UNIVERZA V LJUBLJANI
FAKULTETA ZA DRUŽBENE VEDE

Danica Dovč

UPORABA OBLIK INFORMACIJSKEGA BOJEVANJA V SODOBNEM TERORIZMU: PRIMER TERORISTIČNE ORGANIZACIJE PKK

diplomsko delo

Ljubljana, 2005

UNIVERZA V LJUBLJANI
FAKULTETA ZA DRUŽBENE VEDE

Danica Dovč

Mentor: izred. prof. doc. dr. Marjan Malešič

Somentor: asist. dr. Uroš Svete

UPORABA OBLIK INFORMACIJSKEGA BOJEVANJA V SODOBNEM TERORIZMU: PRIMER TERORISTIČNE ORGANIZACIJE PKK

diplomsko delo

Ljubljana, 2005

IZJAVA O AVTORSTVU DIPLOMSKEGA DELA

Spodaj podpisana DANICA DOVČ, z vpisno številko 21017024, rojena 6. 8. 1981 v Novem mestu, sem avtorica diplomskega dela z naslovom:

UPORABA OBLIK INFORMACIJSKEGA BOJEVANJA V SODOBNEM TERORIZMU: PRIMER TERORISTIČNE ORGANIZACIJE PKK

S svojim podpisom zagotavljam, da:

• je predloženo diplomsko delo izključno rezultat mojega lastnega raziskovalnega dela;

• sem poskrbela, da so dela in mnenja drugih avtorjev oz. avtoric, ki jih uporabljam v predloženem delu, navedena oz. citirana v skladu s fakultetnimi navodili;

• sem poskrbela, da so vsa dela in mnenja drugih avtorjev oz. avtoric navedena v seznamu virov, ki je sestavni element predloženega dela in je zapisan v skladu s fakultetnimi navodili;

• sem pridobila vsa dovoljenja za uporabo avtorskih del, ki so v celoti prenesena v predloženo delo in sem to tudi jasno zapisala v predloženem delu;

• se zavedam, da je plagiatorstvo – predstavljanje tujih del, bodisi v obliki citata bodisi v obliki skoraj dobesednega parafraziranja bodisi v grafični obliki, s katerim so tuje misli oz. ideje predstavljene kot moje lastne – kaznivo po zakonu (Zakon o avtorski in sorodnih pravicah, Uradni list RS št. 21/95), prekršek pa podleže tudi ukrepom Fakultete za družbene vede v skladu z njenimi pravili;

• se zavedam posledic, ki jih dokazano plagiatorstvo lahko predstavlja za predloženo delo in za moj status na Fakulteti za družbene vede;

• je elektronska oblika identična s tiskano obliko diplomskega dela ter soglašam z objavo diplomskega dela v zbirki "Dela FDV".

V Ljubljani, dne _____ Podpis avtorja:

_____

KAZALO

KAZALO SLIK

KAZALO TABEL

KAZALO SHEM

KAZALO GRAFOV

SEZNAM POGOSTEJE UPORABLJENIH KRATIC IN OKRAJŠAV

ADL – Anti-Defamation League

ang. – angleško

ATAA – Assembly of Turkish American Association (Združenje turško ameriškega povezovanja)

DoS – denial of service (napadi za zavrnitev storitve)

FBI – Federal Bureau of Investigation (Zvezni preiskovalni urad)

HPG – Hêzên Parastina Gel (Ljudske obrambne sile)

IASIW – Institute for Advanced Study of Information Technology (Inštitut za napredne študije informacijskega bojevanja)

idr. – in drugo

IKT – informacijsko-komunikacijska tehnologija

ipd. – in podobno

itd. – in tako dlje

KADEK – Kongreya Azadi u Demokrasiya Kurdistane (Kurdski svobodni in demokratični kongres)

KGK – Kongra Gelê Kurdistan (Kongra-Gel, Ljudski kongres Kurdistana)

kur. – kurdsko

MIPT – National Memorial Institute for Prevention of Terrorism (Nacionalni spominski inštitut za preprečevanje terorizma)

nem. – nemško

npr. – na primer

orig. – originalno

oz. – oziroma

PKK – Partiya Karkerên Kurdistan (Kurdska delavska stranka)

slo. – slovensko

TAK – Teyrbazen Azadya Kurdistan (Svobodni sokoli Kurdistana)

t. i. – tako imenovani

tj. – to je

ZDA – Združene države Amerike

1 UVOD

Uporaba informacijskega bojevanja oz. uporaba informacij[1] (podatkov) za doseganje ciljev ni nov pojav. Znano je, da so vojske že od nekdaj zbirale podatke o nasprotnikovih silah in jih uporabljale proti njim ter v ta namen uporabljale različne informacijske tehnologije, kot so dimni signali, telegraf in podobno, vendar pa vse do danes te tehnologije niso imele bistvenega pomena. Vse do prve svetovne vojne je bil oboroženi boj ključna dejavnost vojn, neoborožene oblike bojevanja (politično, ekonomsko, psihološko idr. bojevanje) pa so imele manjšo vlogo. Konkretni uspehi teh neoboroženih oblik bojevanja so prvič vidni v drugi svetovni vojni. Informacijska doba in globalizacija sta tovrstnim oblikam bojevanja odprli nove možnosti. Stare oblike neoboroženega boja so bile predstavljene z novimi (informacijskimi) tehnologijami, pojavijo pa se tudi nekatere nove oblike (npr. hekersko bojevanje). Tisto, kar je danes novega, je predvsem spremenjen način zbiranja, obdelave in posredovanja podatkov, ob uporabi novih informacijskih tehnologij za doseganje želenih učinkov.

Uporaba informacijsko-komunikacijske tehnologije (IKT) je že zdavnaj presegla raziskovalne in vojaško-obrambne okvire, postala je temelj delovanja vseh pomembnejših družbenih podsistemov (Levin, 1996 v Svete, 1999: 1; Svete, 2005: 5). Danes živimo v informacijski družbi, v kateri sta tako vojaško kot civilno področje vse bolj odvisna od IKT in procesov povezanih z njo, saj so skoraj vsi komunikacijski sistemi računalniško nadzorovani. Za primer naj navedem, da imajo zračna in kopenska prevozna sredstva večinoma digitalne računalniške komponente, večina transportnih sistemov (npr. letala, železnice ...) se usmerja s pomočjo komunikacijskih sredstev in računalnikov, zdravstvena in farmacevtska industrija sta vse bolj odvisni od računalniških sistemov, oskrba z električno energijo in pitno vodo postaja vse bolj odvisna od digitalnih komponent in še bi lahko naštevali.

Potrebno je poudariti, da so se hkrati z novimi informacijsko-komunikacijskimi tehnologijam pojavile tudi nove oblike in načini doseganja ciljev države, različnih nedržavnih organizacij (zasebnih organizacij, gospodarskih družb, političnih skupin in strank) ter tudi individualnih partikularnih interesov posameznika. Informacijske tehnologije omogočajo nasprotniku, ki lahko predstavlja državo, teroristično skupino, posameznika ipd., strateško ogrožanje držav, še posebej na tistih področjih, ki temeljijo na uporabi informacijsko-komunikacijskih

[1] Informacija je podatek, pridobljen iz okolja in predelan v uporabno obliko (FM 100-6, v Svete, 1999: 5).

tehnologij. Zaradi tega informacijsko bojevanje danes predstavlja enega aktualnejših varnostnih izzivov na državni, poddržavni in naddržavni ravni.

Informacijsko bojevanje je v sodobnih družbah postalo nevaren rezultat tehnologije v rokah kogarkoli, ki želi oslabiti nekoga drugega. Saj je IKT danes sorazmerno poceni in lahko dostopna. Hkrati IKT akterjem omogoča anonimnost in geografsko-prostorsko neomejenost. Zaradi tega informacijsko bojevanje lahko predstavlja tudi nevarno obliko terorizma. Tako kot so številne privatne korporacije privzele IKT, ker jim omogoča učinkovitejše in bolj fleksibilno delovanje, tako tudi številne teroristične organizacije uporabljajo IKT – kot so računalniki, programska oprema, telekomunikacijska sredstva in internet – za boljšo organizacijo in uskladitev aktivnosti. Z vstopom v informacijsko dobo se je tako spremenil tudi terorizem. Informacijska doba ter uporaba IKT, po mnenju strokovnjakov korporacije RAND, ne vpliva samo na vrsto tarč in orožja, ki ga izbirajo teroristi, ampak tudi na način, na katerega delujejo teroristične organizacije ter na njihovo strukturo. Ta »novi« oz. sodobni terorizem ima drugačne motive, drugačne akterje, drugačne sponzorje in posledično tudi, kot trdi Bruce Hoffman, večjo ubojnost (Hoffman, 1999).

V tej diplomski nalogi se bom ukvarjala z uporabo oblik informacijskega bojevanja v sodobnem terorizmu. Uporabila bom razdelitev, ki jo je predstavil Martin Libicki leta 1995, v delu What is Information warfare?. Če povem natančneje, glede na oblike po Libickem, se bom ukvarjala predvsem z uporabo psihološkega, kibernetskega in hekerskega bojevanja v sodobnem terorizmu ter na študiji primera delovanja PKK. Vendar se ne bom nanašala le na Libickega, njegova dognanja bom skušala dopolniti tudi s pogledi drugih avtorjev.

2 TEORETSKO METODOLOŠKI OKVIR

2.1 Predmet in cilji preučevanja

Predmet preučevanja je uporaba IKT v sodobnem terorizmu ter v povezavi z njo uporaba nekaterih oblik informacijskega bojevanja (psihološkega, hekerskega in kibernetskega) v terorizmu.

Cilj moje diplomske naloge je ugotoviti, katere oblike informacijskega bojevanja oz. delovanja uporabljajo teroristične organizacije. Natančneje povedano želim ugotoviti, kakšna je dejanska vloga in pomen uporabe sodobne informacijsko-komunikacijske tehnologije pri doseganju ciljev terorističnih organizacij ter za vpliv na nasprotnika, lastno (domačo) in nevtralno javnost. Poskušala bom ugotoviti, kako veliko grožnjo terorizem predstavlja mednarodni skupnosti. Preučevala bom predvsem psihološko, kibernetsko in hekersko bojevanje, ki ga izvaja teroristična organizacija PKK – Kurdska delavska stranka (kur. Partya Karkerên Kurdistan, ang. Kurdistan Workers Party, nem. Arbeiterpartei Kurdistan).

2.2 Hipoteze

Glavna hipoteza diplomske naloge je, da *imajo teroristična dejanja z uporabo sodobne informacijsko-komunikacijske tehnologije vse večji učinek, tako v smislu doseganja ciljev, kot tudi vpliva na javno mnenje*.

Druga hipoteza pa je, da *teroristična organizacija PKK med oblikami informacijskega bojevanja daje največji poudarek psihološkemu bojevanju, še posebej propagandi*.

2.3 Metode preučevanja

Pri izdelavi diplomske naloge bom v prvi fazi uprabila metodo zbiranja različnih virov in literature. Pri pisanju uvoda ter opredeljevanju ključnih pojmov in konceptov bom uporabila predvsem analizo vsebine, tako primarnih kot tudi sekundarnih virov in literature. To metodo bom uporabljala tudi v nadaljevanju diplomskega dela, pri opredeljevanju informacijskega bojevanja (definicije, razvoj koncepta, oblike, glavne značilnosti ...), terorizma, informacijskega oz. kibernetskega terorizma in zgodovine interneta. Nato bom uporabila študijo primera teroristične organizacije PKK, v okviru te študije bom poskušala ugotoviti, kako PKK (če sploh) uporablja kibernetsko, hekersko in psihološko bojevanje. Za študijo tega

primera bom uporabila analizo spletnih strani, forumov in klepetalnic, ki so izredno pomembne zlasti pri propagandni dejavnosti terorističnih organizacij, poleg tega bom uporabila metodo pogostosti pojavljanja PKK na svetovnem spletu (gledala bom število zadetkov v posameznem izbranem iskalniku ob različnih iskalnih kriterijih oz. ključnih besedah). Pri ugotavljanju psihološkega bojevanja, predvsem pa propagandne dejavnosti preučevane teroristične organizacije, bom uporabila analizo tiskanih medijev. V okviru te metode bom analizirala turške, nemške in slovenske tiskane medije. Prve dvoje zaradi aktivnega delovanja PKK v teh dveh državah, slovenske pa kot primer države, v kateri PKK ne deluje. Pri samem pisanju naloge pa bom uporabljala opisno (deskriptivno) metodo.

2.4 Struktura analize

Prvo poglavje diplomskega dela predstavlja uvod, v katerem bom podala nekaj splošnih ugotovitev o informacijskem bojevanju in njegovi uporabi v sodobnem terorizmu.

Nato bom podala metodološko-hipotetični okvir, v katerem bom opredelila predmet in cilje preučevanja, zastavila hipoteze, predstavila uporabljene metode preučevanja ter strukturo naloge.

V tretjem poglavju bom definirala in opredelila ključne pojme in koncepte, na katerih bo temeljila analiza. To so informacijsko-komunikacijska tehnologija (IKT), terorizem, teroristična organizacija in javno mnenje.

Četrto poglavje bom posvetila natančnejši opredelitvi koncepta informacijskega bojevanja. V sklopu tega poglavja bom najprej predstavila nekaj različnih definicij in opredelitev informacijskega bojevanja. Nato bom predstavila kratko zgodovino, značilnosti in oblike (po Libickem) informacijskaga bojevanja. Med oblikami bom pozornost namenila predvsem kibernetskem, hekerskem in psihološkem bojevanju, ki bodo predmet moje analize.

V petem poglavju se bom ukvarjala z uporabo oblik informacijskega bojevanja v terorizmu. Najprej bom predstavila nekatere trende v terorizmu. Nato bom predstavila preučevano teroristično organizacijo – PKK. Zatem se bom ukvarjala z uporabo že omenjenih oblik informacijskega bojevanja (kibernetskim, hekerskim in psihološkim) v terorizmu. Eno podpoglavje pa bom namenila informacijskemu oz. kibernetskemu teorizmu. V okviru tega poglavja bom predstavila tudi kratko zgodovino interneta in njegovo uporabo v terorizmu.

Na koncu (v šestem poglavju) pa bom potrdila ali zavrgla na začetku postavljeni hipotezi ter podala sklep.

3 TEMELJNJI POJMI IN KONCEPTI

Informacijsko-komunikacijska tehnologija (IKT)

IKT obsega »zbiranje, obdelavo in prikaz podatkov, vključuje pa tudi komunikacijski element, ki omogoča prenos podatkov« (Alberts, 1996 in Wilson 1998 v Svete, 2005: 14).

IKT vključuje vsa komunikacijka sredstva, kot so: radio, televizija, telefoni, računalniki in računalniška strojna (ang. hardware) in programska (ang. software) oprema, satelitske sisteme ipd., IKT vsebuje tudi različne podporne sisteme in sredstva povezana s komunikacijskimi sistemi (npr. videokonference) (whatis.com definitions, 2004).

Terorizem

Sama beseda **terorizem** izhaja iz francoščine (terreur), kjer je označevala metodo ene izmed faz revolucije v času jakobinske diktature (od leta 1794 do 1796). Koren besede izhaja iz latinščine (terror, terroris – močan strah) iz katerega izhaja beseda **terrere**, ki pomeni prestrašiti (Krunić, 1997: 153; Slovar slovenskega knjižnega jezika, 1991: 71).

Terorizem je »politično motivirana uporaba sile proti posameznikom, skupinam oseb ali predmetom, namen pa je vnesti hudo negotovost med prebivalstvom, s tem vznemiriti državni in družbeni sistem ter zrušiti državno in družbeno ureditev« (Veliki splošni leksikon, 1998: 4360).

FBI (Federal Bureau of Investigation) terorizem opredeljuje kot »nezakonito uporabo sile ali nasilja zoper osebe ali lastnino, z namenom prestrašiti ali priganjati (siliti) vlado, civilno prebivalstvo ali katerikoli segment vlade ali civilnega prebivalstva ter s tem doseči svoje politične ali socialne cilje« (FBI v Thomas, 2002).

Krunić v delu Strategiji posrednega nastopanja ugotavlja, da terorizem in teroristično organizacijo opredeljujo naslednje značilnosti: politični cilj, nasilno dejanje, nelegitimno nasilje, ponavljajoče dejanje, zavestno dejanje, sekundarni učinek, izzivanje strahu in drugih psihičnih reakcij, komunikativnost terorističnega dejanja, brezobzirnost, organiziranost, opremljenost, izurjenost ter konspirativnost (Krunić, 1997:154-158).

Natančneje lahko terorizem opredelimo s pomočjo sinteze definicij, ki jo je v magistrskem delu podal Uroš Svete. Glede na njegovo sintezo je terorizem »naklepno, organizirano in usmerjeno delovanje tako nedržavnih kot od države podprtih akterjev (od terorističnih mrež in organizacij do posameznikov), katerih glavni namen je z nasilnimi sredstvi, usmerjenimi predvsem proti civilnim kot tudi vojaškim ciljem, v času formalnega miru vplivati na domačo,

določeno tujo ali mednarodno javnost ter tako doseči svoje politične, ideološke, religiozne, ekonomske ali kake druge partikularne cilje« (Svete, 2002:99).

Teroristična organizacija

V publikaciji Country Reports on Terrorism **teroristično organizacijo** opredeljujejo kot katerokoli skupino, ki izvršuje mednarodni terorizem ali katera ima značilne podskupine, ki izvršujejo mednarodni terorizem (Country Reports on Terrorism 2004, 2005).

Teroristična organizacija je »združenje posameznikov, ki pripadajo neodvisnemu nedržavnemu, podnacionalnemu revolucionarnemu ali protivladnemu gibanju ter se poslužujejo nasilja za doseganje ciljev. Takšno združenje ima vsaj strukturalni, vodstveni in nadzorni aparat, ki zagotavlja organizacijski okvir in splošne strateške smeri« (MIPT[2], 2005).

Javno mnenje

Univerzalno veljavne definicije javnega mnenja ni mogoče najti. Slavko Splichal ga definira kot »komunikacijski proces, v katerem si posamezniki in skupine prizadevajo doseči konsenz o spornih javnih zadevah z namenom, da bi vplivali na delovanje institucij oblasti« (Splichal, 1997: 4). Javno mnenje je oblika družbene volje, ki se institucionalizira skozi parlament, množične medije in javnomnenjske raziskave (Obča komunikologija II, http://www.fdvinfo.net/uploadi/ editor/vpr_odgovori-komII.doc). Sopomenke javnemu mnenju (ang. public opinion) so: splošno mnenje (ang. popular opinion), mnenje (ang. opinion) in glas ljudstva (ang. vox populi) (WordNet, 2001).

Poznamo štiri skupine definicij javnega mnenja: **Agregatne definicije** javno mnenje obravnavajo kot seštevek individualnih mnenj. Možno jih je seštevati in meriti na osnovi javnomnenjskih raziskav. **Večinske definicije** javno mnenje obravnavajo kot mnenje večine. **Diskurzivno-konsenzualne** definicije, po katerih se javno mnenje oblikuje v javni razpravi; ob soočenju različnih mnenj se sprejme konsenz, ki pomeni javno mnenje. **Definicije, ki trdijo, da javno mnenje ne obstaja,** ker javnomnenjske raziskave izhajajo iz predpostavke, da imajo vsi že izoblikovana mnenja, kar pa ne drži. Vsa mnenja nimajo enake teže, ker imamo ljudje različne možnosti predstavitve mnenj. V družbi ne obstaja konsenz o tem, katera vprašanja so pomembna, temveč jih definirajo mediji. Avtorji, ki zagovarjajo te definicije, na osnovi teh trditev pravijo, da javno mnenje ne obstaja, ampak je le konstrukt, ki se uporablja v politične namene (Obča komunikologija II, http://www.fdvinfo.net/uploadi/editor/ vpr_odgovori- komII.doc).

[2]MIPT - National Memorial Institute for Prevention of Terrorism.

4 INFORMACIJSKO BOJEVANJE

4.1 Opredelitev koncepta

Pri opredeljevanju informacijskega bojevanja[3] naletimo na problem, kajti nekega splošno sprejetega in uveljavljenega pristopa, ki bi opredeljeval informacijsko bojevanje ni. Večina avtorjev, ki se ukvarja s tem področjem, se razhaja v definicijah in opredelitvah, vendar imajo te opredelitve tudi neke skupne točke. Ene definicije in opredelitve bolj poudarjajo sredstva, druge pa cilje delovanja. Nekateri avtorji (npr. Martin Libicki) pa raje kot definicije navajajo oblike informacijskega bojevanja (Svete 1999 in 2002).

Winn Schwartau podaja naslednjo definicijo: »Pravo informacijsko bojevanje je uporaba informacij in informacijskih sistemov kot orožij v boju proti informacijam in informacijskim sistemom« (Schwartau, v Svete 2002: 76). Informacijsko bojevanje Schwartau predstavlja le (digitalne) napade na računalniške sisteme in omrežja. Definicija zanj ne predstavlja univerzalne opredelitve, ampak govori o informacijskem bojevanju na treh nivojih:

- napadi prvega razreda (osebno – napadi na elektronsko zasebnost posameznika),
- napadi drugega razreda (korporacijsko – informacijske vojne med korporacijami po svetu, ki potekajo predvsem na ravni pridobivanja in posredovanja dejanskih ali lažnih informacij) in
- napadi tretjega razreda (globalno – napadi na industrije, globalne ekonomske sile in posamezne države) (Svete, 1999; Arsić, 2004).

Dr. Ivan Goldberg na spletni strani Inštituta za napredne študije informacijskega bojevanja (IASIW[4]) podaja naslednjo definicijo: »Informacijsko bojevanje je ofenzivna in defenzivna uporaba informacij in informacijskih sistemov z namenom izkoristiti, onesposobiti ali uničiti nasprotnikove informacije in informacijske sisteme sisteme, medtem ko želimo obvarovati lastne informacije in informacijske sisteme« (Goldberg, 2004).

Dorothy E. Denning razume koncept informacijskega bojevanja zelo široko. »Obsega informacijo v vseh oblikah, ki se prenaša po zelo različnih medijih. Prenos poteka med ljudmi in njihovim fizičnim okoljem pa do različnih komunikacijskih storitev, televizije, računalnikov in računalniških mrež. Obsega operacije proti vsebini informacij in operacije

[3] Poleg pojma informacijsko bojevanje se uporabljajo še pojmi: digitalno bojevanje (ang. digital warfare), kibernetsko bojevanje (ang. cyber warfare) in neubojno bojevanje (ang. soft warfare) (Arsić, 2004).
[4] Institute for Advanced Study of Information Warfare (Inštitut za napredne študije informacijskega vojskovanja) ima svojo spletno stran na naslovu http://www.psycom.net/.

proti podpornim sistemom, pri čemer je vključena tako strojna kot programska oprema ter človekova dejavnost« (Denning, v Svete, 2002: 76).

Martin Libicki, eden prvih avtorjev, ki se je ukvarjal s področjem informacijskega bojevanja, meni, da informacijsko bojevanje, kot posebna oblika vodenja vojne, ne obstaja. Obstaja pa sedem oblik informacijskega bojevanja, ki imajo informacijo kot sredstvo, cilj in orožje:

- bojevanje na poveljniško-nadzornem področju (ang. command-and-control warfare (C2W)),
- bojevanje, ki temelji na obveščevalni dejavnosti (ang. intelligence-based warfare),
- elektronsko bojevanje (ang. electronic warfare),
- psihološko bojevanje (ang. psyhological warfare),
- hekersko bojevanje (ang. »hacker« warfare),
- ekonomsko informacijsko bojevanje (ang. economic information warfare) in
- kibernetsko bojevanje (ang. cyberwarfare) (Libicki, 1995).

Arquilla in Ronfeldt raje kot o informacijskem bojevanju govorita o kibernetskem – »Cyberwar« in omrežnem bojevanju – »Netwar«. Kibernetsko bojevanje se nanaša na vojaško sfero, kjer je govora predvsem o konfliktih visoke intenzivnosti (HIC – high-intensity conflict) in konfliktih srednje intenzivnosti (MRC – middle-range conflict). Omrežno bojevanje pa obsega socialno, politično, vojaško in ekonomsko obliko konflikta, kjer govorimo predvsem o konfliktih nizke intenzivnosti (LIC – low-intensity conflict), operacijah drugačnih od vojne[5] (OOTW – operations other than war) in drugih, predvsem nevojaških, oblikah konflikta in kriminala (Arquilla in Ronfeldt, 1996: 3).

Za mojo analizo je, od zgoraj naštetega, pomemben predvsem koncept omrežne vojne t. i. netwar. Netwar označuje pojavljajočo obliko konflikta (in kriminala) na družbeni ravni, obsega merila krajše vojne, v kateri protagonisti uporabljajo in so odvisni od mrežne oblike organizacije, doktrine, strategije in komunikacije (Arquilla in Ronfeldt, 1996:5). Omrežno bojevanje izvajajo različne nedržavne, paravojaške in iregularne sile (Whine, 1999).

Strpić ugotavlja, da se Arquilla in Ronfeldt v svojih delih (v letih med 1991 do1994), ukvarjata nekako s tremi definicijami omrežnega bojevanja. Prva definicija je fizična, ki predpostavlja nujnost fizične infrastrukture, kot je na primer električno omrežje. Druga definicija je sintaktična, nanaša se na spreminjanje logike računalniškim sistemom s pomočjo kod, da delajo tisto za kar niso narejeni (takšni so napadi z virusi, trojanskimi konji ipd). To je prava hekerska usmeritev, kjer se s kodo premaga drugo kodo. Tretja definicija pa je

[5] OOTW vključuje mirovne in humanitarne operacije (Arquilla in Ronfeldt, 1996).

semantična. Semantika se nanaša na spreminjanje informacij, ki vstopajo in izstopajo iz nekega sistema, torej na tisto, kar danes razumemo pod pojmoma informacijsko in protiinformacijsko bojevanje (Galley, 1996; Strpić, 2002).

