreben višji prag, tj. utemeljeni razlogi za sum in dovoljenje sodišča, ne pa tožilstva), težave se poleg tega pojavljajo tudi pri pravnem obravnavanju in kvalifikaciji tako pridobljenih informacij tujih varnostnih organov, ki pa ne dosegajo pravnih standardov za kazenski pregon v RS.

V RS je za preiskovanje kaznivih dejanj, povezanih z internetnimi kaznivimi dejanji, in terorizma zadolžena Uprava kriminalistične policije. Njene glavne naloge na področju boja proti terorizmu so:

- spremlja varnostne razmere v RS in tujini;
- pridobiva, analizira in vrednoti operativne podatke;
- odkriva in preiskuje sume različnih oblik terorističnih dejavnosti ali uporabe orožja za množično uničevanje;
- spremlja izvajanje določil Zakona o nadzoru izvoza blaga z dvojno rabo in Zakona o tujcih v povezavi s sumom izvajanja teroristične dejavnosti ter o ugotovitvah obvešča pristojne nadzorne in inšpekcijske organe;
- v primeru podanega suma storitve kaznivih dejanj spremlja odklonska delovanja skrajnih gibanj;
- sodeluje pri pripravi in oblikovanju zakonskih aktov doma in v EU;
- sodeluje v mednarodnih pobudah in telesih na osnovi bi- in multilateralnih sporazumov s področja sodelovanja pri preprečevanju organiziranega kriminala in terorizma;

- sodeluje v večini teles EU, ki se ukvarjajo s terorizmom na področju III. stebra ter v posameznih projektih Evropske komisije in Sveta EU.

Slovenska policija je prve primere računalniške kriminalitete obravnavala že leta 1993, bolj sistematično pa se je s tem začela ukvarjati leta 1995, ko je bil sprejet nov KZ RS. Leta 2000 je bila ustanovljena prva specializirana enota na državni ravni, od leta 2002 pa imamo kriminaliste, ki se ukvarjajo z računalniško kriminaliteto. Zaradi lažjega odkrivanja takšnih storilcev je policija vzpostavila zelo dobro sodelovanje z različnimi inštitucijami, tako državnimi kot zasebnimi, tako na mednarodni kot tudi na domači ravni. Za obveščanje javnosti o pasteh in o nevarnostih pri uporabi interneta je policija v letu 2006 izdala brošuro "Varni na internetu«, ki je dostopna na spletni strani policije, in sicer na naslovu: http://www.policija.si/si/szj/pdf/2006/varniNaInternetu.pdf.

7.2 VLOGA EUROPOLA PRI PREISKOVANJU INTERNETNEGA TERORIZMA

Konvencija o Europolu predvideva pravni okvir, ki državam članicam zagotavlja, da z Europolom delijo informacije o terorizmu. Informacije, ki izvirajo iz dejavnosti nacionalnih varnostnih in obveščevalnih služb, načeloma niso izključene iz posredovanja Europolu. Vendar v svojem poročilu Svetu o izvajanju Akcijskega načrta EU za boj proti terorizmu[19] Europol opisuje, da se podatki s področja varnostnih in obveščevalnih služb Europolovim delovnim datotekam za analizo o terorizmu ne zagotavljajo strukturirano. V ocenjevalnem poročilu o drugi delovni skupini za boj proti terorizmu[20] Europol ocenjuje, da večina podatkov, ki jih države članice prispevajo v ustrezne delovne datoteke za analizo in projekte delovne skupine za boj proti terorizmu, prihaja od organov pregona, in ne od varnostnih in obveščevalnih agencij.

Vodilno vlogo v boju proti internetnemu terorizmu na območju EU ima Europol. Pri Europolu je bila ustanovljena skupina specialistov za boj proti terorizmu, ki ima naloge zbiranja informacij o terorističnih grožnjah, analizo, izdelavo ocene groženj z navedbo možnih ciljev, škode, načina izvršitve, posledic za varnost v državi. Strokovnjaki imajo podporo obstoječih služb, npr. služb za terorizem, analize, finance, informacijsko tehnologijo, varnost (Dobovšek 2002).

[19] Objavljeno v 9156/05 JAI 178.
[20] Objavljeno v 12992/05 EUROPOL 33.

