Revija za kriminalistiko in kriminologijo / Ljubljana 60 / 2009 / 3, s. 211-222

Uporaba interneta v teroristične namene

Matjaž Vidic*

Internet je lahko pripomoček pri izvajanju terorističnih napadov. Z razvojem informacijske družbe in naše odvisnosti od računalnikov, informacijskih sistemov in hitrih povezav, se odpira dodaten poligon za terorizem, internetni terorizem. Tehnološki napredek je tudi terorističnim skupinam omogočil dostop do skoraj vseh vrst orožja in teroristi so začeli uporabljati internetni prostor. Gre predvsem za širjenje informacij in globalno povezovanje celic terorističnih skupin. Internet se uporablja predvsem kot sredstvo za prenos informacij. Za teroristične skupine informacija pomeni moč. Z učinkovito uporabo občil lahko teroristične skupine vplivajo na javnost. Internet s svojimi značilnostmi omogoča terorističnim organizacijam širjenje novodobnih groženj. Omogoča jim takojšnjo svetovno razširjenost, predstavljanje njihovih organizacij in rekrutacijo »borcev«. Pri internetnem terorizmu gre torej za napade na računalniške sisteme, da bi se prizadejala škoda posameznikom in ne računalnikom. Države, ki povečujejo varnost, so že sprejele vrsto zakonskih določil, s katerim so omejile internetni kriminal in terorizem. Trenutno preiskovalci v večini varnostnih organov priznavajo, da je internetni terorizem za zdaj samo teoretični pojem, da možnosti uresničitve niso velike. Do zdaj se še ni zgodilo, da bi terorist kogar koli ubil s pomočjo računalniške tehnologije. Tudi pri svetovno najbolj znani teroristični organizaciji, Al Kaidi, med odkritjem baze, opremljene z visoko računalniško tehnologijo, niso odkrili dokazov, da bi organizacija s pomočjo računalnikov pripravljala resno uničevalno akcijo. Še več, računalniški strokovnjaki so prepričani, da je z uporabo interneta dejansko nemogoče povzročiti smrt posameznika, kaj šele večje skupine ljudi.

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

UDK: 004.738.5 : 323.283

1 Uvod

Z razvojem informacijske družbe in naše odvisnosti od računalnikov, informacijskih sistemov in hitrih povezav se odpira dodaten poligon za širjenje radikalnih idej, kot so internetni terorizem, separatistične težnje, razpihovanje rasne ali verske nestrpnosti ipd. Tehnološki napredek je tudi takim skupinam omogočil dostop do skoraj vseh vrst orožja. Gre predvsem za širjenje informacij in globalno povezanost celic terorističnih in drugih radikalnih skupin. Internet se uporablja predvsem kot sredstvo za prenos informacij. Informacija pomeni moč, z učinkovito uporabo občil lahko različne skupine vplivajo na javnost. Internet s svojimi značilnostmi omogoča radikalnim organizacijam širjenje novodobnih groženj. Ponuja jim takojšnjo svetovno razširjenost, možnost predstavljanja njihovih organizacij in rekrutacijo »borcev«. Države s povečano varnostno problematiko so že sprejele vrsto zakonskih določil, s katerim so omejile internetni kriminal in terorizem.

Ravno tako uporabljajo internet za širjenje idej in propagande tudi različne radikalne skupine, kot denimo protiglobalistična, separatistična, rasistična, nacionalistična gibanja ali subkulture. Internet se uporablja predvsem kot sredstvo za prenos informacij. Za radikalne skupine informacija pomeni moč. Množična občila poročajo predvsem o dramatičnih dogodkih. Vsak poskus ali dejanski teroristični napad občila obravnavajo kot »glavno novico«, kar radikalne skupine uporabljajo za pridobitev publicitete. Dramatičen dogodek je priložnost za javno predstavitev svojega obstoja ali pridobitev širše javne podpore.

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

* Matjaž Vidic, diplomirani politolog, višji kriminalistični inšpektor, Ministrstvo za notranje zadeve, Štefanova ulica 2, 1501 Ljubljana.

2 Terorizem

Danes je v svetovni javnosti – predvsem po zaslugi množičnih občil – terorizem kot oblika kriminalitete razvpit, čeprav nejasno opredeljen pojem. Že to, da obstaja veliko različnih opredelitev, kaže na zapletenost pojava. Opredelitev terorizma je veliko predvsem zaradi težav pri sami opredelitvi, deloma pa tudi zaradi nesoglasij o tem, kdaj bi bil lahko terorizem upravičen. V mednarodnem kazenskem pravu je sicer vse več dokumentov posebej namenjenih terorizmu, vključno s precejšnjim številom večstranskih pogodb, vendar se ti opredelitve terorizma sploh ne lotevajo ali ga opredeljujejo zgolj kot kakšno posebno pojavno obliko (Korošec in Bavcon 2003: 80).