Lahko rečemo, da je zgoraj predstavljen ameriški koncept pojmovanja informacijskega bojevanja, ki sicer ni edini, je pa eden največkrat uporabljenih. Vidimo, da univerzalne opredelitve informacijskega bojevanja ni. Iz teh opredelitev se da določiti nekatere glavne lastnosti informacijskega bojevanja. Vedno zajema uporabo informacijskih tehnologij, vključuje napade na informacije, informacijske procese in informacijsko infrastrukturo nasprotnika ter zavarovanje lastnih informacij, informacijskih procesov in informacijske infrastrukture. Izvaja ga neka organizirana skupina (izjemoma posameznik) za dosego svojih ciljev, ki so lahko vojaški, ekonomski, socialni, politični, ideološki ipd. Nasprotnik v informacijskem spopadu je navadno odvisen od informacijskih sistemov (Mišmaš, 1999; Arsić, 2004).

4.2 Razvoj koncepta

Informacijsko bojevanje je v najširšem smislu boj, ki vključuje informacijsko-komunikacijski proces, boj, ki se je začel s prihodom človeške komunikacije in konflikta (Lewis, http://www.fas.org/irp/eprint/snyder/infowarfare.htm). Informacija je že od nekdaj igrala pomembno vlogo v oboroženih spopadih in v ta namen so vojske uporabljale (takrat razpoložljive) informacijske tehnologije, kot so dimni signali v starodavnih časih, telegraf na prelomu prejšnjega stoletja ipd (Berkowitz, 1997). Že Sun Tzu je predlagal ustvarjalno uporabo informacij za dosego strateških ciljev brez uporabe oborožene sile (Mišmaš, 1999).

Informacijsko bojevanje je največji preobrat doživelo s tretjo industrijsko revolucijo, t. i. informacijsko revolucijo, ki se je začela v 70. letih, ko so se pojavile informacijske družbe oz. družbe tretjega vala, kot jih imenujeta Heidi in Alvin Toffler. Omenjena avtorja v njuni knjigi War and Antiwar človeško zgodovino razdelita v tri različna obdobja (t. i. valove). Prvo fazo, to je poljedelsko obdobje, imenujeta Prvi val (ang. First Wave); Drugi val (ang. Second Wave) sovpada z industrijsko revolucijo; današnje obdobje, za katerega je značilna digitalizacija družbe, pa označujeta kot Tretji val (ang. Thirt Wave) (Toffler v Shahar, 1997).

Vsakemu od teh obdobij Tofflerjeva pripisujeta edinstven način bojevanja, saj se vsaka družba prilagaja razpoložljivi tehnologiji. V poljedelski dobi so se vojne odvijale za nadzor nad lokalnimi viri, vojaki so bili člani določenih plemen, ki so neposredno nadzorovali sporna

ozemlja ali vire. Velike vojske, z redkimi izjemami kot je na primer bila rimska legija, v tem obdobju, zaradi pomanjkanja virov, niso bile možne. Industrijska revolucija je prinesla masovno proizvodnjo, zato se začnejo, v času industrijskih družb (družb drugega vala), odvijati vojne med civilizacijami, ki vključujejo milijone ljudi, vključno s civilnim prebivalstvom (npr. prva svetovna vojna) (Toffler v Shahar, 1997). Mehanizacija in industrializacija sta privedli do prevlade tankov na bojiščih druge svetovne vojne. S prihodom mehaniziranega bojevanja[6], pa je narasel tudi pomen bojevanja proti nasprotnikovim informacijskim in komunikacijskim sistemom. Informacijska revolucija je povzročila porast načina bojevanja, v katerem o izidu ne odločata niti množičnost niti mobilnost; namesto tega bo stran, ki ve več, uživala odločilne koristi (Arquilla in Ronfeldt, 1995).

Povečan pretok informacij, razvoj globalnih ekonomij in izum interneta so dejavniki, ki so v tretjem valu zgodovinskega razvoja svet spremenili v svetovno vas. Moderni koncept informacijskega bojevanja je za nekatere teoretike (npr. Cramerja) posledica razvoja novih tehnologij (Glej prilogo A, ki prikazuje nove informacijske tehnologije, kot jih je opredelil Myron L. Cramer) (Cramer, 1996). Arquilla in Ronfeldt pa trdita, da spremenjen način bojevajna v informacijski dobi ni le posledica razvoja tehnologije, pač pa tudi posledica sprememb v organizaciji, doktrini in strategiji (Aguilla in Ronfeldt, 1997b). V skladu s temi družbenimi spremembami se je spremenil tudi način vodenja vojn. Konflikti so vse manj vojaški, informacijsko bojevanje pa pridobiva vse bolj pomembno vlogo (Shahar, 1997).

Prostor, v konceptu nacionalne varnosti, je informacijsko bojevanje dobilo v obdobju po hladni vojni. Koncept informacijskega bojevanja so začeli razvijati v ZDA, ker so hoteli ohraniti prevlado tudi v spremenjenem varnostno-političnem okolju po hladni vojni. V okviru tega koncepta so poleg tradicionalne vojaške, gospodarske in politične moči, začeli izpostavljati uporabo IKT (Svete, 2005).

Glavni prelomni točki, v zgodovini informacijskega bojevanja, predstavlja Vietnamska in Zalivska vojna (leta 1991). V Zalivski vojni so si ZDA in njihovi zavezniki z uporabo satelitske komunikacije, navigacije, nadzorstva in obveščevalne dejavnosti na vojaškem in civilnem področju, pridobili prednost pred nasprotnikom, ki je bila ključ za zmago (Arquilla in Ronfeldt, 1997b).

[6] Na primer: Nemci so med drugo svetovno vojno predvideli radijske postaje v vseh tankih, kar jim je prineslo veliko prednost pred Rusi, ki so imeli večje število, boljše zgrajenih tankov, vendar so predvideli radijske postaje le za poveljnike (Arquila in Ronfeldt, 1995).

Iz vsega zgoraj povedanega, lahko zaključim, da uporaba IKT v vojne namene ni nov fenomen, spremenil se je le njegov pomen. Sam koncept informacijskega bojevanja pa je relativno nov. Čeprav se je informacijsko bojevanje uporabljalo skozi vso zgodovino, je imelo le sekundarni pomen, glavno vlogo v bojevanju pa je imel oboroženi boj. Danes ima informacija večjo strateško vrednost kot jo je imela kadarkoli v zgodovini. Danes so informacijsko-komunikacijski sistemi tako pomembni za vojaške in tudi nevojaške operacije, da se velikokrat bolj splača onesposobiti ali uničiti nasprotnikov informacijsko-komunikacijski sistem kot fizično uničiti nasprotnika (Devost, 1995).

4.3 Značilnosti informacijskega bojevanja

Informacijsko bojevanje se v veliko pogledih razlikuje od klasičnega načina bojevanja. Zato bom v nadaljevanju predstavila nekaj ključnih točk, v katerih se informacijsko bojevanje razlikuje od klasičnega.

- Informacijsko bojevanje lahko zajame **veliko tarč,** ki so lahko zelo različne in vključujejo informacije, računalnike, sisteme, omrežja, pripomočke in navsezadnje tudi ljudi.
- Napadalec oz. nasprotnik v informacijskem napadu je neznan, **anonimen.**
- Informacijsko bojevanje ima velik **psihološki vpliv,** saj lahko z različnimi psihološkimi sredstvi zavede nasprotnika ali doseže lojalnost.
- V informacijskem bojevanju se praviloma uporablja zelo **preprosta** in lahko dostopna **tehnologija** (računalniki, mobilni telefoni ...), ki je relativno poceni in zahteva le strokovno znanje.
- **Odgovornost** za informacijski napad je **nejasna,** ker ni pravih sredstev za odkrivanja storilca.
- Informacijsko bojevanje **ne pozna omejitev**, saj lahko preseže politične, časovne, geografske in celo vesoljske meje.
- Napadeni nimajo časa, da bi hitro ukrepali, saj ko se napad enkrat izvede, vse poteka zelo hitro.
- Zakonodaja, predvsem mednarodna, še nima povsem jasno določenih zakonov, ki bi opredeljevali to obliko bojevanja.

Poleg zgoraj naštetih značilnosti informacijskega bojevanja se v zvezi z njim postavljata še dve vprašanji. Prvo je: **Ali je to vojna?** Ali lahko informacijsko bojevanje imenujemo vojna,

saj je težko verjetno, da bi lahko nadomestilo klasično obliko vodenja vojne. Poleg tega pa moramo upoštevati, da so za vojno potrebne oborožene sile, ki pa tu niso nujno potrebne.
Drugo vprašanje je: **Ali je to kriminalno dejanje?** Pri tem moramo upoštevati namen bojevanja oz. vojskovanja in ugotoviti kakšne cilje je imel napadalec (Mišmaš, 1999; Svete 2002).

4.4 Oblike informacijskega bojevanja

Libicki, kot sem že omenila, loči sedem oblik informacijskega bojevanja. Pri oblikah informacijskega bojevanja je potrebno poudariti, da so usmerjene tako v delovanje proti vojaški kot proti civilni sferi. Od naštetih oblik so tri, to so bojevanje na poveljniško-nadzornem področju, bojevanje, ki temelji na obveščevalni dejavnosti in elektronsko bojevanje, usmerjene samo v vojaške cilje, tri oblike (psihološko, kibernetsko in hekersko bojevanje) imajo lahko tako vojaške kot tudi civilne cilje, medtem ko je ekonomsko informacijsko bojevanje usmerjeno zgolj na civilne cilje. V tem diplomskem delu se bom ukvarjala predvsem z oblikami informacijkega bojevanja, ki so usmerjene v civilno sfero, in sicer s psihološkim, kibernetskim in hekerskim bojevanjem v sodobnem terorizmu. Te oblike sem izbrala zato, ker je tudi terorizem usmerjen predvsem proti civilnim ciljem. Izbrane tri oblike informacijskega bojevanja bom na tem mestu bolj podrobno opredelila.

4.4.1 Psihološko bojevanje

Psihološko bojevanje zajema uporabo informacije proti človeškemu razumu in vrednotam. Izraz psihološko vojskovanje je prvi uporabil Britanec J. F. C. Fuller (leta 1920 v svoji analizi o tankih), ki je menil, da bi v prihodnosti psihološko bojevanje lahko celo zamenjalo klasična (konvencionalna) sredstva za vodenje vojn (Krunić, 1997).

Daughtery in Janowitz psihološko bojevanje opredeljujeta kot *»načrtno uporabo propagande in drugih akcij za vplivanje na mnenja, čustva in vedenje sovražnih, nevtralnih ali prijateljskih tujih skupin na način, ki podpira uresničevanje nacionalnih namer in ciljev«* (Daugherty in Janowitz v Malešič, 1997:32).

Poznamo negativni in pozitivni način izvajanja psihološkega bojevanja. Pri negativnem načinu poskušamo pri nasprotniku povzročiti negativno mnenje o njihovi državi, vladi, družbi, institucijah itd. in ga tako od njih odtujiti. Pri pozitivnem načinu pa poudarjamo

predvsem lastne oz. zaželene podobe z namenom, da vzpodbudimo nasprotnika, da bi jih sprejel za svoje (Raman v Svete 2002).

V svojem razvoju je tudi psihološko bojevanje uporabilo vsa razpoložljiva sredstva za svoje delovanje, in seveda IKT ni nikakršna izjema. Za namene psihološkega bojevanja se torej lahko danes, poleg tradicionalnih medijev, kot so radio, televizija, tisk ipd., uporabljajo tudi faksi, elektronska pošta, elektronski nosilci podatkov in seveda internet. Ti elektronski instrumenti so dodobra spremenili psihološko bojevanje tako držav kot posameznih skupin, saj nova tehnologija omogoča prilagoditev psihološkega bojevanja izbranim posameznikom, interesnim skupinam in strankam za razliko od preteklosti, ko je bilo usmerjeno na skupnost ali skupino ljudi.

Glavna in najpogosteje uporabljena oblika psihološkega bojevanja je **propaganda**, ki jo Daughtery in Janowitz definirata kot: *načrtno širjenje novic, informacij, specifičnih argumentov in pozivov z namenom vplivati na prepričanja, mnenja in delovanja določenih skupin«* (Daughtery in Janowitz v Malešič, 1997:32). Poleg te definicije obstaja še vrsta drugih opredelitev, iz katerih lahko izluščimo nekatere temeljne značilnosti propagande, in sicer, da se izvaja s komunikacijsko aktivnostjo, da vpliva na ljudi, da poteka zavestno in načrtno, in da so propagandne aktivnosti dobro organizirane ter usmerjene proti specifični ciljni skupini – recipientu (Malešič, 1997: 34).

Na tem mestu velja opozoriti na razliko med propagando in reklamo. Po mnenju Domenach-a ima propaganda politične, reklama pa komercialne cilje (Domenach v Krunić, 1997). Glede na določljivost nosilcev ločimo »belo«, »sivo« in »črno« propagando. Pri prvi je izvor poznan, javen ali uraden, pri drugi je izvor prikrit, vendar ga je z analizo mogoče razkriti, pri zadnji pa je izvor informacij neresničen in se izvaja preko tajnih virov (Krunić, 1997).

Poleg propagande obstajao tudi druge metode za vplivanje na obnašanje in stališča ljudi, kot so: pranje možganov (vsiljevanje določenih vrednot ali vzorcev obnašanja posamezniku ali skupini), deprivacija ali odvzem (hrane, spanja in senzorna deprivacija), sugestija s pomočjo sublimacijske stimulacije (vsiljevanje določenih vrednot v podzavest posameznika ali skupine ljudi), prepričevanje (persuacija), psihokirurgija, električna stimulacija možganov, elektrošok, psihotronski generatorji in mamila (Krunić, 1997: 101–109).

Koncept psihološkega bojevanja vsebuje naslednje štiri oblike: **operacije za slabitev volje prebivalstva**, **operacije proti nasprotnikovim silam**[7], **operacije proti nasprotnikovim poveljnikom**[8] ter **kulturni konflikt.** Bolj podrobno bom opredelila dve izmed oblik, ki sta za mojo analizo bolj pomembni, to so operacije za zmanjševanje volje prebivalstva in kulturni konflikt, saj gre tu za delovanje na civilno sfero. Operacije proti enotam in operacije proti nasprotnikovim poveljnikom pa so usmerjene v vojaško sfero in za mojo analizo niso tako pomembne, vendar vseeno vredne omembe (Libicki, 1995).

Operacije za slabitev volje prebivalstva

Te operacije zajemajo uporabo množičnih medijev[9] za doseganje želene podobe (lastne ali nasprotnikove) med prebivalstvom (lastnim ali nasprotnikovim).

Ker se je uporaba množičnih medijev močno pocenila, si lahko interesne skupine zagotovijo neomejen promet preko satelita, ki je bil še pred nekaj desetletji zelo drag. S tem pa se pojavi problem, saj lahko z majhnimi stroški uporabljajo satelite (prav tako internet in druge informacijsko-komunikacijske sisteme) skupine skrajnežev, kot so teroristi in multinacionalna kriminalna združenja, za širjenje svojih idej in interesov. Množični mediji in tudi mikrooddajniki (tj. oglaševalci preko interneta in drugih informacijskih sistemov) postajajo vedno bolj pomembni pri razširjanju idej interesnih skupin in doseganju njihovih ciljev (Libicki, 1995; Mišmaš, 1999).

Kulturni konflikt

Kulturni konflikt[10] je napad na vrednostno strukturo določene družbe oz. posredovanje lastnih kulturnih vrednot tej družbi. To dosežemo s prenosom prek multinacionalk, interneta, satelitske televizije ...

Kulturno vojskovanje je najbolj učinkovito proti državam, ki imajo trdne in tradicionalne kulturne norme in vrednote (Libicki, 1995).

V okviru tega je potrebno omeniti **strateško kulturo**, ki se v varnostnopolitični analizi nanaša na izkušnje iz preteklih vojn in mirnodobnega stanja, predstave o vlogi oboroženih sil pri zagotavljanju miru, načine zaznavanja ogrožanja, podobe o nasprotnikih, načinih sodelovanja

[7] Delimo jih v dve kategoriji: vzpodbujanje strahu (smrti) in zmanjšanje podpore zaledja (civilnega prebivalstva) do vojakov na fronti (Libicki, 1995).
[8] Cilj teh operacij je zavajanje poveljnikov, da sprejmejo napačno odločitev (Libicki, 1995).
[8]Množični mediji v današnjem času vplivajo na vsa področja človekovega bivanja. Postali so dostopni vedno večjemu krogu ljudi, zmanjšal se je časovni zamik informacij (Mišmaš, 1999).
[10] Libicki kot tipičen primer tega navaja »*amerikanizacijo*« oz. ameriški kulturni imperializem (Libicki, 1995).

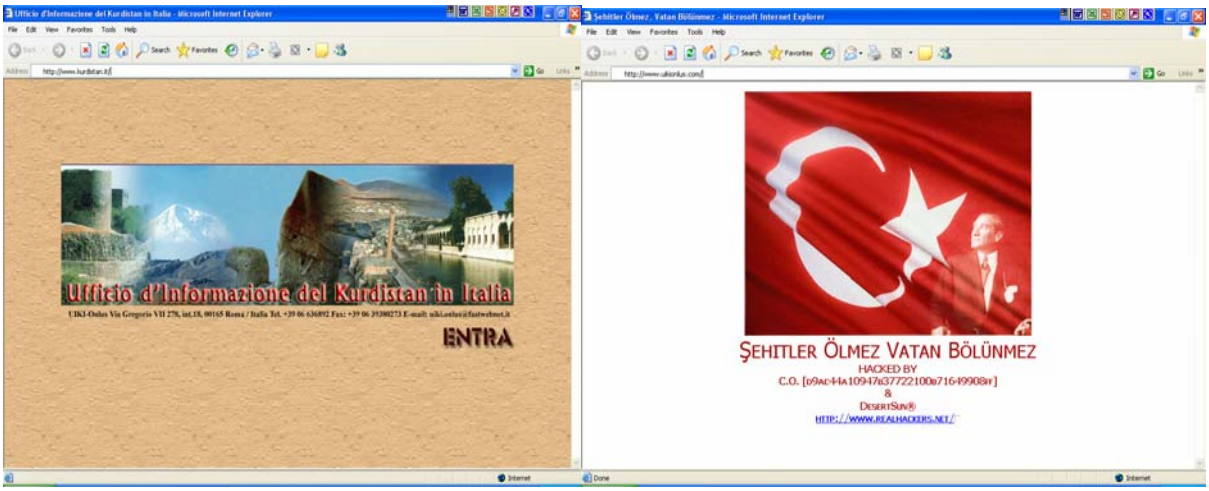
med akterji (unilaterizem, multilaterizem) ter na izkustvenih principih in principih na znanju temelječe vojaške strategije (Siedschlag v Svete, 2005: 58).

4.4.2 Hekersko in kibernetsko bojevanje

Martin Libicki loči hekersko in kibernetsko bojevanje, vendar sta si ti dve obliki informacijskega bojevanja zelo podobni in uporabljata podobna orodja, zato jih bom opredelila na enem mestu. Obe omenjeni obliki se nanašata na napade na računalniške sisteme in omrežja.

Hekersko bojevanje samo po sebi navadno ni nevarno, kajti pravi hekerji želijo opozoriti le na ranljivost sistemov in vdorov v sisteme ne izkoriščajo. Hekerske napade delimo na nenamerne (niso pomembni kot instrument informacijskega bojevanja, čeprav imajo lahko hude posledice) in namerne, v katerih se hekerji postavijo na eno stran v konfliktu in poskušajo: onemogočiti delovanje nasprotnikovih spletnih strani ali samo spremeniti njihovo vsebino, ukrasti in prodati informacije, zlorabiti informacijske sisteme, izvajati programske napake znotraj informacijskih sistemov idr. (to politično delovanje hekerjev imenujemo tudi **hektivizem**) (Mišmaš, 1999; Svete, 2002). Primer hekerskega bojevanja oz. delovanja lahko najdemo tudi na primeru teroristične organizacije PKK (glej sliko 4.1.). V tem primeru gre za delovanje t. i. turških hekerjev proti teroristični organizaciji, in sicer za »prevzem« domače spletne strani Kurdskega informacijskega biroja v Italiji – UIKI-Onlus.

SLIKA 4.1. Primer hekerskega napada na domačo spletno UIKI-Onlus



Vir: http://www.kurdistan.it/, http://www.uikionlus.com/ (18. julij 2005)

Hekerski napadi so danes vsakodnevna stvar[11], vendar pa ima večina napadov minimalne posledice. Hekersko bojevanje se vse pogosteje uporablja tudi kot oblika informacijskega terorizma in informacijskega kriminala (Arsić 2004).

Hekerji za svoje delovanje uporabljajo različna hekerska orodja[12] kot so:

- **Računalniški virusi**, ki se v računalniškem sistemu delijo v neskončnost in s tem upočasnijo delovanje.
- **Črvi** (ang. worm) se podobno kot virusi samodejno razmnožujejo toliko časa, dokler ne zasedejo celoten prostor na trdem disku ali disketi, vendar za razliko od virusov ne okužijo že obstoječih datotek ali programov.
- **Trojanski konji** (ang. trojan horse) so neavtorizirane kode, priključene legitimnemu programu, namenjene izvajanju nepoznanih in za uporabnika nezaželenih operacij.
- **Logične bombe –** škodljivi programi, ki svojo funkcijo izvedejo šele, ko je izpolnjen določen pogoj.
- T. i. **»trap doors«** omogočajo hekerjem izven sistema, da se lahko vključijo v sistem.
- Podobni so tudi **vdori skozi stranska vrata** (ang. back doors), s katerimi si napadalec omogoči dostop do sistema z alternativno dostopno točko.
- Pri **vohljanju** (ang. sniffing), gre za nameščanje virusov (»vohljačev«) znotraj sistema, ki samo opazujejo dogajanje.
- **Socialni inženiring** (ang. social engineering) **–** napadalec prodre v varovano omrežje s pomočjo uporabe manipulativnih sredstev, prek katerih pridobi informacije.
- T. i. **»war dialing« –** odkrivanje nezavarovanih modemov in vstopanje prek njih v omrežje.
- **IP slepljenje** (ang. IP spoofing) – lažno predstavljanje napadalčevega sistema.
- **Lomilci ali razbijalci gesel** (ang. password cracker) so programi, ki obidejo varnostno geslo tako, da razkrijejo predhodno kriptografsko zaščiteno geslo.
- Različni **skenerji**[13] (ang. scanner) so programi, ki samodejno odkrivajo varnostne pomanjkljivosti v računalniških sistemih.
- T. i. **»root kit«** – orodja, ki skrivajo dejstva, da je varnost računalnika ogrožena.
- **Izkoriščanje** (ang. exploit) – izkorišča znano šibkost sistema.

[11] Pentagon dnevno zazna povprečno 500 poskusov vdora v svoje računalniške sisteme (Arsić, 2004).

[12] **Hekerska orodja** so programi, ki jih hekerji lahko uporabljajo za zlonamerne cilje, kot so prevzem nadzora nad računalniki na daljavo, dostop do zaupnih informacij, vzpostavljanje napadov, ki povzročajo zavračanje storitev (DoS), preiskovanje komunikacijskih vrat itd (Kapital, 2004).

[13] V grobem ločimo dve vrsti skenerjev: skenerji računalniških komunikacijskih vrat (ang. port scanners) in skenerji varnostnih lukenj (ang. volnerability scanners) (Bratuša, 2004).

- V zadnjem času pa postajajo vse bolj nevarna orodja za odtujevanje zaupnih osebnih podatkov. Eden najbolj znanih je **ribarjenje** (ang. phishing[14]) – napadalec s kombinacijo uporabe elektronske pošte in lažne spletne strani pridobi zaupne podatke uporabnikov.
- **Vrtanje skozi požarne zidove[15]** z lahko dostopnimi orodji kot so tracert, firewalk, HPING ipd. (Libicki, 1995; Skrt, 2004; Bratuša 2004a, 2004b, 2005a, 2005b, 2005c).

Kibernetsko bojevanje Libicki razume kot futuristični scenarij, številni drugi avtorji (predvsem iz informacijsko razvitih držav) pa poudarjajo, da je tak scenarij povsem možen.

Pri kibernetskem bojevajnu gre za izkoriščanje računalnikov in omrežij za izvajanje napadov na nasprotnika, pri čemer je glavni cilj povzročanje kinetičnih posledic v fizičnem okolju. Kibernetsko bojevanje se nanaša na delovanje v kibernetskem prostoru. Kibernetski prostor obsega vsakršno navidezno resničnost, temelječo na računalnikih in računalniških omrežjih. Najpomembnejši kibernetski prostor je internet, ki služi predvsem kot sredstvo psihološkega bojevanja, lahko pa je tudi infrastruktura za napade na druga omrežja, baze podatkov, pomembne strežnike ali celo računalnike posameznikov (Svete, 2002).
Libicki loči štiri oblike kibernetskega bojevanja:

- informacijski terorizem[16],
- semantični napad – računalniški sistem poskušamo prelisičiti, da v okolju prihaja do nekih sprememb, zaradi česar računalniški sistem preneha delovati pravilno ali pa se popolnoma ustavi,
- simulacijsko bojevanje – temelji na uporabi realističnih simulacij in
- Gibsonovo vojskovanje – temelji na vodenju celotnih vojaških operacij znotraj kibernetskega prostora. Tak napad je le teoretičen in bi bil možen samo v družbah, ki bi imele navidezno resničnost kot pomembno komponento vsakdana (Libicki, 1995).

Sredstva kibernetskega bojevanja so podobna ali celo enaka kot hekerska sredstva, najbolj znani pa so: virusi, črvi, logične in časovne bombe, trojanski konji in vohunska programska oprema (ang. spy-ware), od orodij za fizično uničenje informacijske tehnologije pa so najbolj znani mikrobi, ki razgradijo čipe ter EMP (ang. electromegnetic pulse) orožja (Libicki, 1995).

[14] Phishing je skovanka besed password (geslo) in fishing (ribarjenje), izgovarja se [fišing], tako kot ribarjenje po angleško (Skrt, 2004).
[15] Požarni zidovi so naprave, namenjene zaščiti računalniškega omrežja pred raznovrstnimi oblikami internetnih napadov (Bratuša, 2005c: 38).
[16] Informacijskemu terorizmu bo v nadaljevanju namenjeno samostojno poglavje, kjer ga bom tudi podrobneje opredelila.