Vsaka država članica ima na sedežu Europola v Haagu svojo nacionalno enoto, v kateri deluje vsaj en oficir za zvezo[21]. Vloga Europola je pospeševanje in usklajevanje sodelovanja ter skrb za učinkovitost in sodelovanje organov, pristojnih za odkrivanje in preiskovanje. Konvencija o Europolu je tudi določila vrsto kaznivih dejanj, pri odkrivanju katerih se mora angažirati Europol. Sprva je bilo delovanje Europola osredotočeno le na boj proti mamilom, z uveljavitvijo Konvencije o Europolu pa se je delovanje Europola razširilo na čedalje hujše oblike mednarodnega kriminala, ki so navedene v Prilogi Konvencije o Europolu. Tako v Europolovo pristojnost spadajo terorizem in huda kazniva dejanja zoper življenje in telo, osebno svobodo in premoženje, računalniški kriminal, kazniva dejanja nedovoljene trgovine z mamili ter jedrskimi in radioaktivnimi snovmi ter vozili, ilegalne migracije, trgovina z ljudmi ter pranje denarja in s pranjem povezana kazniva dejanja, ta kazniva dejanja pa se na kakršenkoli način tičejo dveh ali več držav članic EU (Brezigar 2005).

S članstvom v Europolu ima vsaka država možnost hitre izmenjave podatkov in informacij. Zagotovljeno je, da ima vsaka država, ki preiskuje določen primer, dostop do želenih podatkov, ki lahko v veliki meri pripomorejo k uspešnosti preiskovalnih dejavnosti. Zagotovljeno je tudi, da se kriminalistični obveščevalni podatki, pridobljeni v posamezni državi, ne izgubijo, temveč se jih vključi v Europolove baze podatkov, kjer so na voljo tudi drugim državam članicam.

Notranji ministri EU so aprila 2008 v Luksemburgu dosegli politično soglasje o sklepu Sveta o ustanovitvi Europola. Sklep bo nadomestil Konvencijo o Europolu, s čimer bo Europol ostal ena od agencij EU, izveden pa bo tudi prehod z medvladnega financiranja na financiranje iz proračuna Skupnosti, pri čemer bodo stroški ostali nespremenjeni. Europol zagotavlja podporo preiskav znotraj preiskovalnih skupin v okviru svojih pristojnosti, ki mu jih je do zdaj dajala Konvencija o Europolu. Danes v praksi obstajata dva načina Europolovega vključevanja v podporo posamezni preiskavi:

- Prvi način je podpora skozi odprtje AWF (Analitic Work File – analitična delovna datoteka).
- Drugi način pa je neposredna Europolova podpora skupne preiskovalne skupine oziroma posamezne države članice, ki zaprosi za pomoč. Na podlagi te podpore (pomoč pri koordinaciji, tehnična sredstva, analize, zagotavljanje raznih znanj itd.) se lahko države članice in Europol naknadno odločijo za odprtje AWF, ki služi kot okvir za zbiranje in analiziranje vseh podatkov, pridobljenih s preiskovalnim delom skupne

[21] Republika Slovenija ima trenutno dva oficirja za zvezo.

preiskovalne skupine. Analize iz take AWF pa potem pomagajo usmerjati samo preiskavo znotraj skupne preiskovalne skupine (Potparič 2006).

Na podlagi analiz lahko Europol ugotovi, da ima preiskovana zadeva širše razsežnosti in da je treba v zadevo vključiti tudi druge države članice. Tako lahko Europol na podlagi priporočila Sveta z dne 28. septembra 2000 državo članico zaprosi za začetek preiskave v določeni zadevi. Države članice naj bi tako pobudo preučile in ukrepale, v primeru, da ne sprejmejo nikakršnih ukrepov, pa o svoji odločitvi in razlogih zanjo obvestile Europol (Potparič 2006).