V zadnjih letih se stopnjujejo argumenti za enotno opredelitev, čeprav nekateri strokovnjaki poudarjajo, da gre v celoti za politični pojem in enotna opredelitev s pravnega stališča ni potrebna. Razlogov, zakaj državam ne uspe sprejeti enotne opredelitve terorizma, je več. Da je ni, je za vlade pogosto prednost, ker jim omogoča, da oblikujejo svoje opredelitve glede na lastne politične in ideološke preference. Države pri opredelitvi terorizma poudarijo težnje, ki zaznamujejo njihovo zunanjo in notranjo politiko, neredko tako obračunajo s političnimi nasprotniki ali uveljavljajo državne gospodarske interese. Politično občutljivost opredelitve terorizma dodatno ponazarja dejstvo, da ga včasih enotno ne opredeljujejo niti v eni državi. Tako je v ZDA, kjer obrambno ministrstvo, FBI in zunanje ministrstvo terorizem opredeljujejo vsak po svoje (Hohler 2005: 6).

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

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

Teroristična kazniva dejanja ter temeljne pravice in načela

1. Vsaka država članica sprejme vse potrebne ukrepe, ki zagotavljajo, da se namerna dejanja, na katera se nanašajo spodnje točke a do i, in ki so po notranji zakonodaji določena kot kazniva dejanja, ki lahko zaradi svoje narave ali vsebine hudo škodujejo državi ali mednarodni organizaciji, kadar so storjena, da bi:

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

štejejo za teroristična kazniva dejanja:

a) napadi na človekovo življenje, ki lahko povzročijo smrt;
b) napadi na fizično nedotakljivost človeka;
c) ugrabitev ali zajetje talcev;
d) znatno uničevanje vladnih ali javnih objektov, prevoznega sistema, infrastrukture, vključno z informacijskim sistemom, pričvrščenih ploščadi, ki so na epikontinentalnem pasu, javnega kraja ali zasebne lastnine, ki lahko ogrozi človekovo življenje ali povzroči večjo gospodarsko izgubo;
e) ugrabitev letal, ladij ali drugih sredstev javnega ali tovornega prometa;
f) proizvodnja, posedovanje, nakup, prevoz, dobava ali uporaba orožja, razstreliva ali jedrskega, biološkega ali kemičnega orožja ter raziskave in razvijanje biološkega in kemičnega orožja;
g) spuščanje nevarnih snovi ali povzročanje požarov, poplav ali eksplozij, ki lahko ogrozijo človekovo življenje;
h) motnje v oskrbi z vodo, elektriko ali drugimi osnovnimi naravnimi viri, ki lahko ogrozijo človekovo življenje, ali prekinitve oskrbe z njimi;
i) grožnja, da bo storjeno katero od dejanj, naštetih v točkah a do h.

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

Etimološko beseda terorizem izhaja iz besede teror, ki je latinskega izvora in pomeni nasilje, strahovlado, izzivanje

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

strahu z nasilnim delovanjem, za katerim so politični cilji. Kot politični izraz se prvič pojavi v francoski revoluciji (jakobinski teror). Kot odziv na teror državne oblasti se konec 19. stoletja pojavi teror od »spodaj«, terorizem, ki postane v 20. stoletju tudi del strategije različnih narodnoosvobodilnih in gverilskih gibanj (npr. IRA) ter ideoloških skupin (RAF, Rdeče brigade itd.). Državni organizirani terorizem je bistvena značilnost totalitarnih sistemov 20. stoletja (fašizem, stalinizem) (Dolinar 1988: 1078).

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

Na drugi strani pa govorimo o nedržavnem oz. nevladnem terorizmu, ki je pravzaprav težka klasična nasilna kriminaliteta (zlasti zoper življenje in telo, zdravje, prostost, premoženje in splošno varnost) z nekaterimi posebnostmi na strani storilčevega motiva. Kot zelo standardno sestavino opredelitve terorizma, ki temelji na motivu storilca, sodobni teoretiki mednarodnega kazenskega prava navajajo povzročanje strahu v družbi. Podobno »povzročanje strahu v splošni javnosti, v skupini oseb ali pri posameznih osebah« najdemo tudi v opredelitvi terorizma v pozitivnem mednarodnem pravu, in sicer v deklaraciji Generalne skupščine ZN št. 49/60 iz leta 1994 o ukrepih za odpravo mednarodnega terorizma. O strahu – kot razlogu za dejanja teroristov – izrecno govori tudi točka b prvega odstavka 2. člena Mednarodne konvencije o zatiranju financiranja terorizma iz leta 1999.[2]

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

3 Kibernetični prostor[3]

Izraz kibernetični prostor (Cyberspace) je skoval pisatelj znanstvene fantastike William Gibson. V svojih delih ga je uporabil za oznako sveta, podobnega virtualni resničnosti, v kateri poteka interakcija človeških misli[4] (Ulčar 2002).