5 UPORABA OBLIK INFORMACIJSKEGA BOJEVANJA V SODOBNEM TERORIZMU

5.1 Trendi v terorizmu

Terorizem sem opredelila že na začetku diplomskega dela, v poglavju temeljni pojmi in koncepti. V tem poglavju pa bom podala nekaj značilnosti sodobnega terorizma, saj se je terorizem in narava terorističnih groženj po koncu hladne vojne močno spremenila.

Arquilla, Ronfeldt in Zaninijeva menijo, da se bodo tudi v informacijski dobi v terorizmu ohranili nekateri tradicionalni motivi in načela. Terorizem bo še naprej ostal orožje šibkih in orožje v rokah držav – t. i. **državni terorizem**, njegova uporaba pa bo izrazito asimetrična. Še vedno bo to način za pridobivanje pozornosti. Včasih pa se bo pojavljal tudi kot pot do nove prihodnosti, ki jo je možno doseči samo z namernim uničenjem sedanjosti (Arquilla in ostali, 1999:40).

Vendar terorizem ni statični fenomen, zato se bo prilagodil času in situacijam. Po mnenju Arquille in sodelavcev, se v informacijski dobi spremembe v terorizmu nanašajo predvsem na organizacijo[17], doktrino in strategijo ter uporabo tehnologije. Skratka, po mnenju omenjenih avtorjev, se terorizem premika v smeri t. i. omrežne vojne (ang. netwar)[18] (Arquilla in ostali, 1999).

Čeprav so z večjo ubojnostjo terorizma vse pomembnejši neposredni učinki, še vedno ostaja glavna značilnost sodobnega terorizma psihološki dejavnik, kot posledica fizičnega uničenja.

Ena pomembnih značilnosti konvencionalnega terorizma je tudi izredna raznolikost tarč oz. ciljev. Zaradi že omenjenega pomena psihološkega učinka oz vzbujanja pozornosti, je terorizem navadno usmerjen predvsem v civilno sfero. Vendar so cilj terorističnih napadov lahko tudi vojaške enote in infrastruktura (Svete, 2002).

Naslednja značilnost terorizma je tudi vse večja ubojnost (glej prilogo B, ki prikazuje število terorističnih incidentov in žrtev od 1996 do 2003). V zadnjih letih se povečuje tudi število terorističnih incidentov, čeprav je skupno število terorističnih incidentov v primerjavi z 80.

[17] Po mnenju Arquille in sodelavcev, se opušča hierarhična struktura terorističnih organizacij in privzema struktura mreže (Arquilla in ostali, 1999).

[18] Burns in Stalker sta že v začetku 1960. zaznala pojav mrežne strukture nadzora, moči in komunikacij, ki naj bi zamenjala hierarhično strukturo. Mrežna struktura ima horizontalno usmerjeno komunikacijo, za razliko od prejšnjih struktur z vertikalno usmerjeno komunikacijo (Arquilla in ostali, 1999).

leti prejšnjega stoletja, nižje[19] (glej prilogo B). Na vse večjo ubojnost terorističnih dejanj vplivajo predvsem naslednji dejavniki:

- Zaradi velikega števila terorističnih napadov, morajo biti posledice čim bolj dramatične, da pritegnejo zadostno medijsko in javno pozornost.
- Teroristi so na podlagi izkušenj iz preteklosti postali vse bolj učinkoviti in so začeli uporabljati manjša, visoko razvita in bolj ubojna sredstva. Ta sredstva so, zaradi držav podpornic terorizma, teroristom relativno lahko dostopna.
- Aktivna vloga držav, ki podpirajo in sponzorirajo terorizem[20]. Te države omogočajo teroristom različne vire, ki povečajo sposobnosti planiranja, urjenja, obveščanja, financiranja, logistike ...
- Problem bo predstavljal tudi t. i. državni terorizem, pri katerem teroristične akcije izvajajo tajne službe držav ali teroristične organizacije, ki so z določenimi državami posredno ali neposredno povezane.
- Na eni strani povečanje števila amaterjev v terorizmu, kajti danes je relativno lahko pridobiti sredstva in metode terorizma iz knjig, zgoščenk ali prek interneta. Na drugi strani pa narašča prebrisanost in operativna tekmovalnost profesionalnih teroristov (Hoffman, 1999:10–14).

Na ubojnost v terorizmu pa ne vplivajo samo izvajalci terorizma, pač pa tudi tehnologije, ki jih uporabljajo. Ključni faktor pri naraščanju ubojnosti je uporaba celotnega spektra tehnologij v teroristične namene (Svete, 2002). Na tem mestu lahko deloma potrdim del moje prve hipoteze, da je terorizem zaradi uporabe IKT vse bolj učinkovit v smislu doseganja ciljev. Teroristi svoje cilje (politične, ideološke, socialne in druge) dosegajo prek nasilja, ki povzroča žrtve. S tem da terorizem povzroča vse več žrtev, so torej tudi teroristi bolj učinkoviti v doseganju ciljev, k čemur med drugimi dejavniki, kot sem že omenila, pripomore tudi uporaba IKT.

V sodobnem terorizmu se spreminjajo tudi vzroki delovanja. V preteklosti so bili pomembni predvsem ideološki in politični vzroki, danes pa so zelo pomembni tudi religiozni, ekonomski ter drugi družbeni vzroki. Vzroki terorizma vplivajo na cilje in uporabljena sredstva, tu lahko opazimo naslednje značilnosti:

[19] Za primer naj navedem, da je bilo leta 1986 612, 1987 666, 2002 199 in 2003 208 terorističnih incidentov (Kauppi, v Svete 2002:101, Patterns of Global Terrorism 2002, 2003, Patterns of Global Terrorism 2003, 2004).
[20] Leta 1997 je bilo na seznamu ZDA sedem držav podpornic terorizma: Kuba, Iran, Irak, Libija, Severna Koreja, Sudan in Sirija (Hoffman, 1999).

- Tarče teroristov so vse pogosteje turisti in delavci humanitarnih in drugih mednarodnih organizacij.
- Predvsem v Južni Ameriki in v nekdanji Sovjetski zvezi so ugrabitve in zajemanje talcev še vedno pogosta sredstva teroristov.
- Za teroristične napade, osredotočene na ekonomsko infrastrukturo, lahko pričakujemo, da se bodo nadaljevali in celo povečali, zlasti napadi povezani z distribucijo električne energije, transportom, turizmom in bančništvom.
- Lažna sporočila, še posebno grožnje z bombami, imajo velik lokalni učinek v prometu in turizmu.
- Internet postaja teroristom vse bolj pomembno sredstvo za pridobivanje informacij, širjenje propagande, medsebojno komuniciranje in načrtovanje operacij.
- Teroristi vse bolj uporabljajo napredno informacijsko tehnologijo, ki postaja tako sredstvo, kot tudi cilj terorističnega delovanja.
- Psihološki učinki terorističnih dejanj izgubljajo relativni pomen, kajti cilj teroristov ni več le opozoriti nase, pač pa povzročiti čim večjo fizično uničenje. Kljub temu pa psihološki učinki še vedno ostajajo zelo pomembni (Canadian Security Intelligence Service, 1999).

Zgoraj so predstavljene nekatere splošne značilnosti sodobnega terorizma. Za moje diplomsko delo pa so pomembni trendi, ki se nanašajo na predmet analize, in sicer na: kibernetsko in hekersko bojevanje v terorizmu, predvsem na uporabo informacijsko-komunikacijske tehnologije ter psihološke učinke, ki so posledica uporabe psihološkega bojevanja v terorizmu.

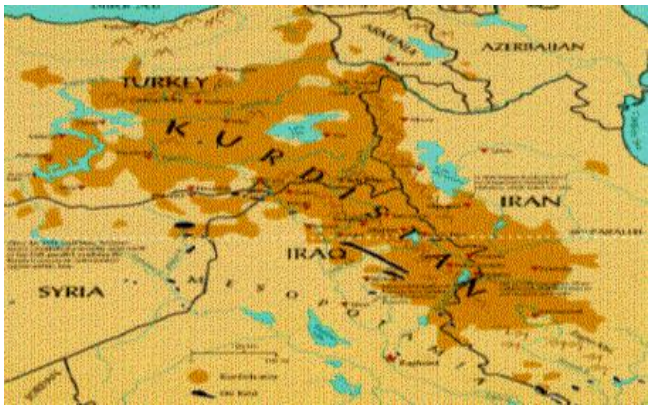
5.2 PKK

5.2.1 Zgodovina organizacije

PKK je kratica za Partiya Karkerên Kurdistan (slo. Kurdska delavska stranka, ang. Kurdistan Workers Party, nem. Arbeiterpartei Kurdistan). Ustanovljena je bila leta 1974, kot marksistično-leninistično uporniško gibanje, pod imenom Revolucionarna mladina. Leta 1978 se je gibanje preimenovalo v organizacijo PKK, ki je bila na začetku sestavljena le iz turških Kurdov. V začetku 1990. je PKK pričela s terorističnimi aktivnostmi proti varnostnim silam in civilnemu prebivalstvu, z namenom ustanoviti neodvisno, demokratično državo Kurdov na

območjih jugovzhodne Turčije, severnega Iraka ter delu Irana in Sirije[21] (glej sliko 5.2, ki prikazuje območja poseljena s Kurdi – Kurdistan) (Pike, 2004).

SLIKA 5.2.: Območja Turčije, Iraka, Irana in Sirije poseljena s Kurdi



Vir: Kurdish Information Network (1996) Dostopno na http://www.xs4all.nl/~tank/kurdish/htdocs/facts/ (25. oktober 2004)

Februarja 1999 so turški obveščevalci, s pomočjo izraelskega Mosada, v Keniji prijeli ustanovitelja in vodjo organizacije Abdullah-a Öcalana. Turško sodišče ga je obsodilo na smrtno kazen, ki jo je oktobra 2002, po odpravi smrtne kazni, spremenilo v dosmrtno ječo, ki jo prestaja na otoku Imrali v Marmanskem morju. Avgusta 1999 je Ocalan oznanil »mirovno pobudo« ter pozval člane PKK k premirju (Country Reports on Terrorism 2004, 2005). Leta 2000 je PKK sklenila enostransko premirje s Turčijo, s tem se je odrekla terorizmu in obljubila, da bo cilje dosegala le po politični poti. Vendar je kljub temu prihajalo do incidentov, saj PKK, izgovarjajoč se na samoobramo, ni nikoli predala orožja (Pike, 2004).

Leta 2002 je PKK spremenila ime v **KADEK** (Kurdski svobodni in demokratični kongres, ang. Kurdistan Freedom and Democracy Congress) ter razglasila, da bo izvajala le nenasilne aktivnosti v podporo kurdskim pravicam (Pike, 2004).

Konec leta 2003 je organizacija ponovno spremenila ime v **Kongra-Gel**[22]**,** kar je okrajšava za Kongra Gelê Kurdistan (KGK, slo. Ljudski kongres Kurdistana, ang. People's Congress of Kurdistan), ter ponovno poudarila »mirovne« namene, vendar je nadaljevala z napadi in še naprej zavračala razorožitev (Country Reports on Terrorism 2004, 2005).

[21] V Turčiji živi, po podatkih kurdske televizije Mezopotamya TV, 14 milijonov Kurdov, v Iranu 7 milijonov, v Iraku 4,5 miljonov in v Siriji 1 200 000 (http://www.metv.dk/).

[22] Zaradi veliko preimenovanj se v dostopni literaturi večinoma uporablja poimenovanje Kurdska delavska stranka s kratico PKK, kar je tudi njeno zadnje znano uradno poimenovanje; zaradi tega sem se tudi jaz odločila, da uporabljam to ime.

Prvega junija 2004 je vojaški del organizacije – Ljudske obrambne sile – HPG (orig. Hêzên Parastina Gel, ang. People's Defense Force) – prekinil enostransko premirje, ker jo je Turčija vseskozi smatrala za teroristično organizacijo in se držala načela »nepogajanja s teroristi« ter ni hotela sprejeti ponujenega premirja (Pike, 2004). Po prekinitvi premirja se je organizacija razdelila v dve skupini; prva je zagovarjala doseganje ciljev po politični poti, druga pa vrnitev k nasilnemu doseganju ciljev, slednja je februarja 2004 prevzela nadzor nad organizacijo (Country Reports on Terrorism 2004, 2005). Aprila 2005 se je organizacija uradno odločila, da se bo vrnila k prvotnemu poimenovanju **PKK** (Partiya Karkerên Kurdistan) (http://www.pkk.org).

5.2.2 Sorodne teroristične organizacije

PKK-ju sorodne teroristične organizacije so: **Apove[23] mladinske maščevalne brigade** (orig. Apocu Genclik Intikam Mufrezeleri, ang. Apo's Youth Revenge Brigades), **Apovi maščevalni sokoli** (orig. Apo'nun Intikam Sahinler, ang. Apo's Revenge Hawks) in **Nacionalistične kurdske maščevalne ekipe** (orig. Milliyetci Kurt Intikam Timleri, ang. Nationalist Kurdish Revenge Teams), ki so (bile) nacionalistične teroristične skupine, o katerih je zelo malo znanega. Za te organizacije ni zanano, ali delujejo samostojno ali pod okriljem PKK, ni pa tudi znano ali sploh še delujejo. **Kurdsko domoljubno združenje** (ang. Kurdish Patriotic Union) je prav tako nacionalistična teroristična organizacija, ki naj bi bila ustanovljena pod okriljem PKK-ja. Domoljubno združenje Kurdistana (PUK) trdi, da organizacija še vedno deluje, vendar v zavezništvu s Kurdskimi nacionalnimi zavezniškimi silami (ang. Kurdistan Allied National Forces). Za zgornje štiri PKK-ju sorodne organizacije ni znano ali še delujejo, nedvomno pa danes delujejo **Svobodni sokoli Kurdistana –** TAK (orig. Teyrbazen Azadiya Kurdistan, ang. Kurdistan Freedom Hawks). Organizacija je bila prvič omenjena 29. julija 2004. Njihove akcije so usmerjene predvsem na turistično industrijo (hotele, apartmaje ...), infrastrukturo in vladne tarče v Turčiji. Uradno ni povsem znano, ali je TAK neodvisna organizacija ali je povezana z drugimi kurdskimi skupinami. Turške oblasti sumijo, da je organizacija ustanovljena pod okriljem Kurdske delavske stranke (PKK), saj naj bi turška policija našla povezave med TAK in borci pod vodstvom Murata Karayilan, enega vodilnih mož PKK/Kongra-Gel (MIPT, 2005).

[23] Imenujejo se po vodji PKK A. Öcalanu, čigar vzdevek je "Apo", kar pomeni "Stric".

5.2.3 Struktura

Današnja organizacija je sestavljana iz:

- predsedstva (predsednik in šest namestnikov),
- Glavne skupščine (sprejema vse odločitve),
- Izvršnega odbora (usklajuje in upravlja aktivnosti),
- deset Izvršnih komitejev (Politični komite[24], Socialni komite, Ekonomski in finančni komite, Znanstveni, kulturni in umetnostni komite, Tiskovni komite[25], Ženski komite, Komite mladih, Komite ekologije in lokalnih oblasti, Komite zakonodaje in človekovih pravic, Komite ljudske obrambe[26]),
- Disciplinskega odbora,
- Posvetovalnega odbora in
- Demokratično-ekoloških usklajevalcev (http://www.kongra-gel.com).

5.2.4 Aktivnosti PKK

Organizacija, ki ima po ocenah nekje med 4000 do 5000 članov (večina – 3000 do 3500 – se jih nahaja v severnem Iraku) ter na tisoče simpatizerjev v Turčiji in Evropi, deluje na območju Turčije, Iraka, Evrope in Srednjega Vzhoda. Organizaciji zagotavljajo varno zavetje in zmerno pomoč Sirija, Iran in Irak. Sirija in Irak v zadnjem času kažeta neke znake sodelovanja s Turčijo proti organizaciji, vendar v zelo omejenem obsegu. PKK izrablja Evropo za zbiranje materialnih in finančnih sredstev ter za širjenje politične propagande (Country Reports on Terrorism 2004, 2005).

Primarne tarče PKK so bile turške vladne vojaške sile v Turčiji, lokalni uradniki ter civilni prebivalci v Turčiji, ki so nasprotovali organizaciji. Spekter tarč je pozneje razširila še na diplomatske in trgovske cilje v zahodnoevropskih mestih. Z namenom uničiti turško turistično industrijo, je PKK po letu 1990 začela napadati turistične točke in hotele ter ugrabljati tuje turiste. Tudi v času premirja je nadaljevala z napadi, znan je vsaj en napad proti Turčiji v letu 2003 (Patterns of Global Terrorism 2003, 2004). V letu 2004 je bilo večino nasilja PKK usmerjenega proti turškim varnostnim silam. Turški tisk poroča o številnih napadih tako v letu

[24] Politični komite sestavljata komiteja za notranje in zunanje zadeve (http://www.kongra-gel.com/).
[25] Njegova naloga je skrb za javno menenje v Kurdistanu in izven njega, organizairanje tiska in publikacij na nacionalni ravni, razvijanje ustreznih in ustanavljanje novih institucij (http://www.kongra-gel.com/).
[26] Ta komite je formiral Ljudske obrambne sile (HPG), ki predstavljajo vojaški del organizacije. Glede na Ustanovno listino organizacije Kongra-Gel, je bil ta del organizacije sprva namenjen zgolj vojaški obrambi za zagotavljanje svobode in temeljnih pravic Kurdov ter varovanju življenj njihovih voditeljev. Prvega junija 2004 pa je ta del organizacije razglasil konec premirja in začel tudi z napadalnimi aktivnostmi (http://www.kongra-gel.com).

2004 kot 2005. Zelo verjetno pa je bila odgovorna za neuspešen julijski napad z avtomobilsko bombo na guvernerja province Van. Vpletena naj bi bila tudi v avgustovsko bombardiranje dveh carigrajskih hotelov in plinskega kompleksa, v katerem sta umrli dve osebi (Country Reports on Terrorism 2004, 2005).

V vojni med PKK in turškimi varnostnimi silami je (od začetka boja za neodvisnost kurdskega dela Turčije leta 1984 do sklenitve enostranskega premirja leta 1999), po nekaterih podatkih, življenje izgubilo prek 30.000 ljudi[27]. Junija 2005 je turška vojska izdala novo poročilo, po katerem naj bi v tem boju umrlo 18.475 turških vojakov in 12.485 civilistov, prejšnje številke pa so bile 5.555 vojakov in 5.302 civilistov. V tem novem poročilu ni podatkov o smrtnih žrtvah med pripadniki PKK. Tako naj bi bilo skupno število mrtvih, če upoštevamo stare podatke o mrtvih teroristih, 54.598, kar je 20.103 več kot v predhodnem poročilu. Če pa upoštevamo še število civilnih žrtev med Kurdi, ki so bile posledica delovanja državno podprte turške Hizbullah, se število žrtev dvigne prek 73.000 (http://www.dozame.org/).

Po prekinitvi premirja od junija 2004 pa do maja 2005, pa naj bi po podatkih HPG (glej prilogo C) turška stran imela 718 žrtev, HPG pa 96 (http://www.dozame.org/).

5.3 Kibernetsko in hekersko bojevanje kot orožje teroristov

5.3.1 Razdiralni napadi

Teroristi, zaradi različnih razlogov, raje kot uničevalne, uporabljajo razdiralne napade. Na primer: teroristi, ki se zanašajo na internet zaradi propagandnih aktivnosti in komunikacije, raje vidijo, da se sistem le upočasni, kot pa da se uniči.

Teroristi lahko uporabljajo IKT v »razdiralne« namene z elektronskimi napadi, ki začasno onesposobijo, vendar ne uničijo fizično ali virtualno infrastrukturo. Ti napadi vključujejo »dušitev« računalniškega sistema s sredstvi kot so: elektronske bombe, zasičenje sistema in različne, hekerske tehnike in orodja (Zanini in Edwards, 2001).

Takšnih napadov je bilo do nedavnega relativno malo, vendar njihova pogostost vse bolj narašča. Primer takšnega napada je bil napad teroristične skupine Tamilskih tigrov (LTTE – Liberation Tigres of Tamil Eelam). Japonske skupine so baje napadle računalniški kontrolni sistem rednih vlakov, kar je paraliziralo glavna mesta za več ur (Devost in ostali, 1997). Leta

[27] V tiskanih medijih in tudi uradnih virih najdemo zelo različne podatke o skupnem številu žrtev. Številke se gibljejo od 30.000 do 40.000 žrtev.

2000 je skupina pakistanskih hekerjev, imenovanih MOS (Muslim Online Syndicate), uničila prek 500 spletnih strani v Indiji, v protest proti konfliktu v Kašmirju. Pakistanski Lashkare-Taiba so trdili, da so v začetku leta 2000 napadli vojaške spletne strani v Indiji (Zanini in Edwards, 2001: 44).

Pri preučevanju teroristične organizacije PKK nisem zasledila nobenega hekerskega napada. Zasledila sem le, že omenjeni, napad turških hekerjev na spletno stran UIKI-Onlus (glej sliko 5.1).

5.3.2 Uničevalni napadi

Uporaba IKT lahko vodi tudi do dejanskega uničenja fizičnega in virtualnega sveta. Uničevalni virusi in črvi lahko trajno uničijo ali pokvarijo podatke in povzročijo veliko gospodarsko škodo – v primerih, ko gre za napade na kritično infrastrukturo (npr. kontrolo letenja, energetski sistem, sistem oskrbe z vodo ...), celo izgubo življenj. Takšne napade večina avtorjev s tega področja označuje kot informacijski terorizem oz. kibernetični terorizem (ang. cyberterrorism) (Zanini in Edwards, 2001).

Nekateri avtorji (npr. Cronin in Crawford) h kibernetskemu bojevanju prištevajo tudi fizično uničenje nasprotnikovih informacijskih in komunikacijskih sredstev s konvencionalnim orožjem[28] (Cronin in Crawford v Svete, 2005). Takšne napade (glede na podatke MIPT Terrorism Knowledge Base) zasledimo tudi pri PKK. Takšnih napadov je PKK oz. z njo povezane teroristične organizacije izvedla malo, znana sta le dva. 03. 06. 2005 so TAK (Svobodni sokoli Kurdistana) v Hassi (Turčija) nastavili eksplozivno telo na postajo mobilne telefonije, v tem napadu je bila huje ranjena ena oseba. Drugi tak napad pa naj bi domnevno izvedla PKK 07. 07. 2004 – razneslo je oddajno postajo (oddajnik) v Kagizmanu (Turčija), kaj je povzročilo eksplozijo ni znano (MIPT, 2005).

[28] To obliko informacijskega bojevanja Libicki prišteva k elektronskemu bojevanju, ki je po njegovem mnenju lahko protiradarsko (ang. antiradar) ali protikomunikacijsko (ang. anticommunication). Poleg teh dveh oblik pa sem šteje še kriptografijo (Libicki, 1995).

5.4 Vprašanje in pomen informacijskega terorizma

5.4.1 Uporaba informacijsko komunikacijske tehnologije v terorizmu

Kot sem že omenila, številne teroristične organizacije uporabljajo IKT – računalnike, programsko opremo[29], telekomunikacijska sredstva in internet – za boljšo organizacijo in uskladitev aktivnosti. Teroristi se polaščajo IKT zaradi različnih vzrokov: izboljša komunikacijo in podpira organizacijo, članom dopušča hitro usklajevanje z velikim številom privržencev ter predstavlja osnovo za propagando in protipropagando ter prenos kodiranih sporočil, pri čemer uporabljajo javno dostopno kodirno opremo in izvajanje napadov za ohromitev nasprotnikovih informacijskih sistemov (virusi ter DoS[30] metode). IKT (internet) omogoča teroristom, da širijo svoje ideje ter dosežejo krog potencialnih donatorjev in rekrutov povsod po svetu (Terrorism files.org, 2002).

Torej, uporaba IKT teroristom ponuja velik spekter prednosti. Največji pomen imajo predvsem naslednje prednosti:

- IKT je močno zmanjšala prenosni čas 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.
- Povezovanje računalništva in komunikacije je znatno povečalo obseg in zapletenost informacij.
- IKT omogoča teroristom, da dosežejo ciljno občinstvo, tudi ko drugi izhodi in mediji zatajijo, ter da dosežejo tudi novo občinstvo (mlade in izobražene) (Whine, 1999, Zanini in Edwards, 2001).

Zanninijeva in Edwards trdita, da IKT omogoča teroristom tri vrste aktivnosti:

- propagandne aktivnosti,
- napade na virtualne tarče, z namenom motenja in ne uničenja ciljnega informacijskega sistema,
- fizično uničenje tarče (informacijski terorizem) (Zaninini in Edvards, 2001).

[29] Programska oprema (ang. software) je oprema za računalniški sistem, sestavljena iz programov, ki se izvajajo v računalniku. Programska oprema je lahko shranjena v osnovnem pomnilniku računalnika (trdi disk) ali v zamenljivem hranilniku (diskete, CD plošče, magnetni trak). Programsko opremo sestavljajo besedilo programa, ki so ga napisali programerji, izvršljive datoteke s strojnim besedilom programa, ki so ga iz izvirnega besedila ustvarili prevajalniki in obsežna dokumentacija (Leksikon rač. in inf., 2002:458).

[30] Denial of service – napadi za zavrnitev storitve.

5.4.1.1 Internet

Med vsemi informacijsko-komunikacijskimi tehnologijami ima največji pomen ravno uporaba interneta. Sicer obstajajo še druga omrežja, vendar internet za razliko od ostalih mrež nima načrtnega strukturiranja in hierarhične delitve. Prednost interneta je tudi, da vsak udeleženec v elektronski mreži ni zgolj uporabnik informacij temveč tudi potencialni proizvajalec informacij (Svete, 2005).

Internet (skrajšano iz angleške besede »inter-network«, *medmrežje*) je največje omrežje računalnikov na svetu, ki združuje na stotisoče krajevnih omrežij in strežnikov ter na milijone osebnih računalnikov (Webdesign.fluido.it, 2002).

Predhodnik interneta je nastal v 70. letih prejšnjega stoletja (leta 1969) kot posledica poskusa ameriškega obrambnega ministrstva, da bi oblikoval porazdeljeno računalniško omrežje brez središča upravljanja, ki bi bilo odporno zoper napake in prekinitve v komunikacijskih kanalih in bi bilo manj občutljivo na posledice jedrskega napada. To omrežje se je takrat imenovalo ARPANET[31] in je povezovalo računalnike na univerzah in v obrambnih ustanovah ter radijska in satelitska omrežja. Omogočalo je delo na oddaljenih računalniških sistemih, prenos datotek, elektronsko pošto in izmenjavo informacij po interesnih skupinah (Dimec, 2002).