Protokol, ki ureja sodelovanje Europola v skupnih preiskovalnih skupinah, je med drugim omenjeno priporočilo Sveta nadgradil in določil, da so države članice dolžne preučiti pobude Europola glede začetka kriminalistične preiskave v določenih zadevah ter o svoji odločitvi in sprejetih ukrepih obvestiti Europol. Tako se je Europol, katerega nastanek je bil deležen velike stopnje nezaupanja[22], prebil iz operativne in institucionalne izolacije. Europol je postal več kot le posrednik kriminalističnih obveščevalnih podatkov. Skozi kasnejše odločitve Sveta je postala vloga Europola v skupnih preiskovalnih skupinah še bolj okrepljena predvsem s tem, da naj Europol ne bi bil pooblaščen le za dajanje pobud za nove preiskave, temveč da bi lahko dajal pobude tudi za ustanovitev skupnih preiskovalnih skupin (Potparič 2006).

7.3 EVROPSKA AGENCIJA ZA VARNOST OMREŽIJ IN INFORMACIJ – ENISA

Evropska agencija za varnost omrežij in informacij (ENISA – European Network and Information Security Agency) deluje kot strokovni center za države članice in institucije EU, ki nudi nasvete o vprašanjih varnosti omrežja in informacij.

ENISA kot taka podpira sposobnost držav članic, institucij EU in gospodarstva, da preprečujejo probleme varnosti omrežij in informacij, jih obravnavajo in se odzivajo nanje.

[22] Ob nastajanju Konvencije o Europolu so države članice nasprotovale temu, da se Europol oblikuje po vzoru FBI, in sicer iz različnih razlogov. Nekatere države so menile, da je tak tip operativne policijske sile obstajal vedno v obdobju diktatorstva (Francija pod Napoleonom in Nemčija pod Hitlerjem). Nekatere druge države pa so menile, da policijska organizacija, kot je FBI, ne spada v evropski kontekst, ker je tu popolnoma druga ustavna ureditev (LeBeuf 2002: 57).

V ta namen so dejavnosti ENISE osredotočene na:

1. svetovanje in pomoč Komisiji in državam članicam glede varnosti informacij ter glede obravnavanja težav, povezanih z varnostjo strojne in programske opreme, v sodelovanju z industrijo;
2. zbiranje in analiziranje podatkov o dogodkih na področju varnosti v Evropi in nastajajočih tveganjih;
3. pospeševanje metod za ocenjevanje tveganj in obvladovanje tveganj, da se okrepi naša sposobnost za odziv na groženje v zvezi z varnostjo informacij;
4. izmenjava najboljših praks v zvezi z ozaveščanjem in sodelovanjem med različnimi akterji na področju varnosti informacij, predvsem z razvijanjem javnih ali zasebnih partnerstev z industrijo na tem področju;
5. spremljanje razvoja standardov za proizvode in storitve za varnost omrežij in informacij.(http://europa.eu/agencies/community_agencies/enisa/index_sl.ht).

Varnostna agencija ENISA je bila ustanovljena leta 2004 kot začasni organ s ciljem nadzora nad varnostjo na internetu. Mandat naj bi ji potekel leta 2009, vendar Evropska komisija načrtuje podaljšanje vsaj do leta 2011. Komisija si tudi prizadeva, da bi delovanje te agencije združili z organi za regulacijo na področju telekomunikacij, kar je predmet številnih polemik v evropskem parlamentu (www.sta.si 12. junij 2008).

Cilj agencije je doseči zadostno raven varnosti in zakonskih obvez za uporabnike ter ponudnike storitev, s katerimi bi lahko zagotovili nemoten pretok informacij. Iz tega naslova nameravajo svoje delovanje razširiti tudi na področje boja proti nezaželeni pošti, ki danes v EU po nekaterih ocenah obsega že 94 % vse elektronske pošte.

8 ZAKLJUČEK

Za teroristične skupine je uporaba nasilja zadnje sredstvo za dosego ciljev. Nasilni cilji so obrnjeni v prihodnost, predstavljajo pa odgovor na neko preteklo nepravilnost (razpad sistema vrednot, družbene krivice ipd.). Sam terorizem je redkokdaj zadosten za uresničitev političnih ciljev. Pokazal pa se je kot zelo učinkovit dodatek v političnem konfliktu. V 20. stoletju se je izkazalo, da je z njim mogoče doseči zastavljene cilje, kar je tudi razlog za uporabo terorizma kot metode boja. Tudi večji teroristični napadi v zadnjih letih so z malo stroški dosegli veliko gospodarsko in politično škodo, dosegli pa so maksimalno publiciteto.

Vprašanje grožnje internetnega terorizma obstaja na dveh ravneh: ali so kritične infrastrukture, ki so možna tarča takih napadov, ranljive in v kolikšni meri so teroristi usposobljeni za tak tip terorizma. Kritične infrastrukture, kot so vojaške, letalske, medicinske, energetske itd., so ranljive do neke mere.

Ameriška vlada je zaradi strahu pred internetnim terorizmom zahtevala dodatnih 4,5 milijarde dolarjev za infrastrukturo, ki bi Združene države Amerike varovala pred nevidnimi sovražniki, ki se skrivajo globoko v navideznem bitnem svetu. Ravno taki ukrepi vplivajo na to, da se internetni terorizem po mnenju javnosti uvršča visoko na lestvici možnih groženj, ki pretijo ZDA. Joshua Green[23] (www.washingtonmonthly.com/features/2001/0211.green.html) je prepričan, da imajo ljudje, predvsem Američani, latentni strah pred katastrofalnim računalniškim napadom že od časa, ko je najstniški Matthew Broderick vdrl v Pentagonov sistem jedrskega orožja in skoraj sprožil tretjo svetovno vojno v filmu iz leta 1983 z naslovom War Games (Vojne igre). Sodeč po javni obravnavi in časopisnih naslovih so tovrstni scenariji v današnjem času še toliko bolj mogoči.

Teroristične skupine sicer uporabljajo internet kot podporo tradicionalnim oblikam terorizma, kjer se naučijo različnih načinov izvedbe terorističnega napada, kot so 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.

[23] Urednik publikacije Washington Monthly.

Zaradi vedno večje uporabe interneta kot prostora za komuniciranje, trgovanje in izmenjavo informacij je zakonodaja na področju obnašanja na spletu vedno bolj pomembna. Tradicionalno je zakonodaja identificirala in kontrolirala družbeno obnašanje z nadzorom in kaznovanjem. Internetni kriminal pa je veliko bolj zapleten. V nasprotju z zločini v fizičnem svetu je te težko opazovati in so ločeni od fizičnega telesa (Thomas 2000: 202).

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, da **mednarodne teroristične skupine uporabljajo internet kot propagandni pripomoček in za pridobivanje novih članov (rekrutacija),** lahko potrdim. Teroristične 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 (Tuman 2003). Število sporočil na internetu se stalno povečuje. Teroristi 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. Grožnje, obglavljanja zahodnih talcev v Iraku, pozivi k umorom – vse to se z bliskovito hitrostjo prek spleta širi med internetnimi uporabniki.

Terorizem in internet sta povezana z več vidikov. Prvič, internet je postal forum teroristov za širjenje svoje ideologije in s tem novačenje ter mobilizacijo novih članov, zbiranje finančne in materialne podpore, za širjenje sporočil sovraštva in nasilja (objavljanje in propagandno dejavnost), iskanje informacij, psihološko bojevanje, načrtovanje in koordinacijo dejavnosti ter za medsebojno komunikacijo, ki omogoča neposredno operativno in taktično zagotovitev akcijam (posredovanje navodil privržencem). Drugič, posamezniki in skupine poskušajo napasti računalniška omrežja, vključno s tistimi na internetu – internetni terorizem (Weimann 2004).

Teroristične skupine z uporabo interneta obveščajo in opozarjajo javnost na svojo prisotnost, objavljajo propagandno gradivo, hkrati pa opravičujejo izvedene klasične teroristične napade s tem, da opozarjajo na pokole nad civilnim prebivalstvom v Iraku.

Drugo hipotezo, da **se je s pomočjo interneta spremenilo komuniciranje med teroristi, da jim omogoča komunikacijo in dajanje napotkov razpršenim celicam organizacij,** lahko ravno tako potrdim. Internet je ne le propagandni pripomoček, ampak tudi sredstvo za komunikacijo med člani terorističnih organizacij. Vse bolj je uporaben za zbiranje kapitala, finančne transakcije in za ostale organizacijske potrebe.

Teroristične organizacije internet vse pogosteje uporabljajo za organiziranje, motiviranje, komuniciranje, vpliv na javnost kot pa za izkoriščanje ranljivosti informacijsko razvitih držav.