Leta 1983 se je ARPANET razcepil na vojaško omrežje MILNET (MILitary NETwork) in na raziskovalno omrežje ARPANET. Vsi računalniki, priključeni na ARPANET, so morali uporabljati protokole TCP/IP (Transmission Control Protocol/Internet Protocol[32]) (Dimec, 2002).

V začetku 80. let so začela nastajati tudi krajevna omrežja in tako so tudi druge organizacije začele graditi svoja omrežja. Eno takšnih omrežij je bilo NSFNET (National Science Foundation Net), ki je uporabljal isti komunikacijski protokol kot ARPANET. Do začetka 90. let je bil Internet sestavljen iz omrežij državnih ustanov (univerze, vladne organizacije in raziskovalna središča) in se je uporabljal predvsem v akademske namene. NSFNET pa je pomenil prelomnico, saj je s tem omrežjem veliko več ljudi dobilo dostop do prostranega omrežja (Dimec, 2002).

Sredi 90. let se je vedno več podjetij odločalo za oblikovanje intranetov – lastnih zaprtih omrežij. Leta 1991 je švicarsko raziskovalno središče CERN objavilo določila za svetovni

[31] ARPANET (Advanced Research Projects Agency Network) je sprva povezoval le tri računalnike v Kaliforniji in enega v zvezni državi Utah, kmalu pa se je razširil čez celotno celino (Webdesign.fluido.it, 2002).
[32] Protokol (ang. protocol) je zbirka pravil, ki določajo postopek za izmenjavo (prenos) podatkov med dvema ali več računalniki, ki so medsebojno povezani (Webdesign.fluido.it, 2002).

splet (ang. www oz. world wide web) in to je sprožilo velik razmah interneta. Leta 1995 je bil ustvarjen Netscape Navigator – standard za spletne programe – in splet je sredi leta postal najbolj rabljena storitev v Internetu. Splet je slikovno okno v Internet in sistem za shranjevanje in pregledovanje informacij v računalniških dokumentih. Osnovna organizacijska enota informacije v spletu je spletna stran oz. dokument (Dimec, 2002).

Danes je internet dostopen skoraj vsem, zato lahko informacija objavljena na internetu v trenutku obkroži ves svet, saj je danes, po podatkih Internet World Stat, v svetu 888.681.131 uporabnikov interneta, kar predstavlja 13,9% svetovne populacije. V Turčiji pa je bilo po podatkih Internet World Stat, marca 2005, 6 miljonov uporabnikov interneta, kar predstavlja 8,2 odstotka celotne populacije[33] (Internet World Stats, 2005).

Terorizem in Internet sta povezana v več vidikih. 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 aktivnosti 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 – informacijski terorizem (ADL, 1998; Weimann, 2004).

5.4.2 Opredelitev informacijskega terorizma

Informacijski terorizem nekateri avtorji vključujejo v okvir informacijskega bojevanja, drugi pa menijo, da je že samo informacijsko bojevanje popolno teroristično orožje (Shahar, 1997).

Teroristi danes vse pogosteje uporabljajo IKT tako za organiziranje, motiviranje, komuniciranje, vpliv na javnost, kot za izkoriščanje ranljivosti informacijsko razvitih držav. Zato danes vse pogosteje govorimo o informacijskem terorizmu. Termin informacijski 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).

Termin informacijski terorizem oz. kibernetski terorizem, kot ga nekateri imenujejo, se nanaša na dva pojma, in sicer kibernetski prostor oz. virtualni svet in terorizem.

[33] Turčija je imela po podatkih CIA World Factbook junija 2005 69.660.559 prebivalcev. Od tega je približno 20% Kurdov (CIA World Factbook).

Collin virtualni svet definira kot »kraj, kjer računalniški programi delujejo in se podatki premikajo« (Collin v Politt, 1997).

Za terorizem pa ne obstaja neke univerzalne opredelitve. Mark Politt, posebni agent FBI, je uporabil opredelitev terorizma, ki jo ponuja Ministrstvo za zunanje zadeve ZDA. »Terorizem pomeni naklepno, politično motivirano nasilje, nedržavnih skupin in tajnih agentov, zagrešeno proti nevojaškim tarčam, navadno z namenom vplivati na občinstvo« (Ministrstvo za zunanje zadeve ZDA v Politt, 1997).

S kombiniranjem zgornjih dveh definicij je Politt izdelal delovno definicijo informacijskga terorizma, ki pravi: »Informacijski terorizem (kibernetski terorizem) je naklepen politično motiviran napad nedržavnih skupin in tajnih agentov na informacije, računalniške sisteme, računalniške programe in podatke, ki ima za rezultat nasilje nad civilnimi tarčami« (Politt, 1997). Politt tudi meni, da informacijski teroristi za doseganje ciljev uporabljajo neubojno (ang. soft) nasilje, ki deluje predvsem psihološko (Politt, 1997).

Podobno definicijo uporablja v številnih člankih, intervjuih in tudi v pričanju pred ameriškim parlamentarnim Odborom vojaških služb (Congress' House Armed Services Committee), Dorothy E. Denning (glej Denning 1999, 2000a, 2000b, 2001).

> Denningova meni, »da je kibernetski terorizem zbliževanje kibernetskega prostora in terorizma. Nanaša se na nezakonite napade ali grožnje z napadi na računalnike, omrežja in informacije shranjene v njih, z namenom prestrašiti ali siliti vlado ali ljudi, v podporo političnim ali socialnim ciljem. Da dejanje ustreza informacijskemu terorizmu mora imeti za posledico nasilje nad osebami ali lastnino, ali povzročiti vsaj toliko škode, da povzroči strah. Primer so napadi, ki vodijo v smrt ali telesne poškodbe, eksplozije ali resne ekonomske izgube. Resni napadi na kritično infrastrukturo[34] so tudi lahko dejanja informacijskega terorizma, vendar je odvisno od njihovega vpliva. Medtem ko napadi, ki uničijo nebistvene službe ali povzročijo predvsem finančno škodo, niso dejanja informacijskega terorizma« (Denning 2001: http://www.ssrc.org/sept11/essays/ denning.htm).

Devost, Houghton in Pollard, informacijski terorizem opredelijo s pomočjo metod informacijskega napada. Avtorji menijo, da v družbah tretjega vala – tj. informacijskih družbah, obstajata dve ključni metodi informacijskega terorističnega napada:

[34] Kritično infrastrukturo, kot sem že omenila, predstavljajo energetsko omrežje, komunikacijska, trensportna in finanačna infrastruktura (Lewis, http://www.fas.org/irp/eprint/snyder/infowarfare. htm).

- IKT kot cilj oz. tarča, ki je lahko fizična ali digitalna.
- IKT kot orodje oz. sredstvo za večjo operacijo, to sredstvo pa je lahko fizično ali digitalno.

Prva metoda vključuje napad na informacijske sisteme, z namenom uničiti ali onesposobiti sam informacijski sistem ali informacijsko infrastrukturo, ki je odvisna od napadene tehnologije.

Druga metoda pa vključuje manipuliranje (z) in izkoriščanje informacijskih sistemov, spreminjanje ali krajo podatkov, ali prisilitev sistema, da opravlja funkcije, za katere ni namenjen (Devost in ostali, 1997–1998).

TABELA 5.1: Metodi terorističnega napada

		CILJ (ang. target)	
		FIZIČEN	DIGITALEN
ORODJE (ang. tool)	FIZIČEN	a) Uporaba fizičnih sredstev za napad na fizične tarče – klasični terorizem.	b) Uporaba fizičnih sredstev oz.orodij za napad na digitalne cilje (npr. napad IRE na London Square Mile 4. oktobra 1992)
	DIGITALEN	c) Izkoriščanje informacijskih sistemov za uničenje fizičnih ciljev (npr. heker prelisiči kontrolo letenja in zaradi tega strmoglavi letalo)	d) Uporaba digitalnih orodij za digitalne tarče oz. cilje (npr. trojanski konj v javnem omrežju)

Vir: Devost, Matthew G., Houghton, Brian K. in Pollard, Neal A. (1997–1998): Information Terrorism: Can You Trust Your Toaster?. (Dostopno tudi na http://all.net/books/tzu/tzu.html, 9. november 2004).V *Sun Tzu Art of War in Information Warfare*.

V tabeli 5.1 točka a) predstavlja klasični (konvencionalni) terorizem (ugrabitve letal, jemanje talcev, bombni napadi, umori ipd). Točke b), c) in d) naj bi predstavljale informacijski terorizem. Točka d) pa je, po mnenju avtorjev, t. i. »čisti« informacijski terorizem, ki ga je najtežje odkriti in se proti njemu boriti (Devost in ostali, 1997–1998).

Pri informacijskem terorizmu gre torej za napade na računalniške sisteme, z namenom prizadejati škodo posameznikom in ne računalnikom. Značilnosti le-tega so 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 takšnih podatkov bi lahko imela hude posledice (Libicki, 1995).

5.4.3 Pomen informacijskega terorizma

Informacijski terorizem predstavlja varnostnemu sektorju zahodnih držav enakovredno ali celo večjo grožnjo kot klasični terorizem. Najnižje oblike informacijskega terorizma, v smislu uničevalnosti, so bombe in napadi prek elektronske pošte na uporabnike interneta, višje oblike pa vključujejo uporabo interneta kot katalizatorja za dosego ciljev klasičnega terorizma višje stopnje. Vendar je bilo po mnenju Denningove zelo malo ali sploh nič računalniških napadov, ki bi ustrezali kriterijem informacijskega terorizma. Vsi dosedanji informacijski napadi so kvečjemu prestrašili žrtve, noben pa ni vodil v nasilje ali poškodovanje ljudi, kot predvideva zgoraj zapisana delovna definicija informacijskega terorizma. Najbližje kriteriju informacijskega terorizma je bil napad z elektronsko pošto[35] teroristične skupine Tamiski tigri na veleposlaništvo Širilanke (Denning, 2000a).

Denningova torej meni, da je grožnja informacijskega terorizma zgolj teoretična, vendar kljub temu vredna pozornosti. Za razumevanje potencialne grožnje informacijskega terorizma moramo upoštevati dva ključna dejavnika: ali obstajajo tarče, ki so ranljive na napad, ki vodi v nasilje ali resno škodo in ali obstajajo sposobni in motivirani akterji za izvajanje dejanj informacijskega terorizma. Če pogledamo najprej ranljivost tarč, lahko ugotovimo, da so številne študije pokazale, da je kritična infrastruktura potencialno ranljiva na informacijski teroristični napad. Kar zadeva sposobne in motivirane akterje, pa je zadeva sledeča: mnogi hekerji imajo znanje, veščine ter orodja, primanjkuje pa jim motivacije za povzročanje nasilja in resne škode ekonomskemu ali socialnemu sistemu, medtem ko teroristi imajo motiv, vendar jim ponavadi primanjkuje sposobnosti (znanja in veščin) za takšen napad (Denning, 1999 in 2000a).

Informacijski terorizem ima tudi slabosti, ki jih predstavljajo kompleksni sistemi, zaradi katerih je težje nadzorovati napad in doseči željeno stopnjo škode. Če niso poškodovani ljudje, je tako dejanje manj dramatično in je manj čustvene prizadetosti. Slabost je tudi, da teroristi prisegajo na preverjene in pristne metode ter odklanjajo nove, dokler so stare učinkovite (Denning, 2001).

Kljub slabostim, ki jih ima informacijski terorizem, pa mu je vseeno treba posvečati pozornost. Nova generacija teroristov bo zrasla v digitalnem svetu, zato bo razpolagala z večjim hekerskim znanjem in veščinami in s še močnejšimi ter lažje uporabljivimi hekerskimi

[35] Leta 1998 je etnična teroristična skupina Tamilski tigri dva tedna pošiljala po 800 elektronskih sporočil na dan veleposlaništvu Širilanke. Vsebina sporočila je bila: »Mi smo Internetni črni tigri in to delamo zato, da motimo vaše komunikacije.« Oblasti so ta dogodek označile za prvi znani teroristični napad na državni računalniški sistem (Denning, 2000a).

orodji. Le-ti bodo lahko videli večji potencial za informacijski terorizem kot današnji teroristi. Lahko pričakujemo tudi, da se bosta v prihodnje resnični in virtualni svet zelo zbližala z velikim številom naprav priklopljenih na internet, in takrat bo informacijski teorizem postal bolj privlačen (Denning, 2001).

Trenutno torej informacijski terorizem ne predstavlja konkretne grožnje, vendar se to lahko kmalu spremeni. Za teroriste imajo take metode lahko prednosti pred klasičnimi. Prednosti informacijskih orožji so, da se tak napad lahko vodi oddaljeno (ni fizičnih meja) in anonimno, je cenejši in ne zahteva rokovanja z eksplozivom in samomorilskih akcij. Informacijska orožja lahko zadanejo več tarč hkrati ali delujejo selektivno. Takšen napad bi tudi pritegnil pozornost medijev in vlade (Denning, 2001; Savino, 2002; Golubev, 2003).

Thomas loči devet možnih načinov delovanja terorističnih organizacij na internetu: zbiranje občutljivih podatkov o tarčah, zbiranje finančne podpore, povezovanje med različnimi skupinami, izsiljevanje, propaganda, vesoljna svoboda[36], psihološki vplivi, goljufije ter prikrite operacije (Thomas, 2002). Podobno Belič v informacijskem smislu loči štiri oblike delovanja teroristčnih 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, so lahko le pripravljalne stopnje v klasično teroristično dejanje. Pri terorističnih napadih z informacijskimi orodji – orožji pa je nujen jasen cilj napada (npr. elektroenergetski sistem, sistem transporta, borza ...) Osnovni cilj takšnega napada je onesposobljenje ciljnega informacijskega sistema (Belič, 2001:263).

Teroristične organizacije (tudi PKK) kibernetski prostor uporabljajo predvsem za pospeševanje, olajševanje klasičnih oblik terorizma, kot je na primer nastavljanje bomb. Izrabljajo torej predvsem komunikacijske možnosti interneta za neposredno in posredno komunikacijo. Neposredna komunikacija se uporablja predvsem za zbiranje finančne podpore, rekrutiranje in mobilizacijo, načrtovanje akcij, posredovanje informacij, koordinacijo aktivnosti ipd. Posredna komunikacija pa se uporablja predvsem za psihološko bojevanje (objavljanje, propagando in protipropagando) Internet se s strani terorističnih organizacij uporablja predvsem za izvajanje propagande in protipropagande, za prenos kodiranih sporočil ter izvajanje napadov za ohromitev nasprotnikovih informacijskih sistemov. Internet omogoča teroristom anonimnost, hkrati pa predstavlja učinkovito sredstvo poveljevanja in nadzora koordinacije ter možnosti integriranega napada (Thomas, 2003).

[36] Informacijski terorizem na pozna fizičnih meja kot so: kontrolne točke, državne meje ipd (Thomas, 2002)

5.5 Psihološko bojevanje kot orožje teroristov

5.5.1 Propaganda in objavljanje

Poskus vplivanja na človeka v konfliktih je že stara tehnika, spremenila so se le sredstva. Sredstva propagande oz. mediji, ki jih uporabljajo propagandisti, so lahko zelo različni[37]. V zadnjem času pa je zelo velik pomen pridobila uporaba IKT, predvsem interneta.

Teroristi uporabljajo propagando za vpliv na javno mnenje, za pridobivanja novih članov, za pridobivanje podpore ter oblikovanje javnega mnenja. Pridobivanje pozornosti medijev in s tem širjenje propagande, je zelo pomembna komponenta strategije teroristov. Teroristi pozornost medijev pogosto privabljajo s pomočjo nasilnih dejanj (t. i. oborožena propaganda) in samomorilskih akcij (Forsnet, 2000).

Danes poleg tradicionalnih medijev (televizija, radijo, tisk ipd.) internet ponuja teroristom alternativno pot za doseganje javnosti, saj razprostira možnosti objavljanja in izpostavljanja brez omejitev, ki jih imajo zgoraj omenjeni mediji.

Teroristi so skozi zgodovino zelo izpopolnili tehnike pridobivanja medijske pozornosti. Nekatere teroristične organizacije (npr. Hizbollah, PKK) so pridobile lastne televizijske in radijske postaje.

Teroristična organizacija PKK daje propagandi velik poudarek vse od nastanka organizacije pa do danes. Sprva je PKK ustanovila neka lažna krila ali fronatalne (čelne) organizacije, z namenom zavarovati njihovo propagando in operacijske sposobnosti. Za propagandno dejavnost je skrbelo politično krilo PKK-ja ERNK (orig. Eniya Rizgariya Netewa Kurdistan), ki je manipulirala in vodila različne frontalne organizacije, pod pretvezo da so to socio-kulturna združenja (Kurdski odbori) in t. i. informacijski centri. Vendar so te institucije zagotavljale politično, moralno, materialno ter finančno podporo, ki je bila nepogrešljiva za preživetje PKK (ATAA[38], dostopno na: http://www.ataa.org/ataa/ref/pkk/mfa/report-pkk-terrorism.html). Tudi današnja struktura organizacije ima poseben komite (Tiskovni komite), ki je namenjen propagandni dejavnosti v Kurdistanu in izven njega (http://www.kongra-gel.com/).

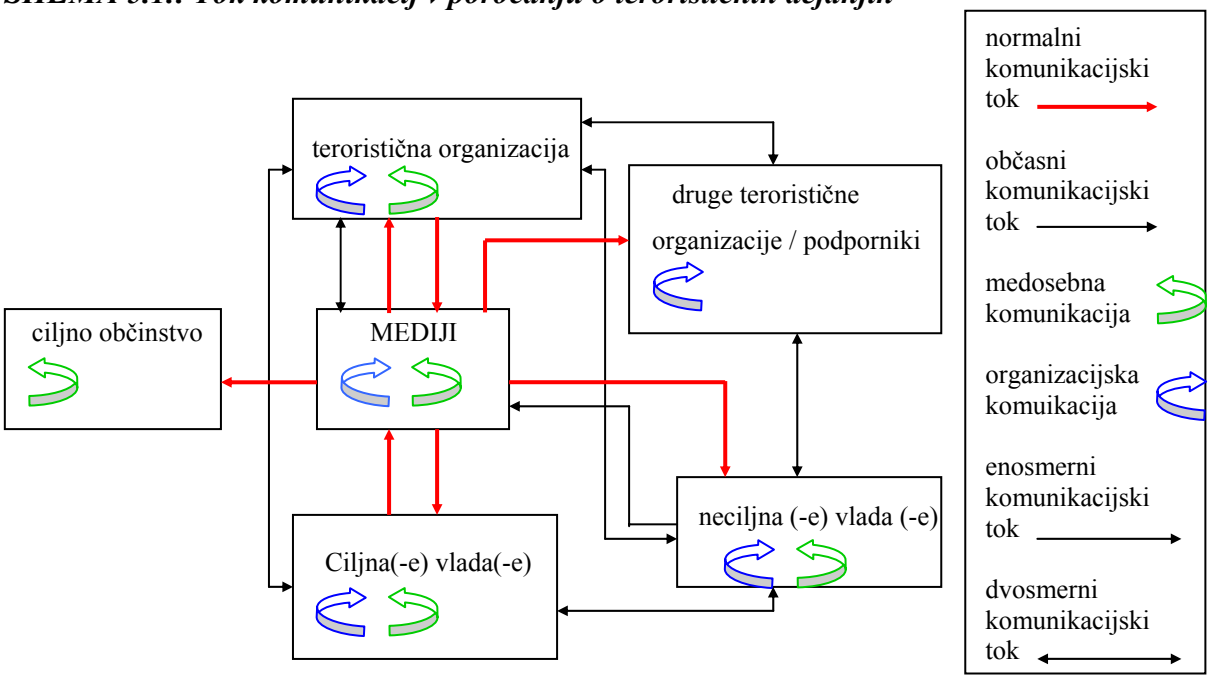
[37] Krunić (1997: 94–101) v Strategiji posrednega nastopanja našteva naslednje medije oz. sredstva propagande: množični mediji (tisk, radio, film, televizija), letaki, govorice, "face-to-face" propaganda ter druga sredstva (kot so pisemske pošiljke, telefon, razglasi, videokasete, plakati idr.).
[38] Assembly of Turkish American Association, Združenje za turško ameriško povezovanje.

5.5.1.1 Vloga medijev v psihološkem bojevanju PKK-ja

Mediji predstavljajo informacijsko-komunikacijsko infrastrukturo, s katero informacijski izvajalci komunicirajo z zunanjo in notranjo javnostjo (televizija, radio, tiskani mediji ...). Medijski vidik delovanja informacijskega bojevanja Omaljev označuje tudi s pojmom »medijska vojna«, s kater razume »vse akcije in ukrepe preko medijev, ki pri ljudeh formirajo nova ali spremenijo stara stališča, mišljenja, občutke, opredelitve in postopke, ali zaščitijo obstoječe vrednote, odnose in akcije« (Omaljev, 2001: 108).

Mediji sporočilo o terorističnem dejanju prenesejo širokemu krogu občinstva. Shema 5.1 prikazuje tok komunikacij v poročanju o terorističnih dejanjih.

SHEMA 5.1.: Tok komunikacij v poročanju o terorističnih dejanjih



Vir: Picard, Robert G. (1993): *Media Portayals of Terrorism: Functions and Meaning of News Coverage*, str: 35, Iowa State University Press, Ames.

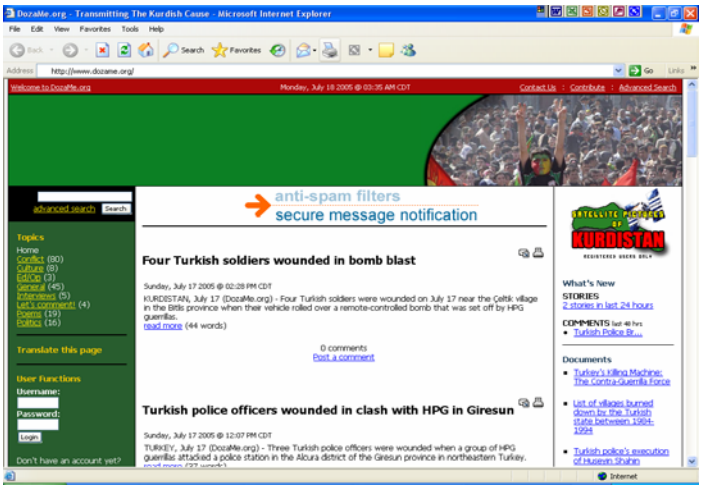
PKK je pred sklenitvijo premirja za propagandne namene izkoriščala zelo različne medije. Po podatkih Forsneta, naj bi takrat organizacija imela 28 različnih publikacij, 17 radijskih postaj, ki so oddajale v 11 različnih jezikih, 1 televizijsko postajo ter 700–750 propagandnega osebja (Forsnet, 2000).

Nekateri zgoraj omenjeni mediji so bili zakoniti, precej pa je bilo nezakonitih. Prek teh medijev je PKK komunicirala s svojimi bojevniki, širila propagando ter pridobivala nove rekrute. Zaradi sklenitve enostranskega premirja je bilo večina teh medijev ukinjenih.

Vseskozi pa so se pojavljali novi, sodobnejši mediji. Tu imam v mislih predvsem pojavljanje različnih spletnih strani povezanih s teroristično organizacijo.

Danes večina informacij v svetovnih medijih o Kurdski delavski stranki izhaja iz kurdskih in turških poročevalskih agencij, kot so: DIHA (orig. Dicle Haber Ajansi, ang. Dicle News Agency), MHA (orig. Mezopotamya Haber Ajansı, ang. Mesopotamia News Agency) ter DM (orig. Denge Mesopotamya). Prva ponuja informacije v angleškem, kurdskem in turškem jeziku prek interneta, na naslovu http://www.diclehaber.com/. DIHA ima urade v Istanbulu, Ankari, Izmiru, Diyarbakiru in Vanu. Spletni strani MHA (http://www.mhanews.com/) in DA (http://www.denge-mezopotamya.com/) pa sta samo v kurdskem jeziku (Kurdish info, 2005). Pomembno vlogo pri širjenju informacij v zvezi s PKK imata tudi svetovni poročevalski agenciji AFP (Agence France-Presse) in Reuters. AFP je svetovno omrežje, ki se razteza prek 165 držav. Eden izmed glavnih birojev AFP je tudi v Turčiji (v Ankari) (http://www.afp.com/english/), Reuters pa deluje v 94 državah, v katerih ima 197 birojev (http://www.reuters.com/).

SLIKA 5.3: Spletna stran http://www.dozame.org/



Vir: http://www.dozame.org/ (18.julij 2005)

Obstaja pa tudi pro-PKK usmerjen spletni medijski portal Doza me, na naslovu http://www.dozame.org/ (glej sliko 5.3), ki ponuja aktualne informacije v angleškem jeziku. Največ pozornosti je namenjene konfliktom med vojaškim krilom Kongra-Gel, HPG (Ljudske obrambne sile), TAK (Svobodni sokoli Kurdistana) in turškimi varnostnimi silami. Na tej spletni strani so objavljene tudi različne vojne bilance, npr. bilanca HPG od julija 2004 do maja 2005 (glej prilogo C), bilanca turške vojske od 1984 do 1999, kot tudi posamezne

mesečne bilance HPG. Poročila HPG izpostavljajo predvsem število žrtev na turški strani, saj naj bi bilo po teh podatkih, od julija 2004 do maja 2005, na turški strani skupno 718 žrtev, med pripadniki HPG pa »samo« 96. Stran ponuja informacije tudi s področja kulture, politike, poezije itd. (http://www.dozame.org/).

Tiskani mediji

Kot sem že omenila, je PKK pred sklenitvijo premirja izdajala 28 različnih publikacij. Glede na to, da obstaja kar precej kurdskih tiskanih medijev (glej prilogo D, v kateri so prikazani turški in kurdski mediji), ima PKK verjetno vpliv na nekatere izmed njih. Organizacija ima verjetno tudi sedaj v lasti katerega izmed tiskanih medijev, vendar je težko ugotoviti, kateri so to, ker je bil kurdski jezik do nedavnega v Turčiji prepovedan in je zato veliko tiskanih medijev nezakonitih in izhajajo precej prikrito ali pa vpliv organizacije ni tako očiten.