Internetni terorizem je novo področje delovanja terorističnih skupin in posameznikov. Spoznavajo, da so profesionalne in intelektualne sposobnosti posameznikov pomembnejše od fizične pripravljenosti in tudi delovanje je težje zaznavno. Investicija v človeške in materialne vire je minimalna. Spremenila se je tudi starost storilcev, mladina je veliko bolj dojemljiva za internetni medij (Karmon 2001).

Teroristične skupine internet uporabljajo tudi za psihološko propagando. Uporabljajo ga lahko za širjenje napačnih informacij, razširjajo grožnje, namenjene povzročanju strahu in nemoči ter širjenju strašnih predstav o svojih akcijah (Weimann 2004). Kot način komuniciranja člani terorističnih skupin uporabljajo različne klepetalnice, ki so ena od storitev interneta, pri kateri je omogočeno neposredno komuniciranje med točno določenimi uporabniki (Svete 2005). Klepetalnice pripomorejo tudi k navezovanju stikov s potencialnimi novimi člani.

Za spletne strani, ki jih upravljajo teroristične skupine, je značilna velika dinamika. Spletne strani se nenadoma pojavijo, pogosto spreminjajo obliko in nato nenadoma izginejo. Velikokrat se samo zdi, da izginejo, dejansko pa le spremenijo spletni naslov in obdržijo precej podobno ali enako vsebino (Weimann 2004b).

Tudi tretjo hipotezo, da so **države EU ustrezno zakonsko spremenile strategije varnostnih organov za preprečevanje tovrstnega terorizma,** lahko potrdim. V boju proti internetnemu terorizmu je pomembno izbrati prave ukrepe; če so premili, opogumijo teroriste; če so preostri, pa imajo lahko nasprotni učinek. Najprej moramo razumeti nevarnost, ki jo internetni terorizem pomeni. Poudarek mora biti na učinkovitosti, ne pa na številu instrumentov, ki so namenjeni zatiranju terorizma, saj v praksi prihaja do vedno večjega prepada med odločitvami in implementacijo teh odločitev. Za boj proti terorizmu so

na področju Evropske unije prvenstveno odgovorne države članice. Zlasti po terorističnih napadih na ZDA so države članice EU povečale mednarodno sodelovanje, ravno tako pa so okrepile tudi lastno protiteroristično delovanje. Ponovno so preverile svoje protiteroristične zmogljivosti, sprejele so novo zakonodajo, dodelile so dodatna finančna sredstva, okrepile osebje za krepitev protiterorističnega delovanja, tudi s poudarkom na preprečevanju internetnega terorizma.

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.

Na koncu lahko ugotovimo, da je tudi pravna ureditev boja proti terorizmu 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 prve korake k učinkovitemu izvajanju teh mednarodnih dokumentov.

Žrtve terorizma od svojih vlad in mednarodne skupnosti legitimno pričakujejo pregon storilcev, povrnitev škode in zaščito pred prihodnjimi napadi. Države svojo dolžnost zaščite lastnih državljanov pred mednarodnim terorizmom zato upravičeno jemljejo zelo resno. Boj proti mednarodnemu terorizmu ni le boj za varnost, temveč tudi boj za temeljne vrednote in svoboščine, ki gradijo temeljno identiteto demokratičnih družb in ki jih terorizem sistematično ogroža (Švarc 2006). Zakonodaja na področju preprečevanja vseh vrst terorizma, tudi internetnega, se je po terorističnih napadih v Madridu in Londonu ter več poskusih napadov v državah EU spremenila in prilagodila novim trendom.

Trenutno še ni primera, da bi terorist kogarkoli ubil s pomočjo uporabe računalniške tehnologije. Tudi pri svetovno najbolj znani teroristični organizaciji, Al Kaidi, ameriški vojaki med odkritjem baze, opremljene z visoko napredno računalniško tehnologijo, niso odkrili dokazov, da bi organizacija s pomočjo računalnikov pripravljala resno uničevalno akcijo. Še več, računalniški strokovnjaki so prepričani, da je z uporabo interneta dejansko nemogoče povzročiti smrt posameznika, kaj šele večje skupine ljudi. Dorothy Denning (Schmit 2001:

70–105), ameriška profesorica in strokovnjakinja za kibernetsko varnost, pravi: "Ponoči spim in me ni strah napadov iz navideznega sveta, ki bi mi lahko uničili življenje. Ne samo da se internetni terorizem ne uvršča med kemične, biološke ali jedrske napade, ampak ni niti približno podoben drugim potencialnim fizičnim grožnjam, kot so avtomobilske bombe ali samomorilski bombni napadi."