Kljub vsemu pa lahko najdemo nekaj publikacij, ki izhajajo pod vplivom privržencev PKK-ja. Taka publikacija je Serxwebûn (kar v prevodu pomeni Neodvisnost), ki je uradna ideološka revija PKK-ja. Serxwebûn izhaja v Nemčiji, v kurdskem in turškem jeziku, dostopen pa je tudi na spletu, na naslovu http://www.serxwebun.org/ (glej prilogo E). Pod vplivom privržencev PKK, naj bi bila tudi uradna revija združenja žensk Jina Serbilind, ki ima tudi spletni dostop (http://www.jinaserbildin.com/). PKK naj bi imela vpliv tudi na Özgurpolitiko (http://www.ozgurpolitika.org/) – najpopularnejši časopis v turškem jeziku, ki piše o kurdskih zadevah (Kurdish info, 2005). Tudi vojaško krilo organizacije (HPG) izdaja dva glasila v kurdskem jeziku: Star (http://star.hpg-online.com/) in Parastina Gel (http://parastinagel.hpg-online.com/).

O PKK-ju pa poročajo tudi drugi tiskani mediji. Da bi ugotovila, kako pogosto se pojavlja PKK v turških in tudi drugih tiskanih medijih, sem analizirala poročanje tiskanih medijev o teroristični organizaciji. Preučevala sem obdobje od začetka januarja 2004 do konca maja 2005. V analizo sem vključila slovenske, turške in nemške tiskane medije. Nemške in turške medije sem analizirala prek spletnega dostopa, pri slovenskih pa sem poleg spleta uporabila tudi dokumentacijo Dela. Kurdskih tiskanih medijev nisem mogla analizirati, ker jih je večina dostopnih le v kurdskem jeziku ali pa nimajo spletnega dostopa. Od slovenskih medijev sem vključila Delo (http://www.delo.si/), Dnevnik (http://www.dnevnik.si/) in Večer (http://www.vecer.si/). Iz množice nemškega tiska[39] sem se odločila, da analiziram tri velike nacionalne

[39] Po podatkih Goethe inštituta ima Nemčija blizu 400 resnih dnevnih časopisov, ki so imeli v letu 2002 skupno prodajo blizu 30 milijonov izvodov (Rainer, 2005).

časopise in tako izbrala: die Welt[40] (dnevno prodanih izvodov v prvi četrtini leta 2003: 250.000) Frankfurter Rundschau[41] (185.000) in Suddeutsche Zeitung[42] (430.000) (Rainer, 2005). Turški časopis v angleškem jeziku z največjo naklado je Turkish Daily News, vendar spletni arhiv tega dnevnika ne obsega celotnega preučevanega obdobja. Zato sem od turških tiskanih medijev pod drobnogled vzela tri časopise, ki imajo prost spletni dostop, dovolj obsežen arhiv in so na voljo v angleškem jeziku. Ti mediji so: Zaman (http://www.zaman.com/), ki izhaja v Carigradu in zajema izčrpne nacionalne novice, Turk. US (http://www.turk.us/), ki črpa turške novice iz različnih virov ter Turkish Press (http://www.turkishpresss.com/), ki vključuje dnevne novice in pregled turških medijev, sestavlja pa ga urad predsednika vlade.

Analizo poročanja tiskanih medijev o teroristični organizaciji PKK sem osredotočila predvsem na naslednje indikatorje:

- **Prekinitev enostranskega premirja** PKK s turško državo (1. junija 2004). PKK je po 5 letih prekinila enostransko premirje s turško državo ter zagrozila z napadi na turistično industrijo in infrastrukturo.
- **Poročanje o napadih Kurdske delavske stranke, konfliktih med PKK in turškimi varnostnimi silami ter o aretacijah pripadnikov PKK.**
- Članki o **A. Öcalanu**, ustanovitelju in bivšemu voditelju PKK.

PKK se v izbranem tisku skozi celotno preučevano obdobje večkrat omenja, predvsem v kontekstu turških prizadevanj za vstop v Evropsko unijo. PKK je velikokrat aktualna tema tudi v zvezi z vojno v Iraku, ker naj bi se večina njenih bojevnikov skrivala v Severnem Iraku ter obljubo ZDA, da bo pomagala Turčiji opraviti s to teroristično organizacijo. V Turških medijih se konec leta 2004 in v začetku 2005 PKK velikokrat omenja v povezavi s problematiko naftno bogatega mesta Kirkuk[43]. Turška oblast se boji, da bi si Kurdi prilastili naftne centre, kar bi jim omogočilo finančno neodvisnost. V takih člankih je PKK samo omenjena in ni poudarek na njej, ampak na drugih temah. Tako da v teh člankih ne moremo govoriti o kakšni propagandni dejavnosti PKK, kvečjemu o propagandi Turčije proti PKK.

Tuji tiskani mediji (slovenski in nemški) v obdobju od januarja do junija 2004 ne poročajo o kakršnihkoli napadih oz. spopadih s turškimi varnostnimi silami. Turški tisk pa skozi celotno omenjeno obdobje poroča o različnih incidentih. V začetku junija vsi preučevani mediji

[40] http://www.welt.de/
[41] http://www.fr-aktuelle.de/
[42] http://www.suddeutsche.de/
[43] Tu se nahaja 6% svetovne rezerve nafte (Singh, 2004).

množično poročajo o prekinitvi premirja s turško državo ter grožnji PKK-ja, da bo napadla turistično industrijo in infrastrukturo. Po 1. juniju 2004 se število člankov o PKK znatno poveča, zaradi vse bolj pogostih incidentov. V tujih medijih se pojavljajo predvsem bolj odmevni incidenti, kot je bil neuspešen julijski (2. julija 2004) atentat na guvernerja province Van[44] ter bombni napad na dva hotela v Carigradu ter plinski kompleks (10. avgusta 2004)[45].

Po prekinitvi premirja pa do konca maja 2005 turški tisk, poleg zgornjih dveh napadov, poroča še o številnih drugih incidentih in napadih, ne samo v Turčiji, pač pa tudi v sosednjih državah. Veliko je govora o t. i. turškem »lovu na teroriste«. Turški tisk tudi vseskozi poroča o žrtvah tako med turškimi vojaki in pripadniki varnostnih sil kot med teroristi, vendar bolj poudarja število žrtev med teroristi. Če bi sešteli številke, ki jih navaja turški tisk, pridemo do zaključka, da je bilo več žrtev med teroristi. Situacija pa je ravno obratna, to je večje število žrtev med pripadniki turških varnostnih sil, če pogledamo bilanco vojne, ki jo je objavil HPG na spletni strani pro-PKK poročevalske agencije Doza me. Turški tisk poroča tudi o številnih aretacijah pripadnikov PKK doma in po svetu. Najbolj obsežna (glede na število ujetih teroristov) in hkrati najbolj odmevna racija v preučevanem obdobju je bila na Nizozemskem – o tem pišejo tudi slovenski in nemški tiskani mediji. Nizozemska protiteroristična policija je vdrla v kamp za urjenje borcev PKK in aretirala 29 oseb, starih od 18 do 23 let, od tega pet žensk.

Članki o A. Öcalanu govorijo predvsem o prizivnem postopku, ki je potekal na Evropskem sodišču za človekove pravice v Strasbourg-u proti turški državi, ki ji Öcalanovi odvetniki očitajo številne kršitve človekovih pravic tako ob aretaciji kot tudi v sodnem postopku. Tako vsi preučevani mediji junija 2004 pišejo o začetku tega postopka. Maja 2005 pa poročajo o odločitvi tega sodišča, ki sicer ni zavezujoča, da je bilo sojenje kurdskemu voditelju nepravično. Turški mediji poleg poročaja o sojenju, pišejo tudi o različnih Öcalanovih izjavah v zvezi s politiko in PKK. Turški tisk ne poroča o zdravju in počutju Öcalana ter razmerah v zaporu, ki naj bi bile po poročanju kurdskih spletnih medijskih portalov, kot sta Kurdistan Observer in Kurdish Media, zelo slabe.

[44] Ob eksploziji avtomobila bombe je bilo ubitih pet mimoidočih ter 24 ranjenih. Guverner Hikmed Tan ni bil ranjen. Turške oblasti so za napad obsodile PKK, čeprav je le-ta na spletnih straneh zanikala odgovornost.

[45] Napad na hotela je terjal dve smrtni žrtvi, ranjenih je bilo 7 ljudi. Na plinskem kompleksu je nastala gmotna škoda, žrtev pa ni bilo. Odgovornost za napad sta prevzeli dve teroristični organizaciji: do sedaj neznana skupina Sokoli za svobodo Kurdistana (TAK, ang. Kurdistan's Freedom Falcons) ter Brigade mudžahedinov Abu Hafs al Masri, ki naj bi bila povezana z Al Kaido. Vendar so turške oblasti dvomile v verodostojnost teh izjav in napad pripisale Kurdski delavski stranki, ki je na domači spletni strani Ljudskih obrambnih sil zanikala obtožbe.

V vseh izbranih medijih lahko zasledimo t. i. »oboroženo propagadno«, pri kateri skušajo teroristi z uporabo nasilja doseči pozornost medijev in s tem širši javni odmev dejanj. Tuji mediji (slovenski in nemški) poročajo predvsem o večjih napadih (Carigrad in Van), ki so povzročili škodo na civilnih objektih in so terjali predvsem civilne žrtve, medtem ko turški mediji poročajo o številnih napadih, spopadih med vojsko in PKK in tudi poskusih napadov. V turških medijih je tudi veliko poročanja o žrtvah, tako med vojaki kot teroristi, s poudarkom predvsem na žrtvah med teroristi.

Tuji mediji PKK omenjajo le ob večjih svetovno bolj odmevnih dogodkih, medtem ko je v turških skoraj vsakdanja tema.

Neposreden prenos (radio in televizija)

Radio je danes eno najbolj razširjenih sredstev. Uporaba radia kot propagandnega sredstva je bila uveljavljena med drugo svetovno vojno. Možnosti uporabe radia v propagandne namene se v današnjem času vseskozi izboljšujejo, na kar vpliva nenehno izboljševanje tehnik za reprodukcijo zvoka ipd. Poleg tega nekateri ameriški raziskovalci opozarjajo, da sodobni človek zelo veliko časa preživi v avtomobilu in da je nanj možno vplivati predvsem prek radia (Krunić, 1997).

PKK je imela pred sklenitvijo premirja leta 1999 v lasti 17 radijskih postaj, ki so oddajale v enajstih različnih jezikih. Današnja naslednica Kongra-Gel naj bi bila po nekaterih podatkih upravljala radijsko postajo Voice of Mesopotamya. Ta radijska postaja se uradno predstavlja kot »neodvisna komercialna radijska postaja«, ki naj ne bi bila pod vplivom nobene politične stranke. Sedež postaje je v Moldovi in Uzbekistanu, leta 2001 ob odprtju postaje pa je delovala tudi v Armeniji in Rusiji. Voice of Mesopotamya oddaja v angleščini in treh kurdskih dialektih (Kurmanci, Zazaki in Sorani). Voice of Mesopotamya za razliko od drugih kurdskih radijskih postaj, ki oddajajo lokalno, oddaja iz Evrope prek kratkih valov, satelita in interneta (http://www.clandestineradio.com/).

Kongra-Gel naj bi imela vpliv tudi na radijsko postajo Denge Mesopotamya, ki oddaja v kurdskem jeziku in ima sedež v Belgiji. Denge Mesopotamia ima tudi svojo spletno stran v kurdskem jeziku na naslovu http://www.denge-mezopotamya.com/.

PKK je za propagandne namene ustanovila leta 1995 tudi svojo TV postajo MED TV, ki je bila hkrati tudi prva mednarodna kurdska televizijska postaja. Zaradi nasilnih in popačenih oddaj je EU, 22. marca 1999, zaprla MED TV (http://www.med-tv.com/) Po zaprtju MED TV

je število terorističnih napadov v Turčiji začelo upadati. Kmalu po zaprtju MED TV se je pojavila nova televizijska postaja CTV (Krščanska TV). Administrativni center CTV-ja je bil v Nemčiji, finančno podporo je dajal Vatikan, licenco pa je izdala Velika Britanija. CTV je oddajala iz Giblartara (Forsnet, 2000).

30. julija 1999 je pričela z delovanjem še ena TV postaja pod okriljam PKK – Medya TV. Leta je uporabljala isti satelit kot CTV, Eutesat-Hot Bird. Vodili so jo isti producenti in napovedovalci, ki so bili pred tem na MED TV (Forsnet, 2000). Medya TV je bila komercialni kurdski satelitski televizijski kanal, s sedežem v Parizu, namenjen kurdskemu prebivalstvu v Kurdistanu in po svetu. Medya TV je oddajala v vseh pomembnejših kurdskih dialektih (Kurmanci, Sorani, Zazaki in Luri), turškem ter arabskem jeziku. Francoske oblasti so televizijski postaji preklicale licenco ter jo 13. februarja 2004 zaprle (Kurdistan Observer, 2004). Še vedno pa obstaja spletno stran[46] v kurdskem, angleškem, francoskem in turškem jeziku (http://www.medyatv.com/).

Po zaprtju Medya TV, je prvega marca 2004 začela delovati Roj TV, s sedežem na Danskem (Kopenhagen). Roj TV oddaja v treh pomembnejših kurdskih dialektih, kot tudi v asirskem, arabskem in turškem jeziku. Potencialno občinstvo Roj TV obsega okoli 40 milijonov Kurdov po svetu (glej prilogo F). Roj TV prek satelita doseže okoli 28 milijonov Kurdov v 77 državah v Srednjem Vzhodu, Evropi[47] in severni Afriki. Roj TV ima tudi svojo spletno stran – http://www.roj.tv/ (glej prilogo G) v angleškem, nemškem, francoskem, danskem, nizozemskem, turškem in kurdskem jeziku, kjer je možen tudi ogled programov. Danska radiotelevizijska uprava je prejela že več pritožb glede Roj TV[48].

Internet kot orodje psihološkega bojevanja

Najpomembnejša osnova informacijske družbe je digitalizacija. Medtem ko so se včasih za prenos in shranjevanje informacij uporabljali materialni nosilci in analogne tehnike, je danes večina področij informacij digitalnih[49]. Na digitalni tehniki temelječa računalniška omrežja tako predstavljajo medij, ki je sposoben združiti vse dosedanje komunikacijske in

[46] http://www.medyatv.com (4. april 2005).
[47] V Evropi živi okoli dva milijona Kurdov, od tega 800.000 samo v Nemčiji (http://www.roj.tv/).
[48] Na primer, aprila 2005 je ta uprava prejela pritožbo Turške ambasade v Kopenhagnu, da Roj TV s programi v podporo PKK-ju spodbuja sovraštvo in strah med ljudmi in s tem krši tretji odstavek enajstega članka Izvršilne odredbe številka 1174 z dne 17. december 2002. Ta odstavek pravi »da programi ne smejo pod nobenim pogojem spodbujati sovraštva temelječega na rasi, spolu, veri, narodnosti ali seksualni usmerjenosti«. Uprava je odločila, da Roj TV ni kršila tega odstavka (EPRA, 2004).
[49] Digitalizacija pomeni razčlenitev informacij v najenostavnejše elementarne dele, pri čemer ni pomembno ali gre za govor , pisavo, tonske zapise, slike, grafike ali video (Svete, 2005).

informacijske medije ter jih hkrati še izpopolniti s funkcionalnimi zmogljivostmi (Svete, 2005).

Psihološko bojevanje prek interneta lahko teroristi izvajajo na več načinov. Na primer internet lahko uporabijo za širjenje napačnih informacij, da razširijo grožnje namenjene povzročanju strahu in nemoči ter raztrosenju strašnih predstav o nedavnih akcijah (Weimann, 2004).

Internet predstavlja za teroriste idealno propagandno orodje. Ker omogoča besedno, zvočno in slikovno komunikacijo, lahko služi kot tiskani medij, radijska postaja ali televizijsko omrežje. V preteklosti so teroristi komunicirali prek nasilnih dejanj ter so upali, da bodo ta dejanja pritegnila zadostno medijsko pozornost ter s tem dosegla širši javni odmev. Danes to ni več potrebno, saj internet omogoča terorističnim organizacijam, da širijo svoja sporočila neodvisno od medijev in brez vpliva oblasti. Zato je danes internet eden najbolj uporabljenih medijev s strani terorističnih organizacij. Internet tako vse bolj nadomešča tradicionalna sredstva za širjenje propagande. Pri tem teroristi uporabljajo vse storitve, npr. za medsebojno komunikacijo lahko uporabljajo elektronsko pošto, različne forume, klepetalnice ipd. Na tem mestu je potrebno še posebej poudariti IRC oz. klepetalnice, ki so edina storitev interneta, kjer je omogočeno neposredno komuniciranje med točno določenimi uporabniki v realnem času. Ne glede na to, da ima ta storitev bistveno manjši domet kot npr. svetovni splet, pa teroristom omogoča neposredno povezavo in navezavo stikov s potencialnimi novimi člani (Svete, 2005). Do danes so si vse aktivne teroristične organizacije zagotovile prisotnost na internetu (glej prilogo H, v kateri so podatki iz leta 2002 in 2005), kar je bilo še pred nekaj leti prava redkost. Inštitut za mir ZDA (ang. United States Institute of Peace) je leta 2003 izvedel pregled interneta in odkril na stotine spletnih strani namenjenih terorističnim organizacijam in njihovim privržencem. Za teroristične spletne strani je značilna velika dinamika: spletne strani se nanadoma 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. Kakšna je vsebina terorističnih spletnih strani? Navadno na takšnih spletnih straneh najdemo zgodovino organizacije, aktivnosti, 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 oz. sovražna publika (Weimann, 2004).

Za teroristično organizacijo PKK lahko rečem, da kar dobro sledi razvoju IKT. Pokazatelj prisotnosti PKK na svetovnem spletu je prav gotovo pogostost pojavljanja PKK na svetovnem

spletu[50] (gledala sem število zadetkov v posameznem izbranem iskalniku, ob različnih ključnih besedah). Za to analizo sem izbrala naslednje štiri iskalnike: Yahoo, Google, AltaVista in MSN. Preverjala sem tudi različna poimenovanja organizacije. Rezultate analize predstavlja tabela 5.2. Največ zadetkov dobimo, če v iskalnike vpisujemo kratice različnih poimenovanj organizacije, PKK, KADEK, KGK, vendar s tem dobimo veliko »napačnih« zadetkov, ki nimajo nikakršne povezave z našo organizacijo. Zato sem kriterij iskanja skušala izboljšati z dodajanjem besed »Kurds« (Kurdi) in »terrorism« (terorizem), kar privede do manjšega števila zadetkov, ki pa so bolj relevantni. Veliko število zadetkov dobimo tudi če vpišemo angleško poimenovanje organizacije (Kurdistan Workers Party) ter poimenovanje Kongra-Gel.

TABELA 5.2: Pogostost pojavljanja PKK na svetovnem spletu

Spletni iskalnik / Ključne besede	Google	Yahoo	AltaVista	MSN
PKK	751.000	776.000	779.000	1.810.120
PKK+Kurds	67.200	83.300	82.400	95
PKK+terrorism	80.900	78.000	77.800	1.372
»Partya Karkerên Kurdistan«	0	0	0	0
»Kurdistan Worker's Party«	549	1.170	1.170	905
»Kurdistan Workers Party«	53.300	70.800	70.900	16.617
»Kurdska delavska stranka«	22	3	3	1
»Delavska stranka Kurdistana«	6	6	6	0
KADEK	81.000	61.000	61.000	1.256.279
KADEK+Kurds	4.670	6.010	6.040	2
KADEK+terrorism	4.600	3.270	3.290	16
»Freedom and Democracy Congress of Kurdistan«	170	116	116	205
»Kurdistan Freedom and Democracy Congress«	607	881	881	900
KGK	211.000	118.000	118.000	62.543
KGK+Kurds	98	85	88	0
KGK+terrorism	222	105	107	0
»Kongra-Gel«	48.000	40.400	40.200	17.735
»People's Congress of Kurdistan«	255	558	560	460

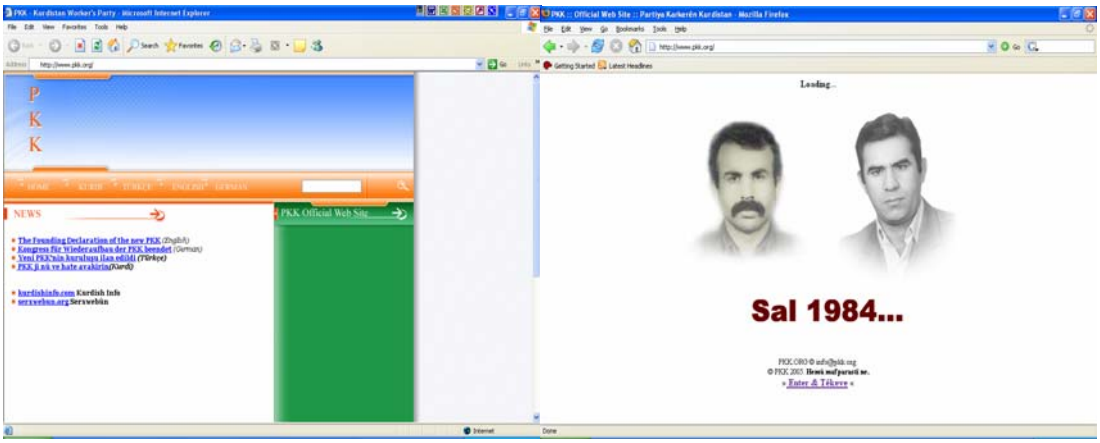
Vir: http://www.google.com/, http://www.yahoo.com/, http://www.altavista.com/, http://www.msn.com/ (7. april 2005)

Spletnih strani, ki jih lahko povežemo s Kurdsko delavsko stranko, je veliko, vendar je analiza teh strani zapletena, saj je resničnost podatkov zaradi že omenjene dinamike

[50] Podatke sem pridobila 7. aprila 2005

terorističnih spletnih strani zelo kratkotrajna. Za primer lahko navedem domačo spletno stran organizacije PKK (glej sliko 5.4). Spletne strani z naslovom http://www.pkk.org/ se je ob koncu leta 2004 posluževala Mednarodna pobuda svoboda za A. Ocalana – mir v Kurdistanu, ki se je pozneje preselila na drug spletni naslov. V začetku leta 2005, po kongresu o ustanovitvi nove PKK, se je na istem naslovu ponovno pojavila prenovljena spletna stran organizacije PKK, ki naj bi delovala v kurdski, turški, angleški in nemški različici. Ob mojem obisku (17. 05. 2005) je bila na njej le Ustanovna deklaracija »nove« PKK v vseh štirih zgoraj omenjenih jezikovnih različicah. Ta stran se je kmalu spremenila, saj je ob obisku strani (12. 07. 2005) delovala nova spletna stran v kurdskem jeziku.

SLIKA 5.4: Spletna stran http://www.pkk.org/



Vir: http://www.pkk.org/ (17. maj 2005 in 17. avgust 2005)

Na domačo stran organizacije pod imenom Kongra-Gel (http://www.kongra-gel.com/[51]), lahko vstopimo tudi prek spletnih naslovov: http://www.kongra-gel.net/ ter http://kongra-gel.org/. Spletna stran je na voljo v kurdskem, turškem, angleškem in nemškem jeziku. Na njej najdemo: ustanovno listino organizacije[52], program organizacije, apel za mir v Kurdistanu, pravila vodenja bojevanje ter vsakodnevne novice povezane z organizacijo in Kurdi (http://www.kongra-gel.com/).

[51] Stran sem obiskala 11. julija 2005.
[52] Ta listina je bila izdana 25. julija 2004, potem ko je organizacija spremenila ime v Kongra-Gel. Na začetku so podana splošna pravila, ki se tičejo imena organizacije in ciljev, nato so navdena pravila v zvezi s članstvom v organizaciji, sledi struktura organizacije ter funkcije organizacije, na koncu pa so opredeljeni disciplinski postopki (http://www.kongra-gel.com/).

SLIKA 5.5: Domača spletna stran Kongra-Gel

Vir: http://www.kongra-gel.com/ (11. julij 2005)

Svojo spletno stran (http://www.hpg-online.com/[53]) ima tudi vojaško krilo Kongra-Gel, Ljudske obrambne sile (HPG – Hêzên Parastina Gel). To stran si je možno ogledati v turškem ali kurdskem jeziku. Obstajata pa tudi angleško-nemška različica na naslovu http://www.hazenparastine.com/[54], vendar le-ta ne ponuja vseh vsebin, ki se nahajajo na turški in kurdski spletni strani. Ta spletna stran je precej propagandno naravnana. Tu se nahaja preveden izvleček izjave o odpovedi premirja Ljudskih obrambnih sil z dne 1. junija 2004, ki vsebuje opozorilo turistom in investitorjem, ki želijo vlagati v Turčijo. Predstavljena je tudi fotogalerija s posnetki urjenja pripadnikov HPG. Na tej strani HPG zanika (že omenjene) obtožbe medijev in oblasti, da je izvedla (neuspešen) atentat na guvernerja province Van ter avgustovski bombni napad na Carigrajska hotela in plinski kompleks.

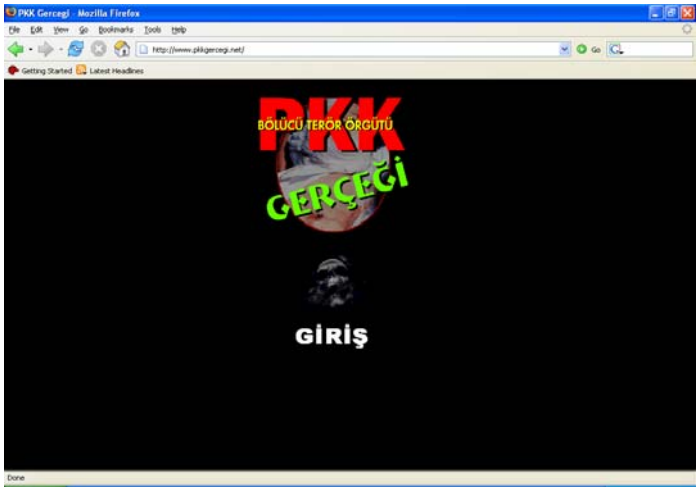
[53] Stran sem obiskala 17. maja 2005.
[54] Stran sem obiskala 13. maja 2005.

SLIKA 5.6: Domači spletni strani HPG kurdsko-turška (levo) in angleško-nemška različica (desno)

Vir: http://www.hpg-online.com/ (17. maj 2005), http://www.hezenparastine.com/index.php (13. maj 2005)

Preko spletnega naslova http://pkkgercegi.net/[55] lahko tudi vstopimo na eno izmed strani v lasti privržencev PKK (http://www.pkkgercegi.net/eski_gundem). Na njej je precej slikovnega materiala s posnetki žrtev. Ob večkratnem obisku strani sem ugotovila, da je redno obnovljena, vendar na voljo le v kurdskem jeziku, zato je nisem podrobneje analizirala.

SLIKA5.7: Spletna stran http://www.pkkgercegi.net/

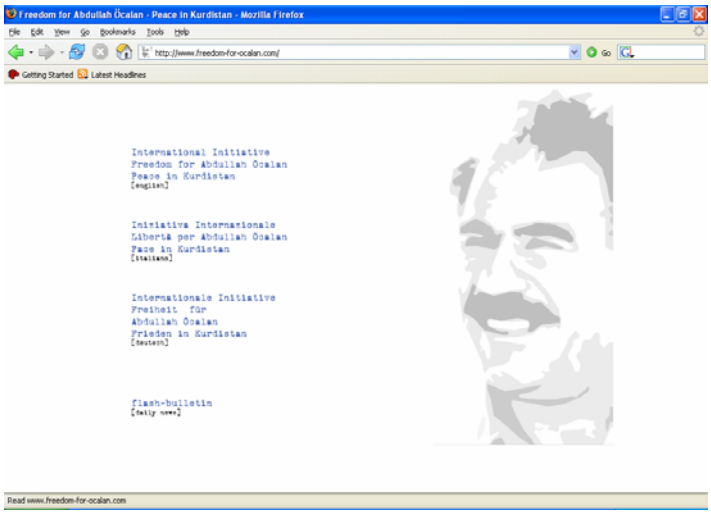


Vir: http://www.pkkgercegi.net/ (14. marec 2005)

[55] Stran sem obiskala 14. marca 2005.

Na spletu se nahajajo tudi strani, ki so posvečene nekdanjemu voditelju in ustanovitelju PKK A. Öcalanu. Spletno stran http://www.freedom-for-ocalan.com/[56] ureja Mednarodna pobuda Svoboda za A. Öcalan-a – mir v Kurdistanu (ang. International Initiative Freedom for A. Öcalan – Peace in Kurdistan, nem. Internationale Initiative freiheit für Abdullah Öcalan – Frieden in Kurdistan) s sedežem v Kolnu (v Nemčiji). Ta pobuda sodeluje z italijansko pobudo Svoboda za A. Öcalan-a – mir v Kurdistanu (Rim), Kampanjo za mir v Kurdistanu (London) ter organizacijo Asrin Hukuk Bürosu (Carigrad). Stran je na voljo v angleškem, nemškem in italijanskem jeziku. Na tej strani najdemo informacije in pojasnila o položaju A. Öcalan-a (zdravstveno stanje in splošno počutje). Tu se nahajajo različne peticije, ki jih lahko podpišejo posamezniki in organizacije. Prva na seznamu je peticija za svobodo A. Öcalan-a, temu pa sledijo različne peticije povezane s kurdskim vprašanjem. Ta pobuda ima tudi svoje spletno glasilo Flash bulletin. To glasilo zbira članke iz različnih turških, kurdskih in tudi svetovnih medijev, ki govorijo o Kurdih, Turčiji in PKK-ju.

SLIKA 5.8: Spletna stran http://www.freedom-for-ocalan.com/



Vir: http://www.freedom-for-ocalan.com/ (4. april 2005)

Informacije, o A. Öcalanu, v turškem jeziku, ponuja spletna stran http://www.abdullah-ocalan.com/[57]. Na tej strani najdemo veliko fotografij in posnetkov. Večina povezav na tej strani deluje samo v kurdskem in turškem jeziku.

[56] Stran sem obiskala 04. aprila 2005.
[57] Stran sem obiskala 04. aprila 2005.

SLIKA 5.9: Spletna stran http://www.abdullah-ocalan.com/

Vir: http://www.abdullah-ocalan.com/ (04. april 2005)

Svojo spletno stran ima tudi Doza me (http://www.dozame.org/) (glej sliko 5.3), pro-PKK usmerjena tiskovna agencija. Ta agencija je zelo pomembna pri širjenju propagande PKK-ja. Saj veliko drugih tiskovnih agencij in medijev uporablja njene informacije o organizaciji.

Pod vplivom privržencev PKK je tudi spletna stran http://www.rojaciwan.com/[58], ki jo oblikuje Združenje kurdske mladine. Prav tako tudi spletna stran http://www.tecakonline.com/, domača stran Združenja kurdske mladine na Švedskem. Ta stran ima za razliko od prejšnje poleg kurdske še angleško, nemško in turško jezikovno različico. Na obeh straneh se nahaja poleg resne vsebine npr. Ustanovna deklaracija nove PKK, veliko zabavne vsebine od glasbe, fotografij, klepetalnic, forumov ipd. Združenje TECAK ima še en forum na spletni strani http://www.kurd.se/forum/. Svoj forum pa ima tudi spletna stran ROJAME (http://www.rojame.com/[60]), še ena izmed strani privržencev PKK.

PKK podpirajo tudi nekatere druge organizacije, kot na primer Informacijska služba Kurdistan (ISKU) (http://www.nadir.org/nadir/initiativ/isku/[61]), ki ima sedež v Nemčiji (Berlin, Hamburg, Köln), Kurdski informacijski biro v Italiji (UIKI-Onlus, it. Ufficio

[58] Stran sem obiskala 12. julija 2005.
[59] Stran sem obiskala 18. julija 2005.
[60] Stran sem obiskala 18. julija 2005.
[61] Stran sem obiskala 12. julija 2005.

d'Informazione del Kurdistan in Italia) (http://www.uikionlus.com/[62]), žensko združenje CENI (http://www.ceni-kurdistan.de/) s sedežem v Düsseldorf-u, društvo AZADI (http://www.nadir.org/nadir/initiativ/azadi/), ki služi potrebam Kurdov v Nemčiji.

Neposredna komunikacija

Dejavnost teroristične organizacije PKK na svetovnem spletu sem poskušala ugotoviti tudi z analizo forumov in klepetalnic, ki so izredno pomembne pri medsebojni komunikaciji in povezovanju med teroristi ter navezavi stikov s potencialnimi novimi privrženci in donatorji. Vidimo, da ima organizacija forume in klepetalnice na svojih straneh oz. straneh različnih podpornikov organizacije (glej tabelo 5.3). Ti forumi in klepetalnice zagotovo pripomorejo k medsebojni komunikaciji in navezovanju stikov s potencialnimi novimi člani, saj omogočajo neposredno komunikacijo v realnem času. Nahajajo se predvsem na spletnih straneh, ki so namenjene mladim, verjetno z namenom pritegniti njihovo zanimanje za vključitev v organizacijo.

Poskušala sem tudi ugotoviti, ali se PKK poslužuje tudi drugih turških in kurdskih forumov in klepetalnic (glej tabelo 5.3), ki se nahajajo na različnih seznamih turških in kurdskih medijev. Pri tem sem naletela na problem, ker je večina teh forumov in klepetalnic v meni neznanih jezikih (kurdski, turški, nizozemski ipd.) Tako, da sem od forumov v spodnji tabeli analizirala le forum E Kurd, ki je v nemškem jeziku. Na tem forumu je PKK ena izmed tematik, vendar tu najdemo le argumente za in proti tej teroristični organizaciji. Med brskanjem po teh forumih pa sem na spletnem naslovu http://www.politik-forum.at/ zasledila proti PKK-ju naravnan forum v nemškem jeziku.

[62] Ta stran je ob mojem obisku 12. julija 2005 še delovala. Na njej so se nahajale fotografije A. Öcalan-a, informacije o Kurdistanu in gverilskem boju, ki poteka tam ipd. Dne 18. julija 2005 pa je bila spletna stran že zasežena s strani hekerjev, kar sem navedla kot primer v 4.4.2 poglavju (slika 4.1) pri hekerskem bojevanju.

TABELA 5.3: Forumi in klepetalnice

FORUMI IN KLEPETALNICE		
KURDSKI	**TURŠKI**	**NA SPLETNIH STRANEH POVEZANIH S PKK**
ekurd.de (http://www.ekurd.de/)	Balca (http://www.balca.net/)	TECAK Comunity (http://www.kurd.se/forum/default.asp)
Koerdistan Forum (http://www.koerdistan.nl/)	Dostum.net (http://www.dostum.net/)	ROJAME (http://www.rojame.com)
KURD IT GROUP on msn (http://www.groups.msn.com/ KURDITGROUP)	Fistik (http://www.fistik.com/index.htm/)	Rojaciwan (http://www.rojaciwan.com/modules. php?op=modload&name=eBoard)
Nawendi-kurd Forum (http://www.nawendi-kurd.com/)	Fikralar (http://www.fikralar.com/)	
Rebir.com (http://www.rebir.com/)	Hayalevi (http://www.hayalevi.com/)	
Rezgari.org (http://www.rezgari.org/)	HosmuBosmu (http.//www.	
Zana Forum (http://zana.conforums.com/)	Komikaze (http://www.komikaze.net)	
Denge Yezidiyan (http://www.yezidi.org/)	SesliChat	
Gelawej (http://www.gelawej.com/)	TurkChat (http://www.turkchat.com/)	
RojBas.nl (http://www.rojbas.nl/)	Turk Unluleri Arsivi (http://www.aysum.com/)	
Koma Welat (http://groups.msn.com/wealt/)		
Kurdistan forum (http://akha.4×2.net/)		
Kurdistan Chat (http://www.kurdistanchat.tk/)		
Yahoo chat (http://chat.yahoo.com/)		

Vir: http://www.kurdishpoint.com/, http://www.kurdistan4all.com, http://www.turkishmedia.net/ (28. julij 2005).

5.6 Terorizem in javno mnenje

Moja prva hipoteza pravi, da imajo teroristična dejanja z uporabo sodobne informacijsko-komunikacijske tehnologije vse večji učinek, tako v smislu doseganja ciljev, kot tudi vpliva na javno mnenje. Kot smo videli obstajajo štiri kategorije definicij javnega mnenja. Za mojo analizo se zdi najbolj primerno uporabiti agregatno pojmovanje javnega mnenja, po katerem je javno mnenje seštevek individualnih mnenj. Možno jih je seštevati in meriti na osnovi javnomnenjskih raziskav. Ena takšnih definicij se nahaja na spletni strani Dictationary.LaborLawTalk.com (http://encyclopedia.laborlawtalk.com/public_opinion). Ta definicija pravi, da je "javno mnenje skupek posameznih vedenj ali prepričanj odrasle populacije«. Na javno mnenje lahko vplivajo javni odnosi in politični mediji. Poleg tega pa množični mediji, ki uporabljajo širok spekter oglaševalskih tehnik, da razširijo svoje sporočilo in spremenijo mišljenje ljudi, igrajo ključno vlogo pri oblikovanju in odražanju javnega mnenja. Množični mediji sporočajo informacije posameznikom in ustvarjajo samopodobo moderne družbe.

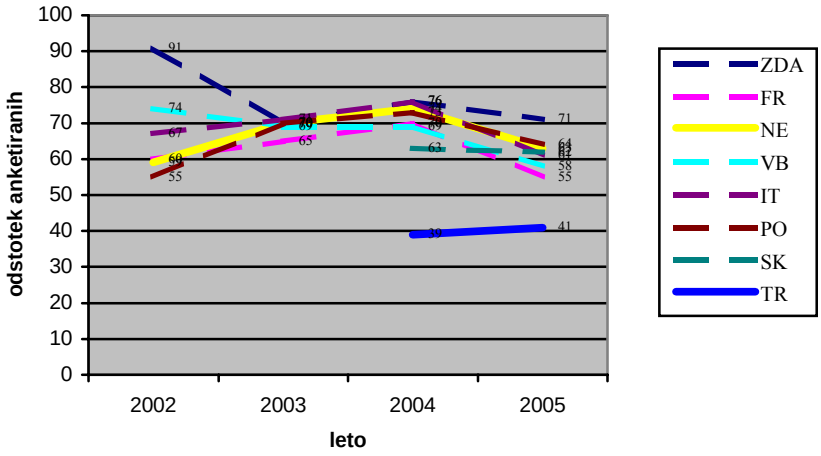
Drugi del prve hipoteze (... vse večji vpliv na javno mnenje ...) bom torej poskušala preveriti s pomočjo javnomnenjske raziskave Transatlantic Trends 2005, ki jo je izvedel German Marshall Found of the United States. Raziskava je potekala maja in junija 2005 v 10 evropskih državah in ZDA. Ankete so bile izvedene prek telefona, razen v Turčiji, na Poljskem in Slovaškem, kjer je raziskava temeljila na osebnem (face-to-face) anketiranju. Iz te raziskave sem izbrala Združene Države Amerika in nekaj evropskih držav: Velika Britanija, Francija, Italija, Nemčija, Slovaška, Poljska in Turčija[63]. Zanima me, ali terorizem ljudem predstavlja vedno večjo ali vse manjšo grožnjo. Med izbranimi državami sta tudi Turčija in Nemčija, v katerih sem preučevala poročanje medijev o PKK. Za Slovenijo pa bom uporabila podatke, ki sta jih pridobila, v raziskavi z naslovom Stališča o nacionalni in mednarodni varnosti[64], Obramboslovni raziskovalni center (ORC) ter Center za raziskovanje slovenskega javnega mnenja in množičnih komunikacij v okviru Fakultete za družbene vede. Podatke te raziskave sem pridobila iz časnika Večer (12. julij 2005) in spletne strani Slovenija – NATO.

Podatke za leta 2004, 2003 in 2002 sem pridobila iz rezultatov raziskave za leto 2005 (glej Transatlantic Trends, Topline Data, str. 17), kjer so prikazani tudi rezultati raziskav Transatlantic Trends 2004, Transatlantic Trends 2003 in Worldview 2002.

[63] Vzorec raziskave Transatlantic Trends 2005 je bil sledeč: ZDA 1000, Velika Britanija 1012, Francija 1005, Italija 1001, Slovaška 1018, Poljska 1000 in Turčija 1021 anketirancev (Transatlantic Trends 2005, 2005: 2).
[64] Raziskava je potekala od 17. marca do 25. aprila 2005 na reprezentativnem vzorcu 1594 ljudi, na vprašanja sta odgovarjala 1002 vprašana (Zgaga, 2005).

Eno izmed vprašanj v omenjeni raziskavi se je nanašalo tudi na terorizem, in sicer kako pomembno grožnjo varnosti, po mnenju anketiranih, predstavlja mednarodni terorizem. Možni odgovori so bili zelo pomembna grožnja, pomembna grožnja ali nepomembna grožnja. (celotne rezultate ankete prikazuje priloga I). Sedaj pa poglejmo odstotek anketiranih (graf 5.1), ki menijo, da terorizem predstavlja zelo pomembno grožnjo varnosti.

GRAF 5.1: Odstotki anketirancev po posameznih izbranih državah, ki menijo, da mednarodni terorizem predstavlja zelo nevarno grožnjo varnosti.



Vir: Transatlantic Trends, Topline Data (2005): 17

Če pogledamo najprej natančneje državi, v katerih sem preučevala zastopanost PKK v tiskanih medijih. Za Turčijo imamo podatke le za leti 2004 in 2005. V tem obdobju zaznavanje terorizma kot pomembne grožnje rahlo naraste. Kar je deloma posledica tudi prekinitve t. i. enostranskega premirja (1. 6. 2004) PKK s turško državo ter vrnitev k nasilnim dejanjem. Saj se je, glede na poročanje medijev, število terorističnih dejanj in incidentov med PKK in turško vojsko po tem datumu precej povečalo.

V Nemčiji pa podobno kot v večini preučevanih državah zaznavanje terorizma kot zelo pomembne grožnje do leta 2004 narašča, do leta 2005 pa upade.

Če pogledamo na tem mestu najprej še slovensko raziskavo. Slovenci se na splošno počutimo varne (82% vprašanih), le 9% anketirancev pa se počuti ogrožene. Med najpomembnejše grožnje nacionalni varnosti slovenska javnost uvršča nevojaške vire ogrožanja. Med njimi izstopajo viri, ki se nanašajo na notranjo varnost, degradacijo okolja in socialno-ekonomske vidike varnosti, na vrhu lestvice so brezposelnost, mamila, kriminal, majhna nataliteta ...

Terorizem in vojaško ogrožanje države pa se nahajata prav na dnu lestvice. Danes terorizem kot grožnjo zaznava nekaj več kot 20% vprašanih. Kar je, glede na raziskavo Transatlantic Trends 2005, precej manj kot v ostalih preučevanih državah (Zgaga, 2005).

Iz zgornjih raziskav vidimo, da se je zaznavanje terorizma, kot zelo pomembne grožnje od leta 2002 do leta 2004, v večini preučevanih držav povečevalo. Izjemi sta ZDA in Velika Britanija (ter Turčijo in Slovaška, za kateri do leta 2004 ni podatkov), ker od leta 2002 do 2003 zaznavanje terorizma kot zelo pomembne grožnje zmanjša, do leta 2004 pa zopet naraste. Velik odstotek anketirancev v ZDA in Veliki Britaniji, ki zaznavajo terorizem kot veliko grožnjo v letu 2002, je nedvomno posledica napada na ZDA 11. septembra 2001. V letu 2005 pa so odstotki približno enaki predhodnemu letu. V večini držav lahko opazimo celo rahel upad zaznavanja terorizma kot velikega dejavnika ogrožanja varnosti, z izjemo Turčije, kjer se odstotek rahlo poveča. Glede na podatke slovenske raziskave od večine odstopa tudi Slovenija, kjer se je strah pred terorizmom precej zmanjšal (glej tabelo 5.3), saj je leta 1999 terorizem kot grožnjo zaznavalo skoraj polovica vprašanih, danes le še petina.

TABELA 5.4: Primerjalni podatki povezani z odnosom slovenske javnosti do grožnje terorizma (vrednosti 1 do 4, pri čemer 1 pomeni nepomembno grožnjo, 4 pa zelo pomembno grožnjo).

leto	**1999**	**2001**	**2003**
terorizem	2,64	2,09	1,97

Vir: Slovenija – NATO (2002) Dostopno na http://nato.gov.si/slo/javno-mnenje/varnost/podatki-varnost/ (5. oktober 2005); ORC (2003) Dostopno tudi na http://nato.gov.si/slo/javno-mnenje/nacionalna-varnost.pdf (5. oktober 2005).

Na zaznavanje terorizma kot zelo pomembne grožnje varnosti prav gotovo vpliva več medsebojno povezanih in soodvisnih dejavnikov. Najpomebnejši dejavnik oblikovanja javnega mnenja so nedvomno množični mediji. To se najbolj jasno odrazi na primeru Poljske in Slovaške, v katerih od leta 2000 do 2004 ni bilo terorističnih incidentov (priloga J prikazuje število terorističnih incidentov v izbranih državah po podatkih MIPT), terorizem kot pomembno grožnjo varnosti pa zaznavajo podobno visoko kot druge države. Število terorističnih incidentov v lastni državi torej ne pogojuje nujno zaznavnja terorizma kot grožnje. Drugače pa je s Slovenijo, kjer prav tako ni bilo terorističnih napadov, terorizem pa je zaznan kot majhna grožnja varnosti.

6 SKLEP

Moja prva hipoteza pravi, da *imajo teroristična dejanja z uporabo sodobne IKT vse večji učinek, tako v smislu doseganja ciljev, kot tudi vpliva na javno mnenje*.

Sodobni terorizem ima politične, nacionalne, ideološke, verske, socialne, ekonomske in druge motive. Ti cilji vodijo k morilskemu nasilju, izsiljevanju, ugrabljanju ipd. Z namenom doseči željeni politični ali drug cilj, morajo teroristi najprej doseči pomemben vmesni cilj, ki je ustvarjanje negotovosti in bojazni med ciljno populacijo. V večini primerov teroristi nočejo smrt točno določene osebe, ampak želijo ustvariti strah in demoralizacijo v veliko širši populaciji kot v neposrednih žrtvah. Eden izmed teh vmesnih ciljev je torej tudi povzročanje žrtev, zato sem, ker je končne cilje (politične, ideološke in druge) težko dokazovati, naredila analizo žrtev terorističnih dejanj (priloga B). Glede na statistike (publikacije Patterns of Global Terrorism) lahko ugotovim, da je terorizem bolj ubojen, kljub današnjemu manjšemu številu napadov, kot v 80. in 90. letih prejšnjega stoletja. Takšno stališče imajo tudi nekateri teoretiki (npr. Bruce Hoffmann), ki se ukvarjajo s tem področjem. V tem smislu tudi lahko trdim, da ima terorizem vse večji vpliv v smislu doseganja ciljev, vendar se sedaj postavlja še vprašanje, kakšno vlogo pri tem igra IKT. Vse večja ubojnost terorizma, vsekakor ni le posledica uporabe sodobne IKT, k temu pripomore več dejavnikov, ki sem jih naštela v poglavju 4.1 Trendi v terorizmu. Kljub vsem tem dejavnikom, pa je ključni faktor pri naraščanju ubojnosti uporaba celotnega spektra tehnologij v teroristične namene. IKT, ki je sorazmerno poceni, lahko dostopna ter omogoča anonimnost pripomore k boljši, hitrejši in enostavnejši medsebojni komunikaciji, koordinaciji in organizaciji terorističnih aktivnosti.

Drugi del prve hipoteze *»da imajo teroristična dejanja z uporabo sodobne IKT vse večji vpliv ... na javno mnenje«* pa sem dokazovala v poglavju 4.6 Terorizem in javno mnenje. V tem poglavju sem predstavila izsledke iz raziskav Transatlantic Trends 2005, 2004 in 2003 in Worldview 2002, od koder sem povzela podatke za ZDA, Francijo, Nemčijo, Veliko Britanijo, Italijo, Poljsko, Slovaško in Turčijo. Kot sem že omenila, se je eno izmed vprašanj v teh raziskavah nanašalo na terorizem, in sicer, kako pomembno (zelo pomembno, pomembno ali nepomembno) grožnjo, po mnenju ljudi predstavlja mednarodni terorizem. Kakšnih starejših raziskav, da bi lahko predstavila bolj dolgoročen trend, pa nisem zasledila. Vendar tudi v tem kratkem obdobju lahko zaznamo neke kratkoročne trende. Za Slovenijo pa sem, kot sem že omenila, uporabila podatke, ki sta jih pridobila Obramboslovni raziskovalni center (ORC) ter Center za raziskovanje slovenskega javnega mnenja in množičnih

komunikacij v letih 1999, 2001 in 2003. Te podatke sem primerjala tudi s številom terorističnih incidentov v posamezni državi.

Kot sem ugotovila, javno mnenje ne održa nujno stanja oz. dogodkov (v tem primeru število terorističnih incidentov) v lastni državi. To se lepo odrazi na primeru Poljske in Slovaške, v katerih v preučevanem obdobju ni bilo terorističnih incidentov, vendar zaznavata terorizem kot zelo pomembno grožnjo, podobno kot druge preučevne države. Obstajajo pa tudi izjeme, kot je na primer Slovenija, v kateri prav tako ni bilo terorističnih napadov, terorizem pa zaznava kot majhnjo grožnjo, saj se terorizem med vsemi naštetimi grožnjami varnosti, skupaj z vojaškim ogrožanjem države nahaja na dnu lestvice groženj. Iz tega lahko ugotovim, da število terorističnih dejanj ne vpliva nujno na zaznavanje terorizma kot grožnje, odločilen vpliv na javno mnenje imajo množični mediji. Množični mediji narekujejo katera vprašanja so v družbi pomembnjša. Tako so v Sloveniji v ospredju vprašanja, ki se nanašajo na notranjo varnost, degradacijo okolja in socialno-ekonomske vidike. Poljski in Slovaški mediji pa verjetno več pozornosti, med drugim, namenjajo tudi terorizmu. Množični mediji imajo v modernih družbah več vlog: sporočajo informacije javnosti, interpretirajo dogodke in prinašajo (ali umikajo) zadeve v (iz) javnost(i). Glavni vmesni cilj teroristov ni samo povzročanje žrtev in destrukcije, pač pa je eden izmed teh ciljev tudi povzročanje strahu in negotovosti med ljudmi, zato sta propaganda in objavljanje oz. publiciteda zelo pomembna sestavna dela strategije teroristov. Teroristi hočejo pritegniti pozornost ljudi in vlad, množični mediji pa predstavljajo kanal, prek katerega to dosežejo. Zato je eden izmed ciljev teroristov pritegniti pozornost medijev. V preteklosti so le-to dosegli prek samomorilskih in drugih nasilnih napadov, danes pa internet (IKT) teroristom omogoča, da brez nadzora oblasti (cenzure) in neodvisno od drugih množičnih medijev v zelo kratkem času dosežejo velik krog občinstva. V tem smislu uporaba IKT (predvsem interneta) vpliva na javno mnenje. Ta vpliv pa je še toliko večji, ker teroristi sami objavljajo kar hočejo (npr. posnetki z obglavljanjem žrtev), nad tem pa je zelo težko, v veliko primerih celo nemogoče, izvajati nadzor.

Iz vsega do sedaj povedanega lahko potrdim mojo prvo hipotezo, da imajo teroristična dejanja z uporabo sodobne IKT vse večji učinek, tako v smislu doseganja ciljev, kot tudi vpliva na javno mnenje.

Druga hipoteza mojega diplomskega dela pa se nanaša na študijo primera in pravi, da *teroristična organizacija PKK med oblikami informacijskega bojevanja daje največji poudarek psihološkemu bojevanju, še posebej propagandi*.