9 LITERATURA

1. ANŽIČ, Andrej (1997): *Varnostni sistem Republike Slovenije*. Ljubljana: Časopisni zavod Uradni list RS.
2. ASHENDEN, Debi (2002): *CYBER TERRORISM & Threat to Critical National Infrastructures*. INTERSEC 12. (11/12).
3. ARMSTRONG, Helen in Paddy FORDE (2003): Internet Anonimity Practices in Computer Crime. *Information Management & Computer Security* 11(5), 209–215.
4. BELIČ, Igor (2001): Informacijski terorizem. *Varstvoslovje* 3(4), 262-268.
5. BREZIGAR, Barbara (2005): *Eurojust in druge institucije EU za koordinacijo in sodelovanje pri boju proti čezmejnemu kriminalu.* Ljubljana: GV Založba, d. o. o.
6. BALLARD, James David, Joseph G. HORNIK in Douglas McKENZIE (2002): Technological Facilitation of Terrorism, Defenition, Legal, and Poicy Issue. *American Behavioral Scientist* 45 (6), 989-1016.
7. CHALK, Peter (1996): *West Europian Terrorism*. London: Hampshier RG21.
8. COHEN, Fred (2003): *Cyber-Risk and Critical Infrastructures. Strategic Security Intelligenece, Cyberterrorism, The National Library of Essays in Terrorism*. London: Ashgate Publishing Limited.
9. COLEMAN, Kevin (2005): *Cyber Terrorism*. Dostopno na http://www.crime-research.org/library/Cyberterrorism.html (1. maj 2006).
10. DENNING, Dorothy E. (2000): *Cyberterrorism. Dostopno na* http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html (20. november 2003).
11. DENNING, Dorothy E. (2001): *Activism, Hacktivism, and Cyberterrorism: The internet as a Tool for Influencing Foreign Policy.* Dostopno na http://www.rand.org/publications/MR/MR1382/MR1382.ch8.pdf (20. november 2003).
12. DELEUZE, Gilles in Felix GUATTARI (2000): *Micelij*. Koper: Hyperion.
13. DOBOVŠEK, Mateja (2002): EU proti terorizmu. *Pravna praksa* 2002(7), 34.
14. DOLINAR, Ksenija (1998): *LEKSIKON Cankarjeve založbe – dopolnjena 5. izdaja,* 1078. Ljubljana: Cankarjeva založba.
15. LIBICKI, Martin (1995): *What is Information Werfare*? Dostopno na http://www.iwar.org.ukIiwar/resources/nduIinfowar/contents (24. marec 2007).
16. LITTLEJOHN SHNIDER, Debra (2002): *Scene of the Cybercrime: Computer forensics Handbook*. Rocklan: Rockland Syngress.