Ugotovila sem, da poskuša PKK razvijati propagando v veliko množičnih medijih, še vedno uporablja tradicionalne medije kot so tisk, radijo in televizija, vse bolj pa se poslužuje tudi IKT, predvsem interneta. Organizacija ima v lasti vsaj en tiskani medij (Sexwerbûn), najmanj dve radijski postaji (Denge Mesopotamya in Voice of Mesopotamya) in eno TV postajo (Roj TV). PKK pa daje vse večji poudarek internetu, kar kaže dejstvo, da imajo vsi omenjeni tradicionalni mediji svoj spletni dostop, kar jim omogoča svetovno občinstvo, brez tega bi bili ti mediji dostopni veliko manjšemu krogu občinstva kot so sedaj. Organizacija razpolaga tudi s svojim spletnim medijskim portalom Doza me. Poleg tega ima organizacija in njeni privrženci veliko število lastnih spletnih strani (kolikor sem jih zasledila, dejansko jih je lahko se več). Propaganda ima tudi v strukturi organizacije svoje mesto, saj je PKK ustanovila poseben organ – Tiskovni komite, čigar naloga je skrb za javno menenje v Kurdistanu in izven njega, organizanje tiska in publikacij na nacionalni ravni, razvijanje ustreznih in ustanavljanje novih institucij.

Uporabo ostalih preučevanih oblik informacijskega bojevanja (hekersko in kibernetsko) pri PKK nisem zasledila, z izjemo dveh fizičnih napadov na komunikacijska sredstva. Kar pa ne pomeni, da PKK ne izvaja kibernetskega in hekerskega bojevanja, pač pa je takšne napade težko odkriti oz. težko je odkriti povzročitelje takšnih napadov, saj IKT akterjem omogoča anonimnost.

Pri dokazovanju prve hipoteze je potrebno upoštevati dejstvo, da v moji analizi ni zajeto vse psihološko bojevanje in propaganda, ki ga lahko izvaja PKK, ampak predvsem tisti del, ki ga izvaja prek in s pomočjo interneta (IKT), tudi analiza tradicionalnih medijev (tiska, radia in televizije) je temeljila na analizi spletnih dostopov. Psihološko bojevanje ter propaganda pa se lahko izvajata tudi prek drugih medijev (npr. filmi, videokasete, »face-to-face«, letaki itd). Glede na to lahko samo deloma potrdim mojo drugo hipotezo, da teroristična organizacija PKK med oblikami informacijskega bojevanja daje največji poudarek psihološkemu bojevanju, še posebej propagandi.

Vidimo, da se teroristi v današnjem času vse bolj poslužujejo IKT, predvsem interneta. To se lepo odrazi tudi na teroristični organizaciji PKK, ne samo zaradi velikega števila spletnih strani teroristov in njihovih privržencev, pač pa tudi zaradi tega, ker večino njenih medijev in tudi medijev (tisk, radio, tv), ki poročajo o njej, najdemo na svetovnem spletu. O veliki prisotnosti PKK na svetovnem spletu govorijo tudi podatki analize o pogostosti pojavljanja PKK na svetovnem spletu.

Kot ugotavljajo nekateri avtorji (Cronin in Crawford) je uporaba IKT lahko trojna:

- **Fizična,** ki se nanaša na fizično uničenje nasprotnikovih informacijskih in komunikacijskih sredstev tudi s konvencionalnim orožjem. Tako uporabo lahko imenujemo tudi kibernetsko bojevanje.
- **»Mehka«** (sintaktična raven) – nasprotnikove sisteme se onesposablja s pomočjo programskih sredstev kot so: virusi, črvi, trojanski konji ter druga podobna orodja ali pa se poskuša z vdori od zunaj in znotraj onemogočiti delovanje informacijskih sistemov.
- **Psihična** (semantična raven ali omrežno bojevanje) – poudarja vdore, katerih glavni namen je vplivanje na zaznave nasprotnika, oblikovanje njegovih mnenj in stališč, zagotavljanje in utrjevanje prevar ter delovanje v »epistimološkem« bojevanju (Cronin in Crawford v Svete 2005: 288,289).

Glede na analizirane vire in literaturo ter študijo primera lahko zaključim, da danes teroristi IKT (internet) lahko uporabljajo, predvsem za naslednje dejavnosti:

- Prihološko bojevanje, ki ga teroristi lahko izvajajo na več načinov. Na primer: internet lahko uporabijo za širjenje napačnih informacij, da razširijo grožnje namenjene povzročanju strahu in nemoči ter raztrosenju strašnih predstav o nedavnih akcijah, kot je bil npr. posnetek umora ameriškega novinarja Daniel-a Pearl, ki je bil predvajan na mnogih terorističnih spletnih straneh. V okviru psihološkega bojevanja teroristi IKT najbolj uporabljajo predvsem za propagando in objavljanje. Pred pojavom interneta so si morali teroristi prizadevati (z uporabo velikega nasilja, samomorilskih akcij ipd.) pritegniti pozornost radia, televizije ali tiskanih medijev. Z uporabo interneta pa to ni več potrebno, sedaj imajo tororisti neposreden nadzor nad vsebino svojih sporočil, oblasti pa nimajo nadzora.
- Zbiranje podatkov in informacij (npr. o potencialnih žrtvah napadov) – svetovni splet ponuja na miljone strani z informacijami, ki so večinoma brezplačne.
- Zbirnje finančne in materialne podpore.
- Novačenje in mobilizacijo članov.
- Mreženje – mnoge teroristične organizacije, med njimi Hamas in Al Kaida, so prešle iz strogo hierarhične strukture organizacije z določenimi voditelji k bolj decentraliziranim oblikam organizacije, sestavljenim iz delno samostojnih celic brez hierarhičnega vodstva.
- Deljenje informacij – na svetovnem spletu lahko najdemo mnogo strani, ki ponujajo informacije, kako izdelati kemična ali eksplozivna orožja. Mnoge spletne strani

ponujajo priročnike, kot sta na primer Teroristični priročnik (The Terrorist Handbook) in Anarhistična kuharska knjiga (The Anarchist CookBook).

- Načrtovanje in koordinacijo aktivnosti – npr. Al Kaida je za načrtovanje in koordinacijo napada na ZDA (11. septembra 2001) veliko uporabljala internet. Po aretaciji Abu Zubaydah-a, ki naj bi bil po nekaterih domnevah vodja teh napadov, so v njegovem računalniku našli na tisoče kodiranih sporočil, ki so bili poslani prek zaščitenih delov spletnih strni (Weimann, 2004).

V vseh teh primerih teroristi izrabljajo predvsem komunikacijske sposobnosti interneta. Narašča tudi uporaba IKT v razdiralne namene, katerih cilj je motenje informacijskih sistemov. Uničevanje informacijskih sistemov oz. informacijski terorizem pa za enkrat še ni cilj teroristov. Tudi primerov fizičnega uničenja informacijskih sistemov, ki ga Cronin in Crawford, kot sem že omenila, štejeta pod kibernetsko bojevanje, je bilo, glede na študijo primera, relativno malo (samo dva). Če pogledamo bazo podatkov o terorističnih incidentih MIPT, lahko ugotovimo, da je bilo tudi skupno število fizičnih napadov na informacijske sisteme (število napadov vseh terorističnih organizacij) relativno majhno. Takšni napadi so se začeli pojavljati po letu 1998, zdi pa se, da njihovo število počasi narašča, zato in zaradi vse večjega strateškega pomene IKT lahko v bodoče pričakujemo več takšnih napadov. Cilj takšnih napadov, gleda na dosedanje izkušnje, ni povzročanje velikega števila žrtev, pač pa le fizično uničenje informacijsko-komunikacijskih sistemov.

Na tem mestu se lahko strinjamo s Thomasom, ki meni, da se najnevarnejša oblika uporabe interneta ne nanaša (vsaj zaenkrat še ne) na informacijski terorizem oz. programske ali fizične napade na informacijske sisteme, temveč na njegovo komunikacijsko zmogljivost – kibernetsko načrtovanje (ang. Cyberplanning). Le-to se, po Thomasu (2003: 113), nanaša na »digitalno koordinacijo integriranega načrta, ki presega geografske meje ter ima ali ne za posledico prelivanje krvi«. Kibernetsko načrtovaje je pomemben način operativnega delovanja tako za teroristične kot druge uporniške skupine. Internet omogoča teroristom anonimnost in fleksibilnost, hkrati pa predstavlja učinkovito sredstvo poveljevanja in nadzora koordinacije ter možnosti integriranega napada (Thomas, 2003). Kar pa ne pomeni, da informacijskemu terorizmu oz. programskemu ali fizičnemu napadu na informacijske sisteme ni vredno posvečati pozornosti. Kajti nova generacija teroristov bo, kot sem že omenila, zrasla v digitalnem svetu, zato bo razpolagala z večjim hekerskim znanjem in veščinami in s še močnejšimi ter lažje uporabljivimi hekerskimi orodji. Le-ti bodo lahko videli večji potencial v uporabi IKT v uničevalne namene kot današnji teroristi. Lahko pričakujemo tudi, da se bosta

v prihodnostni resnični in virtualni svet zelo zbližala z velikim številom naprav priklopljenih na internet in takrat bodo te oblike uporabe IKT postale bolj privlačne.

7 UPORABLJENI VIRI IN LITERATURA

Monografije

Knjige, diplomska in magistrska dela, doktorske disertacije

1) Arquilla, John in Ronfeldt, David (1996): *The Advent of Netwar*. Washington D:C.: RAND Corporation. (Dostopno tudi na http://www.rand.org/publications/MR/MR789/ index.html, 3. marec 2005).
2) Galley, Patrick (1996): *Computer terrorism: What are the risks?*, prevod v angleški jezik Janmohamed, Arif M. (1998). Swiss Federal Institute of Technology. (Dostopno tudi na http://www.iwar.org.uk/cyberterror/resources/risks/index.html, 16. februar 2005).
3) Krunić, Zoran (1997): *Strategija posrednega nastopanja: način uresničevanja agresivnih političnih ciljev brez odkrite uporabe oboroženega nasilja*. Ljubljana: Unigraf.
4) Libicki, Martin (1995): *What is Information Warfare?*. Washington D.C.: Institute for National Strategic Studies. (Dostopno tudi na http://www.iwar.org.uk/iwar/resources/ ndu/infowar/ contents, 9. december 2004).
5) Mišmaš, Aleš (1999): *Strateško informacijsko vojskovanje*. diplomsko delo. Ljubljana: Fakulteta za družbene vede,
6) Picard, Robert G. (1993): *Media Portayals of Terrorism: Functions and Meaning of News Coverage.* Ames: Iowa State University Press.
7) Shahar, Yael (1997): *Information warfare*. Herzlia (Izrael): International Policy Institute for Counter-Terrorism. (Dostopno tudi na http://www.iwar.org.uk/cyberterror/resources/CIT.htm, 16. februar 2005).
8) Splichal, Slavko (1997): *Javno mnenje: teoretski razvoj in spori v XX. stoletju*. Ljubljana: Fakulteta za družbene vede (Knjižna zbirka Javnost).
9) Svete, Uroš (1999): *Informacijsko bojevanje – opredelitev in koncept*. diplomsko delo. Ljubljana: Fakulteta za družbene vede.
10) Svete, Uroš (2002): *Vloga in pomen informacijske tehnologije v sodobnem asimetričnem vojskovanju*. magistrsko delo. Ljubljana: Fakulteta za družbene vede.
11) Svete, Uroš (2005): *Varnostne implikacije uporabe informacijsko-komunikacijske tehnologije*. doktorska disertacija. Ljubljana: Fakulteta za družbene vede.

Poglavja iz zbornikov

12) Arquilla, John in Ronfeldt, David (1997a): Information, Power and Grand Strategy: In Athena's Camp – Section 1. (Dostopno tudi na http://www.rand.org/publications/MR/MR880/ MR880. ch6.pdf, 9. december 2004). V Arquilla, John, Ronfeldt, David (ur.): *In Athena's Camp: Preparing for Conflict in the Information Age*, 141-171. Washington D.C.: RAND Corporation.

13) Arquilla, John in Ronfeldt, David (1997b/1993): Cyberwar is Comming!. (Dostopno tudi na http://www. rand.org/publications/ MR/MR880/MR880.ch2.pdf, 9. december 2004). V Arquilla, John in Ronfeldt, David (ur.): *In Athena's Camp: Preparing for Conflict in the Information Age*, 23-60. Washington D.C.: RAND Corporation.

14) Arquilla, John, Ronfeldt, David in Zanini, Michele (1999): Networks, Netwar, and Information-Age Terrorism. (Dostopno tudi na http://www.rand.org/publications/MR/MR989/MR989.chap3.pdf, 9. december 2004). V Lesser, Ian O., Hoffman, Bruce, Arquilla, John, Ronfeldt, David F., Zanini, Michele, Jenkins, Brian Michael (ur.): *Countering the New Terrorism*, 39-84. Washington D.C.: RAND Corporation.

15) Berkowitz, Bruce (1997): Warfare in the information age. (Dostopno tudi na http://www.rand.org/ publications/MR/MR880/MR880ch7. pdf, 9. december 2004). V Arquilla, John in Ronfeldt David (ur.): *In Athena's Camp: Preparing for the Conflict in the Information Age*, 175-189. Washington D.C.: RAND Corporation.

16) Devost, Matthew, Houghton, Brian In Pollard, Neal (1997–1998): Information Terrorism: Can You Trust Your Toaster?. (Dostopno tudi na http://all.net/books/tzu/tzu.html, 9. november 2004). V Sun Tzu Art of War in Information Warfare.

17) Hoffman, Bruce (1999): Terrorism Trends and Prospects. (Dostopno tudi na http://www.rand.org/publications/MR/MR989/MR989.chap2.pdf 9. december 2004). V Lesser, Ian, Hoffman, Bruce, Arquilla, John, Ronfeldt, David, Zanini, Michele, Jenkins, Brian Michael (ur.): *Countering the New Terrorism*, Washington D.C.: RAND Corporation.

18) Malešič, Marjan (1997): A Model of Propaganda, Psychological and Political Warfare and Propaganda. V Malešič, Marjan (ur), *Propagand in War*, Stocholm.

19) (1999): Trends in Terrorism. (Dostopno tudi na http://www.iwar.org.uk/cyberterror/resources/csis/terror-trends.htm, 16. februar 2005).

V *Canadian Security Intelligence Service Publication*. Ottawa: Canadian Security Intelligence Service.

20) Zanini, Michele in Edwards, Sean (2001): The Networking of Trror in the Information Age. (Dostopno tudi na http://www.rand.org/publications/MR/MR1382/MR1392.ch2.pdf, 3. marec 2005).V Arquilla, John in Ronfeldt, David (ur.): *Networks and Netwars: The Future of Terror, Crime and Militancy*, 29-60. Washington D.C.: RAND Corporation.

Članki v znanstvenih in strokovnih publikacijah

21) Arsić, Sranislav (2004): Informacijsko bojevanje, Nevidni sovražnik. *Revija Obramba*, 12/2004, 23–25.

22) Arquilla, John in Ronfeldt, David: (1995): Cyberwar and Netwar: New Models, Old Concepts, of Conflict. V: Shoben, Ann (ur.): Information War and Cyberspace Security, *Rand Research Review*, 19 (2). (Dostopno tudi na http://www.rand.org/publications/randreview/issues/RRR.fall95.cyber/ cyberwar.html, 9. december 2004).

23) Belič, Igor (2001): Informacijski terorizem. *Varstvoslovje* 3 (4), 262–268.

24) Bratuša, Tomaž (2004a): Hekerji in zaščitniki (1. del). Moj mikro 10/2004, 30–32. (Dostopno tudi na http://www.mojmikro.si/artiles/ 30_32_hekerske metode.pdf 5. junij 2005).

25) Bratuša, Tomaž (2004b): Skeniranja, slepljenje, vohljanje ..., hekerske metode (2. del). *Moj mikro* 12/2004, 38–41. (Dostopno tudi na http://www.mojmikro.si/articles/38_41_hekerske_metode_2_del.pdf, 5. junij 2005).

26) Bratuša, Tomaž (2005a): Vsem dostopna nevarna orodja, hekerske metode (3.del). *Moj mikro* 1/2005, 38–43. (Dostopno tudi na http://www.mojmikro.si/articles/mi04_38_40protihekerska_orodja.pdf, 5. junij 2005).

27) Bratuša, Tomaž (2005b): War dialing – napad na vaše modeme, hekerska orodja (4. del). *Moj mikro* 2/ 2005, 34–37. (Dostopno tudi na http://www.mojmikro.si/articles/02_34_37_hekerska_orodja_4_del.pdf, 5. junij 2005).

28) Bratuša, Tomaž (2005c): Vrtanje skozi požarne zidove, hekerska orodja (6. del). *Moj mikro*, 4/2005, 36–38. (Dostopno tudi na http://www.mojmikro.si/articles/mi04_36-38hakerska_orodja.pdf., 5. junij 2005).

29) Conway, Maura (2002): Reality Bytes: Cyberterrorism and Terrorist »Use« of Internet. *First Monday*, 7 (11). (Dostopno tudi na http://firstmonday.org/issues/issue7_11/ conway/index.html, 13. januar 2005).

30) Denning, Dhoroty E. (2000a): Cyberterrorism. *Global Dialogue*. (Dostopno tudi na http://www.cs.georgetown.edu/~denning/infosec/cyberterror-GD.doc, 9. november 2004).

31) (2004): Nove grožnje z interneta (VI): hekerska orodja. *Kapital, revija za naložbo denarja,* 1/2004. (Dostopno tudi na http://www. revijakapital.com/kapital/, 6. maj 2005).

32) Omaljev, Jovan (2001): Medijski rat. *Vojno delo, opštevojni teorijski časopis*, 53 (1), 106–114.

33) Skrt, Radoš (2004): "Ribarjenje" zaupnih osebnih podatkov. *Moj mikro* 12/2004, 26–28. (Dostopno tudi na http://www.mojmikro.si/articles/26_28_nevarnosti_interneta.pdf, 5. junij 2005).

34) Thomas, Thimoty (2003): Al Qaeda and the Internet: The Danger of »Cyberplanning. *Parameters*, XXXIII (1), 112–123. (Dostopno tudi na http://carliste-www.army.mil/usawc/Parameters/03spring/thomas.pdf, 1. december 2004).

35) Whine, Michael (1999): Cyberspace, A New Medium for Communication, Command and Control by Extremists. *Studies in Conflict and Terrorism*. (Dostopno tudi na http://www.ict.org.il/articles/articledet.cfm? articleid=76, 9. december 2004).

Članki v tiskanih medijih

36) *Delo*: 02.04.04, 07.04.04, 10.06.04, 14.06.04, 03.07.04, 11.08.04, 23.10.04, 13.05.05. Dostopno dokumentcija Dela, Ljubljana in http://www.delo.si/ (15. junij 2005).

37) *Dnevnik*: 22.04.04, 09.06.04, 02.07.04, 10.08.04, 20.08.04, 10.09.04, 15.02.05, 12.05.05. Dostopno dokumentacija Dela, Ljubljana in http://www.dnevnik.si/ (15. junij 2005).

38) *Die Welt*: 16.02.04, 29.05.04, 01.06.04, 10.06.04, 25.06.04, 02.07.04, 15.07.04, 10.08.04, 11.08.04, 20.08.04, 15.09.04, 13.10.04, 20.10.04, 15.11.04, 16.11.04, 08.01.05, 21.01.05, 22.03.05. Dostopno na http://www.welt.de/ (15. junij 2005).

39) 2004*: France Silenced The Kurdish Voice Of Freedom And Peace!*. Kurdistan Observer, 14.februar, 2004. Dostopno na http://home.cogeco.ca/~kurdistan1/15-2-04-france-closes-media-tv.htm (25. avgust 2005).

40) *Frankfurter Rundschau*: 07.02.04, 27.03.04, 03.06.04, 11.08.04, 13.11.04, 15.05.05, 28.05.05. Dostopno na http://www.fr-aktuell.de/ (15. junij 2005).

41) *Turk US*: 11.01.04, 13.01.04, 20.01.04, 05.05.04, 11.05.04, 29.05.04, 02.06.04, 09.06.04, 12.06.04, 15.06.04, 23.06.04, 25.06.04, 29.07.04, 09.08.04, 11.08.04, 22.09.04, 23.09.04, 28.09.04, 26.10.04, 27.10.04, 15.11.04, 14.01.05, 15.01.05, 27.03.05, 14.04.05, 11.05.05, 15.05.05, 19.05.05, 27.05.05. Dostopno na http://www.turk.us/ (15. junij 2005).

42) *Turkish Press*: 02.01.04, 08.01.04, 23.06.04, 23.06.04, 16.08.04, 17.11.04, 15.03.05, 16.03.05, 24.03.05, 25.03.05, 09.04.05, 14.04.04, 15.04.05, 18.04.05, 19.04.05. Dostopno na http://www.turkishpress.com/ (15. junij 2005).

43) Singh, Gajendra, K. (2004): Turkey snaps over US bombing of its brethren. *Asia Times*, 18. september 2004. Dostopno na http://www.atimes.com/ (13. april 2005).

44) *Suddeutsche Zeitung*: 23.02.04, 10.08.04, 18.10.04, 21.10.04, 13.11.04, 10.01.05, 09.05.05, 12.05.05. Dostopno na http://www.suddeutsche.de/ (15.junij 2005).

45) *Večer*: 17.01.04, 10.06.04, 15.06.04, 03.07.04, 11.08.04, 12.08.04, 28.08.04, 13.11.04, 07.12.04 Dostopno dokumentacija Dela, Ljubljana in http://www.vecer.si/ (15. junij 2005).

46) *Zaman*: 05.01.04, 09.01.04, 27.02.04, 28.02.04, 22.03.04, 09.04.04, 07.05.04, 11.05.04, 20.05.04, 05.06.04, 09.06.04, 10.06.04, 15.06.04, 22.06.04, 24.06.04, 03.07.04, 06.07.04, 07.07.04, 14.07.04, 15.07.04, 18.07.04, 26.07.04, 14.08.04, 11.09.04, 17.09.04, 10.10.04, 13.11.04, 06.04.05, 08.04.05, 12.04.05, 30.04.05, 13.05.05, 14.05.05, 21.05.05, 27.05.05. Dostopno na http://www.zaman.com/ (15. junij 2005).

47) Zgaga, Blaž (2005): Raziskava stališč o nacionalni in mednarodni varnosti: Le petina Slovencev se boji terorizma. *Večer*, 12. julij 2005, str. 3. (Dostopno tudi na http://www.vecer.si/vecer2003/default.asp?kaj=1&p=V%20AEARI%A9%C8U, 5. oktober 2005).

Enciklopedije in leksikoni

48) (2000) *Dictationary.LaborLawTalk.com*. Dostopno na: http://encyclopedia.laborlawtalk.com/public_opinion (16. september 2005).

49) Pahor, David (ur.) (2002): *Leksikon računalništva in informatike*, Ljubljana: Pasadena.

50) (1991) *Slovar slovenskega knjižnega jezika*, peta knjiga (T-Ž). Slovenska akademija znanosti in umetnosti, Znanastvenoraziskovalni center Slovenske akademije znanosti in umetnosti. Ljubljana: DZS.
51) (1998) *Veliki splošni leksikon*. Ljubljana: DZS.
52) (2004), *Whatis.com definitions,* The leading IT Encyklopedia and learning center. Dostopno na http://whatis.techtarget.com/ (11. marec 2005).
53) (2001) *WordNet.* Princeton: Princeton University, Dostopno na http://www.answers.com/ library/WordNet;jsessionid=b8h6905sh238u-cid-1341761451-sbid-lc01a (16. september 2005).

Baze podatkov in raziskave

54) *Country Reports on Terrorism 2004* (2005) Washington D.C.: U. S. Department of State. (Dostopno tudi na http://www.state.gov/s/ct/rls/c14812.htm, 5. maj 2005).
55) *Internet World Stats* (2005) Usage and Population Statistics. Dostopno na http://www.internetworldstats.com/stats.htm (12. julij 2005).
56) (2003) Javnomnenjska raziskava, *Nacionalna in mednarodna varnost 2003*. Ljubljana: Obramboslovni raziskovalni center, Fakulteta za družbene vede – Inštitut za družbene vede Univerze v Ljubljani. (Dostopno tudi na http://nato.gov.si/slo/javno-mnenje/nacionalna-varnost.pdf, 5. oktober 2005).
57) *MIPT Terrorism Knowledge Base* (2005) A Comprehensive Databank of Global Terrorist Incidents and Organizations. Olkohoma City: National Memorial Institute for Prevention of Terrorism. Dostopno na http://www.tkb.org/, (5. avgust 2005).
58) *Patterns of Global Terrorism 1996* (1997) Washington D.C.: U. S. Department of State. (Dostopno tudi na http://www.state.gov/www/global/terrorism/1996Report/1996index.html, 1. marec 2005).
59) *Patterns of Global Terrorism 1997* (1998) Washington D.C.: U. S. Department of State. (Dostopno tudi na http://www.state.gov/www/global/terrorism/1997Report/1997index.html, 1. marec 2005).
60) *Patterns of Global Terrorism 1998* (1999) Washington D.C.: U. S. Department of State. (Dostopno tudi na

http://www.state.gov/www/global/terrorism/1998Report/1998index.html, 1. marec 2005).

61) *Patterns of Global Terrorism 1999* (2000) Washington D.C.: U. S. Department of State. (Dostopno tudi na http://www.state.gov/www/global/terrorism/1999Report/1999index.html, 1. marec 2005).
62) *Patterns of Global Terrorism 2000* (2001) Washington D.C.: U. S. Department of State. (Dostopno tudi na http://www.state.gov/s/ct/rls/pgtrpt/2000, 1. marec 2005).
63) *Patterns of Global Terrorism 2001* (2002) Washington D.C.: U. S. Department of State. (Dostopno tudi na http://www.state.gov/s/ct/rls/pgtrpt/2001, 1. marec 2005).
64) *Patterns of Global Terrorism 2002* (2003) Washington D.C.: U. S. Department of State. (Dostopno tudi na http://www.state.gov/s/ct/rls/pgtrpt/2002, 1. marec 2005).
65) *Patterns of Global Terrorism 2003* (2004) Washington D.C.: U. S. Department of State. (Dostopno tudi na (http://state.gov/s/ct/rls/pgtrpt/2003, 1. marec 2005).
66) (2002): Raziskava Slovensko javno mnenje – Primerjalni podatki povezani z odnosom slovenske javnosti do Nata v letih 1999 in 2001, *Ogrožanje varnosti*, Urad vlade RS za informairanje: Slovenija – NATO. Dostopno na http://nato.gov.si/slo/javno-mnenje/varnost/podatki-varnost/ (5. oktober 2005).
67) *The World Factbook 2005*. (Dostopno tudi na http://www.cia.gov/cia/publications/factbook/, 15. februar 2005).
68) *Transatlantic Trends 2005*, Topline Data. Washington D.C.: German Marshall Found of the United States. (Dostopno tudi na http://www.transatlantictrends.org/doc/TTToplineData2005.pdf, 16. september 2005).