17. FOUCAULT, Michel (2000): *Zgodovina seksualnosti 1 – volja do znanja*. Ljubljana: ŠKUC.
18. GROSEK, Manja (2005): Odškodninska odgovornost za teroristične napade: *Pravna praksa* 2005 (33), 8-26.
19. GUS, Martin (2003): *Understanding Terrorism – Challenges, Perspectives and Issues*. London: Sage Publications.
20. HARAWAY, Donna (1999): *Opice, kiborgi in ženske – reinvencija narave*. Ljubljana: ŠOU, Študentska založba.
21. HOHLER, Beti (2005): Problem definicije terorizma, *Pravna praksa* 33, 6-15.
22. KOROŠEC, BAVCON (2003): *Mednarodno kazensko pravo – Posebni del.* Ljubljana: Pravna fakulteta.
23. KEČANOVIĆ, Bećir (1995): Protiteroristična zakonodaja – nujna tudi v Sloveniji? *Pravna praksa* 1995 (337), 5-21.
24. KEČANOVIĆ, Bečir (1994): Protiterorizem v sistemu nacionalne varnosti Republike Slovenije kot poglavitni dejavnik pri zatiranju kaznivih dejanj zoper temeljne družbene vrednote. *Revija Policija* 5-6 (1994), 34-43.
25. KARMON, Ely (2001): *The Role of Intelligence in the Fight against Terrorism.* Dostopno na http://www.ict.org.il/articles/intelligence_vs_terrorism.htm (12 december 2007).
26. LEBEUF, Marcel-Eugene (2002): On organized Crime and Police Cooperation in the European Union – Lessons learned. An interview with professor Cyrille Fijnaut. *Trends in Organised Crime* 2002 (7/4), 62-85.
27. MARKOVIČ, Dejan (1997): Računalniška kriminaliteta*. Pravna praksa* 1997 (380), 38.
28. MARTONOSI, Pavel (1993): Kriminaliteta v zvezi z računalniki v novi slovenski kazenski zakonodaji. *Podjetje in delo: revija za gospodarsko, delovno in socialno pravo* 1993 (5/6), 489–500.
29. MOŽINA, Damjan (2002): Novi pogledi na pravo informacijske tehnologije. *Pravna praksa* 2002 (26), 34-46.
30. OBERSTAR, Jože (2001): Boj proti mednarodnemu terorizmu. *Pravna praksa* 2001 (20), 17-34.
31. OBERSTAR, Jože (2001): Boj proti nezakoniti trgovini z mamili in terorizmu. *Pravna praksa* 2001 (20), 25-37.
32. O'DAY, Alan (2004): *CYBERTERRORISM. Dyfining terrorism*, *The National Library of Essays in Terrorism*. London: Ashgate Publishing Limited, England.

33. POLLIT, Mark M. (1997): *Cyberterrorism – Fact or Fancy?* Dostopno na http://www.cs.georgetown.edu/~denning/infosec/pollit.html (20. november 2007).
34. POTPARIČ, Damjan (2006): Skupne preiskovalne skupine kot oblika institucionaliziranega policijskega sodelovanja. *Pravna praksa* 2006, (2) 18-29.
35. PREZELJ, Iztok (2006): *Teroristično ogrožanje nacionalne varnosti Republike Slovenije*. Dostopno na http://www.sos112.si/slo/tdocs/ujma/2006/prezelj.pdf (12. december 2007).
36. RUPNIK, Andrej (2002): *Konvencija o kibernetski kriminaliteti.* Dostopno na *https://lms.uni-mb.si/vitel/14delavnica/clanki/andrej_rupnik.pdf*. (12. december 2007).
37. SCHMIT, Alex P. (2001): *Countering Terrorism Through International Cooperation*. Dunaj: Transnational.
38. SEIBER, Urlich (1998): *Legal Aspects of Computer-Related Crime in the Information Society – COMCRIME – Study*. Prepared for the European Commision by University of Wurzburg.
39. SELINŠEK, Liljana (2005): Odzivi slovenskega kazenskega prava na kibernetski kriminal. *Pravna praksa* 2005 (28), 19-27.
40. SVETE, Uroš (2007): *Informacijske razsežnosti sodobnega terorizma – teoretična vprašanja in praktični vidiki*. Dostopno na http://www.sos112.si/slo/tdocs/ujma/2007/124.pdf (6. julij 2008).
41. SVETE, Uroš (2005): *Varnostne implikacije uporabe informacijsko-komunikacijske tehnologije*. Doktorska disertacija. Ljubljana: FDV.
42. ŠELIH, Alenka (2003): Človekove pravice in izziv terorizma. *Pravna praksa* 2003 (1), 3-17.
43. ŠVARC, Dominika (2004): Unija v boju proti terorizmu. *Evro pravna praksa* 2004 (6), 54-67.
44. ŠVARC, Dominika (2006): Teror prava: človekove pravice v globalni vojni proti terorizmu. *Revus – revija za evropsko ustavnost* 2006 (6), 13-27.
45. THOMAS, Douglas, (2003): *Al Qaeda and the Internet: The Danger of »Cyberplanning«*. Dostopno na http://carlistewww.army.mil/usawc/Parameters/03spring/thomas.pdf (1. december 2004).
46. THOMAS, Douglas (2000): New Ways to Break the Law: Cybercrime and the Politics of Hacking. V David Gauntlett (ur.): *Web Studies: Rewiring media studies for the digital age,* 202-211. London: Arnold.

47. THACKRAH, John Richard (2004): *Cyber-terrorism*. Dictionary of Terrorism. London: Routledge.
48. TOPLIŠEK, Janez (1998): *Elektronsko poslovanje*. Ljubljana: Založba Atlantis.
49. TUMAN, S. Joseph (2003): *Communicating*. London: Sage Publications.
50. ULČAR, Matjaž (2001): Mednarodna pristojnost in kiberprostor. *Pravna praksa* 2001 (8), 21-34.
51. VELIKONJA, Urška (2001): Svoboda izražanja in varstvo zasebnosti v kiberprostoru. *Pravna praksa* 2001 (22), 6-18.
52. VODUŠEK, Mojca (1992): Računalniški kriminal. *Varnost – strokovni bilten* 1992 (12), 27-39.
53. WALL, S. David (2001): *Crime and the Internet*. London: Routledge.
54. WHINE, Michael (1999): *Cyberspace, A New Medium for Communication, Command and Control by Extremists*. Dostopno na http://www.ict.org.il/articles/articledet.cfm?articleid=76 (6. julij 2008).
55. WEIMANN, Gabriel (2004): *Cyberterrorism: How Real Is the Threat?* Dostopno na http://www.usip.org/pubs/specialreports/sr119.html (1. maj 2006).
56. WEIMAN, Gabriel (2004b): *How Modern Terrorism Uses the Internet, special report 116.* Dostopno na http://www.usip.org/pubs/specialreports/sr116 (15. marec 2007).
57. ZANINI, Michele in Sean EDWARDS (2001): *The Networking of Terror in the Information Age*. Dostopno na http://www.rand.org/publications/MR/MR1382/MR1392.ch2.pdf (6. julij 2008).
58. ZUPANČIČ, Maja (1997): Kriminaliteta v globalni komunikacijski mreži (internet). *Revija za kriminalistiko in kriminologijo* 48 (2), 23-36.
59. Anti-Defamation League (2007). *Terrorist Activities in the Internet.* Dostopno na http://www.adl.org/terror/focus/16_focus_a.asp (21. marec 2007).
60. *ODS: "Hacker's guide to protect your Internet Network" (Hekerjev vodič za zaščito Interneta).* Dostopen na www.ods.com.ua/win/eng/security/max_security (26. februar 2007).
61. Slovensko izobraževalno omrežje (2007): *Računalniški virusi*. Dostopno na http://ro.zrsss.si/projekti/comp/racopismen/anti-virus/Anti%20virus.html (13. junij 2007).
62. GREEN, Joshua (2002): *The Myth of Cyberterrorism*. Dostopno na www.washingtonmonthly.com/features/2001/0211.green.html (13. junij 2007).
63. DAKIČ, Lana (2008): *Tudi talibani brskajo po internetu*. Dostopno na http://www.finance.si/208119 (14. maj 2008).

Pravni viri in dokumenti:

1) *Kazenski zakonik Slovenije*. Ur. list RS, 63/94, 70/94, 23/99, 40/2004, 55/2008.
2) *Zakon o kazenskem postopku.* Ur. list RS 63/94, 70/94, 72/98, 55/2003.
3) *Mednarodna konvencija za preprečevanje financiranja terorizma*. Ur. list RS 21/2004.
4) Oddelek za protiteroristično dejavnost in ekstremno nasilje GPU UKP (2005). *Organiziranost in dejavnost Oddelka za terorizem in ekstremno nasilje*. Arhiv GPU UKP.
5) Ustava Slovenije, *Ur. list RS*, št. 33/91-I; 42/1997, 66/2000;
6) Zakon o policiji, *Ur. list RS*, 210/94, 43/2004, 2303/2004 in 54/2004.

Ustni viri:

1) Gelbart, Ivan, EUROPOL, intervju z avtorjem. Haag, 16. november 2007.
2) Blažina, Bruno, intervju z avtorjem. Ljubljana 12. december 2007.
3) Černigoj, Albert, intervju z avtorjem. Ljubljana 13. december 2007.