Gradivo, prispevki iz interneta

69) (2005) *Aktuelle Nachrichten.* Kurdish info. Dostopno na http://www.kurdishinfo.com/ (17. maj 2005).
70) (1998) *Terrorist Activities on the Internet*. Anti-Defamation League (ADL). Dostopno na http://www.adl.org/terror/focus/16_focus_a.asp (25. januar 2005).
71) *PKK and Terrorism, A Report on PKK and Terrorism*. Washington D. C.: Asembly of Turkish American Associations (ATAA). Dostopno na http://www.ataa.org/ataa/ref/pkk/mfa/report-pkk-terrorism.html (22. oktober 2004).

72) Braun, Rainer (2005): *The print sector in the Federal Republic of Germany*. Berlin: Goethe-Institut. Dostopno na http://www.goethe.de/enindex.htm (19. maj 2005).

73) Cramer, Myron C. (1996): *Information Warfare, Information revolution, It´s Current and Future Consequences*. Maryland: Georgia Institute of Technology. Dostopno na http://iw.windermeregroup.com/Papers/infowar.html (5. januar 2005).

74) Denning, Dorothy E. (1999): *Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy*. Georgetown University. Dostopno na http://www.cs.georgetown.edu/~denning/infosec/nautilus.html (9. november 2004).

75) Denning, Dorothy E. (2000b): *Testimony before the Special Oversight Panel on Terrorism*. U.S. House of Representatives, Committee on Armed Services. Dostopno na http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html (9. november 2004).

76) Denning, Dorothy E. (2001): *Is Cyber Terror Next?*. New York: U.S. Social Science Research Council, (1. novemeber 2001). Dostopno na http://www.ssrc.org/sept11/essays/ denning.htm (9. november 2004).

77) Devost, Matthew G. (1995): *National Security in the Information Age*. Dostopno na http://matt.devost.net/mattd/papers_and_essays/ (9. december 2004).

78) Dimec, Jure (2002):. *Uvod in Zgodovina interneta*. Predavanje: Računalniška omrežja 1. Bib: Informatika 2, Rač Komuniciranje. Dostopno na http://www.mf.uni-lj.si/~jure/pred_bib/rač-komun/p1/omrežja1.html (25. avgust 2005).

79) (2004) EPRA – European Platform of Regulatory Authotities. Dostopno na http://www.epra.org/comasystem/output_presse.pl?language=e. (12. julij 2005)

80) Goldberg, Ivan (2004) Institute for Advanced Study of Information Warfare. Dostopno na http://www.psycom.net (09. december 2004).

81) Golubev, Vladimir (2003): *Cyberterrorism - the new side of terrorism*. Zaporozhye (Ukrajina): Computer Crime Research Center. Dostopno na http://www.crime-research.org/news/2003/07/ Mess2102.html, (12. november 2004).

82) (1996) *Kurdish Information Network*. Dostopno na http://www.xs4all.nl/~tank/kurdish/ htdocs/facts/ (25. oktober 2004).

83) Lewis, Brian C. *Information Warfare*. Executive Summary. Dostopno na http://www.fas.org/irp/eprint/snyder/infowarfare.htm (22. oktober 2004).

84) Obča Komunikologija, *Vprašanja in odgovori*. Dostopno na http://www.fdvinfo.net/uploadi/editor/vpr_odgovori-komII.doc (5. september 2005).

85) Pike, John (2004): *Kongra-Gel, Kurdistan Freedom and Democracy Congress (KADEK), Kurdistan Workers' Party (PKK)*. Globalsecurity. Dostopno na http://www.globalsecurity.org/military/world/para/pkk.htm (14. marec 2005).

86) Politt, Mark M. (1997): *Cyberterrorism – Fact or Fancy?* Washington D. C.: FBI Laboratory. Dostopno na http://www.cs.georgetown.edu/~denning/infosec/pollitt.html (9. november 2004).

87) Savino, Adam (2002): *Cyber-Terrorism*. Introduction. Dostopno na http://cybercrimes.net/ Terrorism/ct.html (9. december 2004).

88) Strpić, Ognjen (2002): Ricardo Dominguez: *Umrežno ratovanje i druge priče*. Projekt, Broadcasting. Dostopno na http://boo.mi2.hr/~ognjen/tekst/dominguez_hr.html. (13. oktober 2004).

89) (2000) *Terror Organisations in Turkey, Separatist Terror Organisation, KADEK Terror Organisation*. Ankara: Forsnet. Dostopno na http://www.terror.gen.tr/english/organisations/pkk.html (16. februar 2005).

90) Thomas, Timothy (2002): *30 Informationa-Age »De-Terror-Ance«*. Dostopno na http://www.leavenworth.army.mil/milrev/English/JanFeb02/thomas.htm (1. december 2004).

91) (2002) *Weapons & Terrorism, Terrorists Use of Information Technology*. Terrorism files. Dostopno na http://www.terrorismfiles.org/weapons/information_technology.html (22. marec 2005).

92) Weimann, Gabriel (2004): *How Modern Terrorism Uses the Internet*, special report 116. Washington D.C.: United States Institute of Peace. Dostopno na http://www.usip.org/pubs/specialreports/sr116html (5. maj 2005).

93) (2002) *Zgodovina interneta*. Webdesign.fluido.it. Dostopno na http://www.fluido.it/webdesign/internet/02.html, (29. avgust 2005).

Spletne strani in iskalniki

94) Abdullah Öcalan, http://www.abdullah-obalan.com/ (4. april 2005).

95) AFP, http://www.afp.com/english/ (4. april 2005).

96) Alta Vista, http://www.altavista.com/, (7. april 2005).

97) ClandestineRadio.com, http://www.clandestineradio.com/ (8. april 2005).

98) Denge Mesopotamya, http://www.denge-mezopotamya.com/ (4. april 2005).

99) Doza me, http://www.dozame.org/ (18. junij 2005).
100) Google, http://www.google.com/, (7. april 2005).
101) HPG, Ljudske obrambne sile, http://www.hpg-online.com/ (17. maj 2005).
102) HPG, Ljudske obrambne sile http://www.hazenparastine.com/ (13. maj 2005).
103) Kongra-Gel, http://www.kongra-gel.com/, http://www.kongra-gel.net/, http://www.kongra-gel.org/ (11.junij 2005).
104) Kurdish point, http://www.kurdishpoint.com/, (28. julij 2005).
105) Kurdistan4all, http://www.kurdistan4all.com/, (28. julij 2005).
106) Mednarodna pobuda Svoboda za A. Öcalana – Mir v Kurdistanu http://www.freedom-for-ocalan.com/ (4. april 2005).
107) Medya TV, http://www.medyatv.com/ (4. april 2005).
108) Mezopotamya TV, http://www.metv.dk/english%20pages/audience.htm (12. junij 2005).
109) MSN, http://www.msn.com/, (7. april 2005).
110) Onlinenewspapers.com, http://www.onlinenewspapers.com/, (28. julij 2005).
111) PKK, http://www.pkk.org/ (17. maj 2005 in 17. avgust 2005).
112) PKK, http://www.pkkgercegi.net/ (14. marec 2005).
113) Reuters, http://www.reuters.com/ (4. april 2005).
114) Roj TV, http://www.roj.tv/ (12. julij 2005).
115) Rojaciwan, http://www.rojaciwan.com/ (12. julij 2005).
116) Rojame, http://www.rojame.com/ (18. julij 2005).
117) Serxwerbun, http://www.serxwebun.org/index.php (12. julij 2005).
118) Tecak, http://tecakonline.com/ (12. julij 2005).
119) Tecak, forum, http://www.kurd.se/forum (12. julij 2005).
120) Turk Basini, http://www.byegm.gov.tr/TURKBASINI/turkishpress/, (28. julij 2005).
121) Turkish Media, http://www.turkishmedia.net/, (28. julij 2005).
122) UIKI-Onlus, http://www.kurdistan.it/, (18. julij 2005).
123) UIKI-Onlus, http://www.uikionlus.com/, (18. julij 2005).
124) Yahoo, http://www.yahoo.com/, (7. april 2005).

8 PRILOGE

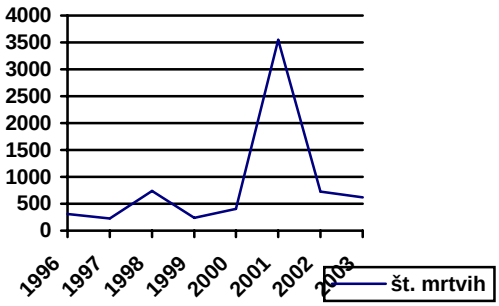
PRILOGA A: Nove informacijske tehnologije, kot jih je opredelil Cramer

Nove informacijske tehnologije	
Računalniško podprto oblikovanje	Digitalno faksiranje
Nepapirnata digitalna oblika proizvodnje in upravljanja organizacije	Optični čitalci (skenerji)
	Prenosni in žepni računalniki
Skupinsko delo (Groupware)	Flash tehnologija
Online storitve	Tehnologija optičnih vlaken
Upravljanje dokumentov	Brezžična tehnologija
Sistemi odjemalec – strežnik	Video – konference
Strežniki	Grafična tehnologija
Mreže	Kompresija (stiskanje) podatkov
Baze podatkov	Predmetna orientacija
Tiskalniki	Navidezna resničnost (virtual reality)
Prepoznavanje glasu	Geografski sistemi (GPS – global positioning system)
Zaščita shranjevanja podatkov	

Vir: Cramer, Myron L. (1996): *Information Warfare, The Information Revolution: It´s Current and Future Consequences*. Georgia Institute of Technology, Maryland. Dostopno na http://iw.windermeregroup.com/Papers/infowar.html (5. januar, 2005)

PRILOGA B: Število terorističnih incidentov in število žrtev (mrtvi in ranjeni) od 1996 do 2003 ter skupno število incidentov od 1982 do 2003

leto	napadi	mrtvi	ranjeni
1996	296	311	2.652
1997	304	221	693
1998	273	741	5.952
1999	392	233	706
2000	423	405	791
2001	346	3.549	1.080
2002	199	725	2.013
2003	208	625	3.646

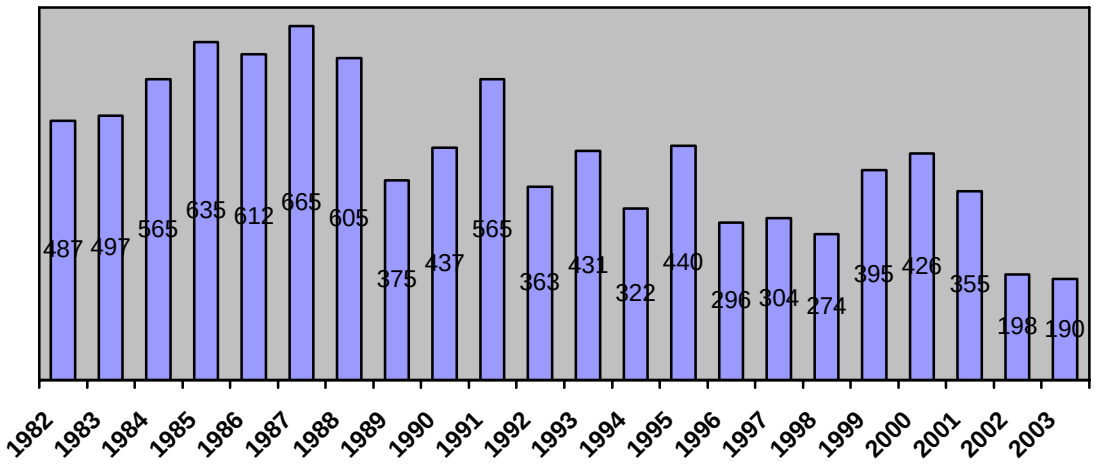


Vir: Patterns of Global Terrorism, 1997, 1998, 1999, 2000, 2001, 2002, 2003 in 2004

Podake sem pridobila iz publikacije ameriškega State Departmenta – Patterns of Global Terrorism. Podatki so zgolj približni, ker se številke tudi v uradnih virih zelo razlikujejo.

Velik porast števila smrtnih žrtev leta 2001 je posledica terorističnega napada na ZDA 11. septembra, ki je terjal več kot 3.000 življenj. Te žrtve predstavljajo nad 90% vseh mrtvih v terorističnih napadih tega leta.

Skupno število terorističnih incidentov od 1982 do 2003



Vir: Patterns of Global Terrorism 2003 (2004): *Total International Terrorist Attacks*, 1982–2003. U. S. Department of State, Washington D.C.. (Dostopno tudi na http://state.gov/s/ct/rls/pgtrpt/2003, 1.marec 2005).

PRILOGA C: Bilanca vojne (od julija 2004 do maja 2005), ki so jo izdale Ljudske obrambne sile (HPG)

Vir: http://www.dozame.org/article.php/2005053102450027 (18. junij 2005).

PRILOGA D: Kurdski in turški mediji(tisk, televizija in radio)

TISK		TV		RADIO	
KURDSKI	**TURŠKI**	**KURDSKI**	**TURŠKI**	**KURDSKI**	**TURŠKI**
Al-furat	Aksam	KNN TV	ATV	Azadi	Show Radyo
Alitihad	Aydinlik	Kurdistan TV	BayrakTV	Dengę mezopotamya	Number One FM
Arunak	Cumhuriyet	KurdSat TV	Cine 5	Dengy Kurdistani Iran	Power FM
Azadiyawelat	Dunya	KTV	CNN Turk	kurdish Radio (Tehran)	Kral FM
Barzan	Evrensel	Khak TV	DIGITURK	Kurdworld Radio	Radyo ODTU
Dema Nu	Fanatik	Mesopotamya TV	FlashTV	Radio Denge kurdistan	İTÜ Radyo
Deng	Finansal Forum	Roj TV	Kanal 6	Radio Dersim	Radyo Bilkent
Denge Kurd	Fotomac	Rojava TV	Kanal 7	Radio Dewane	Radyo Barış
Evro.nu	Gecce	Zagros TV	Kanal D	Radio ERF (Kurmancî)	Best FM
Ewraq kurdiye	Gunes		Kanal E / CNBC-e	Radio ERF (soranî)	Dünya Radyo
Gulan	Gozlem		Kral TV	Radio from sweden-Live	Capital Radyo
Gulan News	Hurriyet		Meltem TV	Radio Haubiran	Alem FM
Gzing	Kazete		MTV	Radio Komala (Shorishgęr)	TGRT FM
Halabja	Milli Gazete		NTV	Radio Komalah	Açık Radyo
Hawlatî	Milliyet		Samanyolu TV	Radio SBS Beshę kurdî	Burç FM
Hevgirtina gel	Mukellef		Show TV	VOA (USA)	Radyo Boğaziçi
Jamawar	Ozgur Politika		Star TV	Voice of Australian Kurds	Radyo Ege
JNiwe	Radikal		TGRT	Zayele (Sweden)	Radyo Eksen
Kurd-L	Resmi Gazete		TRT		Radyo Merhaba
Kurdinfo	Sabah		TV8		Radyo Mydonose
Kurdistan Report	Star				Radyo Poyraz
Kurdistani Newę	Ticaret Gazetesi				Radyo Viva
Kurdistannews.org	Turkiye				Radyo Vizyon
kurdistanpost	Turkey Post (ang.)				SüperFM
Media	Turkish Daily News (ang.)				TRT / Radyo1 / Radyo3 /
Nozhan	Turkish Press (ang.)				Radyo4 / TRT-FM
Ozgurpolitika	Turkish Press				VOA Turkish

	Scaner (ang.)				
Peyam	Turk. US (ang.)				Turkish Radios Online
Peyama Kurd	Vakit Gasetesi (ang.)				Anadolu'nun Sesi Radyosu
Raman News	Vatan				Olay - FM Radyo
Rastî	Yeni Asir				Radyo 99
Regay Kurdistan	Yeni Asya				AkraFM
Resen	YeYeni Gundemni Safak				Radyo58
Ręwan	Zaman (tr., ang.)				Radyokaradeniz
Serdem Niwę					RadyoOnbeş
Serxwebun					YAYINONLINE
Sipede					
Yekgirtu					

Vir: http://www.kurdishpoint.com/, http://www.byegm.gov.tr/TURKBASINI/turkishpress/, http://www.kurdistan4all.com/, http://www.turkishmedia.net/, http://www.onlinenewspapers.com/ (28. julij 2005).

PRILOGA E: Spletna stran Serxwebûn

Vir: http://www.serxwebun.org/index.php (12. junij 2005).

PRILOGA F: Število Kurdov po svetu

Država	**število kurdov**
Turčija	14.000.000
Iran	7.000.000
Irak	4.500.000
Sirija	1.200.000
Nemčija	400.000
Francija	60.000
Nizozemska	50.000
Avstrija	40.000
Združeno Kraljestvo	30.000
Švica	30.000
Švedska	20.000
Danska	15.000
Belgija	15.000
Norveška	10.000
Grčija	5.000
Italija	5.000
Španija	5.000
Finska	3.000
Ciper	3.000
Vzhodna in Srednja Evropa	20.000
Libanon	100.000
Izrael (Judje iz Kurdistana)	150.000
Jordanija	20.000
Nekdanja ozemlja Sovjetske Zveze	500.000

Vir: http://www.metv.dk/english%20pages/audience.htm (12. junij 2005).

PRILOGA G: Spletna stran http://www.roj.tv/

Vir: http://www.roj.tv/ (12. julij 2005).

PRILOGA H: Spletne strani nekaterih terorističnih organizacij 2001/2002 in 2005.

Organizacija	URL (2001/2002)	URL (2005)
Almurabeton	http://www.almurabeton.org	http://www.almurabeton.tk
Al-Jama'ah Al-Islamiyyah	http://www.webstorage.com/~azzam/	stran ni več na tem serverju
Hizb Al- Ikhwan Al Muslimoon	http://www.ummah.org.uk/ikhwan/	http://www.ummah.org.uk/ikhwan/ http://www.muslimmatrimonial.com/muslim-matrimonials/articles/muslim-articles/muslim-brotherhood.shtml
Aum Supreme Truth (Aum)	http://www.aleph.to/index_e.html http://www.aleph.to	http://www.aleph.to http://www.religioustolerance.org/dc_aumsh.htm
Basque Homeland and Liberty (ETA)	http://www.contrast.org/mirrors/ehj/index.html http://www.batasuna.org/	http://www.contrast.org/mirrors/ehj/index.html
Al-Gama'a al-Islamiyya (Islamic Group)	http://www.azzam.com	stran je prazna
Hamas	http://www.palestine-info.com/hamas	stran ni več na tem strežniku
Harakat ul-Mujahidin (HUM)	http://www.ummah.net.pk/harkat/	stran ni več na tem strežniku
Hizbollah	http://www.hizbollah.org http://moqawama.org/page2/main.htm http://www.almanar.com.lb	http://www.hizbollah.org http://www.almanar.com.lb http://www.hizbollah.org/english/frames/index_eg.htm
Kahane Chai (Kach)	http://www.kahane.org	http://www.kahane.org
Kurdska delavska stranka (PKK)	http://www.pkk.org/	http://www.pkk.org http://www.kongragel
Lashkar-e-Tayyiba	http://www.markazdawa.org.pk/	
Liberation Tigers of Tamil Eelam	http://www.eelamweb.com/	http://www.eelamweb.com/
Mujahedin-e Khalq Organization	http://www.iran-e-azad.org/english/index.html	
National Liberation Army (ELN), Colombia	http://www.eln-voces.com/	http://www.eln-voces.com/
Palestine Islamic Jihad (PIJ)	http://www.entifada.net/	
Popular Front for the Liberation of Palestine (PFLP)	http://www.pflp-pal.org/main.html	http://www.pflp.net/
al-Qaida	http://www.alneda.com	http://www.amerika.org/ -domača stran Osame bin Ladna
Revolutionary Armed Forces of Colombia (FARC)	http://www.farc-ep.org/	http://www.farcep.org/ http://www.farcep.org/pagina_ingles/
Revolutionary People's Liberation Party/Front	http://www.ozgurluk.org	http://www.ozgurluk.org

(DHKP/C, Dev Sol)		
Sendero Luminoso (Shining Path)	http://www.csrp.org/	http://www.csrp.org/
United Self-Defense Forces of Colombia (AUC)	http://colombia-libre.org/colombialibre/pp.asp	

Vir: Conway, Maura (2002): Reality Bytes: Cyberterrorism and Terrorist »Use« of Internet. *First Monday*, 7, (11). (Dostopno tudi na http://firstmonday.org/issues/issue7_11/conway/index.html, 13. januar 2005); Zanini, Michele in Edwards, Sean J. A. (2001): The Networking of Terror in the Information Age. (Dostopno tudi na http://www.rand.org/publications/MR/MR1382/MR1392.ch2.pdf, 3. marec 2005) V Arquilla, John, Ronfeldt, David (ur): *Networks and Netwars: The Future of Terror, Crime and Militancy*, RAND Corporation, Washington D.C.; http://www.google.com/ (28. julij 2005).

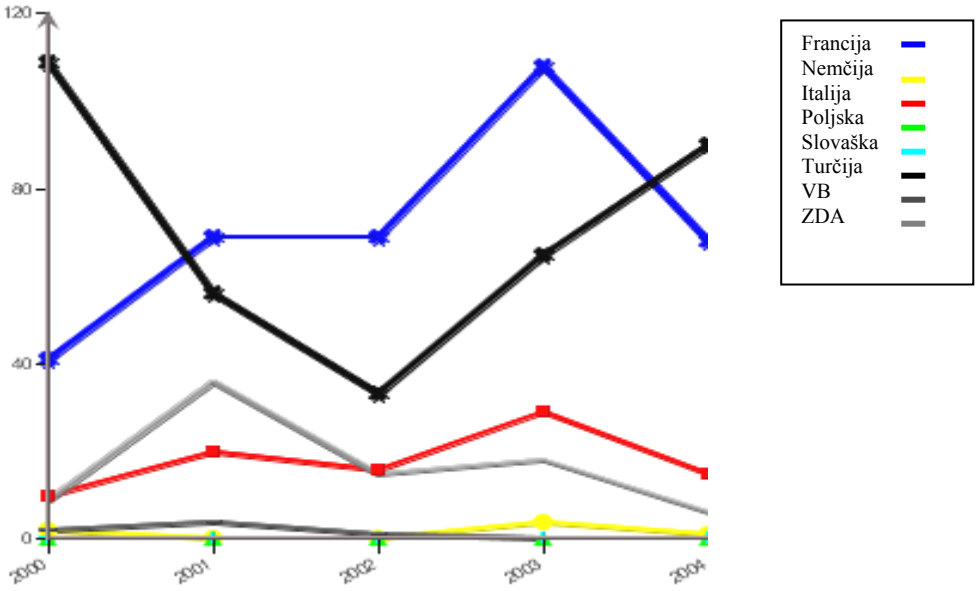
Za leti 2001/2002 sem podatke pridobila iz zgornjih virov. Zaradi že omenjene dinamike terorističnih spletnih strani, sem poskušala ugotoviti, koliko teh spletnih strani še obstaja oz. deluje na istih spletnih naslovih. Rezultate moje analize, ki sem jo izvedla 19. septembra 2005, sem predstavila v tretjem stolpcu zgornje tabele. Nekaj spletnih strani se še vedno nahaja na spletnih naslovih iz leta 2001/2002, veliko jih je spremenilo spletne naslove, kar nekaj pa jih je izginilo oz. se ne nahajajo več na istem strežniku.

PRILOGA I: Rezultati raziskave Transatlantic Trends 2005 (podani v odstotkih anketiranih), ki se nanašajo na vprašanje kako pomembno grožnjo (zelo pomembno, pomembno, nepomembno), po mnenju ljudi, predstavlja mednarodni terorizem.

	država / leto	ZDA	Francija	Nemčija	VB	Italija	Poljska	Slovaška	Turčija
zelo pomembno	**2005**	71	59	58	55	61	64	62	41
	2004	76	70	69	70	76	73	63	39
	2003	70	74	69	65	71	70	/	/
	2002	91	63	74	60	67	55	/	/
pomembno	**2005**	25	36	35	41	34	31	29	41
	2004	20	26	25	27	22	24	28	46
	2003	26	23	26	33	25	25	/	/
	2002	7	33	23	37	27	34	/	/
nepomembno	**2005**	4	5	6	4	4	2	7	12
	2004	3	3	4	2	2	1	6	6
	2003	4	3	4	2	3	2	/	/
	2002	2	3	2	3	6	6	/	/
ne vem/ ni odgovoril	**2005**	1	0	1	0	1	2	2	5
	2004	1	1	2	1	0	2	3	9
	2003	0	0	1	/	1	3	/	/
	2002	2	0	1	1	/	6	/	/

Vir: *Transatlantic Trends 2005* (2005), Topline Data, str. 17 . German Marshall Found of the United States, Washington D.C. (Dostopno tudi na http://www.transatlantictrends.org/doc/TTToplineData2005.pdf, 16. september 2005).

PRILOGA J: Število terorističnih napadov od leta 2000 do 2004 po posameznih preučevanih državah.



Vir: MIPT (2005), Terrorism Knowledge Base, A comprehensive Databank of Global Terrorist Incidents and Organisations. Olkohoma City. Dostopno na http://www.tkb.org/ChartModule.jsp (16. september 2005).

Podatke sem pridobila s pomočjo čarovnika, ki se nahaja na spletni strani MIPT. V treh korakih vpišemo podatke, ki jih želimo primerjati, za rezultat pa dobimo zgornji graf.