Kibernetični prostor ni prostor v klasičnem pomenu besede, saj nima ne razsežnosti ne drugih fizičnih značilnosti prostora. V pravu je kibernetični prostor konstrukt, ki so ga oblikovali ameriški pravni teoretiki in omogoča lažje reševanje pravnih vprašanj, povezanih z izmenjavo informacij po internetu. S pojmovno ločitvijo kibernetičnega prostora (torej prostora, v katerem potekajo interakcije med uporabniki interneta) in interneta (komunikacijskega omrežja, sestavljenega iz računalnikov in kablov) se lažje spopademo tudi s to problematiko (Ulčar 2002).

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

Za pravno pojmovanje je bistvena razlika med realnim in kibernetičnim prostorom odsotnost meja v kibernetičnem prostoru. Globalna oziroma brezmejna narava kibernetičnega prostora povzroča teritorialnim konceptom mednarodne pristojnosti velike težave. Težave pri določanju sodne pristojnosti namreč nastanejo, ko je treba neki sporni dogodek, ki se je zgodil povsod in nikjer hkrati, v teritorialno neomejenem kibernetičnem prostoru, povezati z določenim, na načelu teritorialnosti temelječim pravnim redom in tako rešiti pravni

---

[2] International Convention for the Suppression of the Financing of Terrorism, New York, 1999. Konvencija je začela veljati 10. aprila 2002, RS jo je podpisala 10. novembra 2001 in jo ratificirala leta 2004.

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

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

primer (npr. kibernetični spor). Povedano drugače, ali se zaradi nekrajevne oziroma vsekrajevne narave kibernetičnega prostora oseba, ki opravlja določeno dejavnost (najpogosteje gre za vzpostavitev spletne strani z neomejenim dostopom, na kateri so posamezne informacije), zaradi tega izpostavi sodni pristojnosti vseh držav, v katerih je mogoč dostop do spletne strani (Ulčar 2002)

Zaradi »nekrajevne« narave interneta je eno najzahtevnejših vprašanj, kako neko sporno elektronsko dejavnost povezati z območjem določenega sodišča (pri tem gre lahko tudi za notranjedržavno sodno razmejitev). Problem ponazarja povsem mogoč primer z interneta: katero pravo oziroma sodišče uporabiti, če nemški državljan v Mehiki napiše žaljivo sporočilo, ki se nanaša na norveškega državljana, sporočilo pa je bilo poslano s strežnika v ZDA in ga je prebral nekdo na Češkem (Toplišek 1997).

4 Internetni terorizem

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

Izraz internetni terorizem, ki se nanaša na zbliževanje kibernetičnega prostora in terorizma, je v osemdesetih letih prvi uporabil Barry Collin, starejši raziskovalni sodelavec z Inštituta za varnost in obveščanje v Kaliforniji (Institute for Security and Intelligence in California) (Denning 2000).

Pri informacijskem terorizmu gre torej za napade na računalniške sisteme, da bi se prizadejala škoda posameznikom in ne računalnikom. Značilnosti tega terorizma so potencialna velika učinkovitost v družbah, v katerih računalniški sistemi nadzorujejo večino posameznikovega življenja. To pomeni, da gre za nadzor nad različnimi državnimi podsistemi (zdravstvo, izobraževanje, poslovanje, sodni pozivi), ki so danes del kritične infrastrukture in njene zaščite. Zloraba takih podatkov bi lahko imela hude posledice in bi dejansko lahko ohromila normalno delovanje družb (Svete 2007: 128).

Na splošno lahko internetni terorizem opredelimo kot združitev terorizma in kibernetičnega prostora. To so nezakonite grožnje ali napadi na računalnike, mreže in informacije, ki so v njih shranjene, pod pogojem, da so izvedeni z namenom ustrahovati ali prisiliti vlado, da bi podpirala določene politične ali družbene cilje. Posledica napada mora biti nasilje nad ljudmi ali lastnino ali vsaj tolikšna škoda, da povzroča dovolj velik strah. Napadi, ki uničijo nepomembne službe ali povzročijo predvsem finančno škodo, niso dejanja informacijskega terorizma (Denning 2000 in 2001).

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

- IKT je močno zmanjšala čas prenosa informacij, kar omogoča medsebojno povezanost s hitro zunanjo in notranjo komunikacijo ter usklajevanje;
- uporaba kibernetičnega prostora omogoča prikrito komuniciranje in anonimnost;
- nove informacijsko-komunikacijske tehnologije so močno pocenile komuniciranje (npr. uporaba interneta je razmeroma poceni);
- IKT prispeva h krepitvi moči, zato se danes vse pogosteje poudarjata informacijska moč in prostor kot novi področji geopolitike;
- povezovanje računalništva in komuniciranja je bistveno povečalo obseg in zapletenost informacij;
- IKT teroristom omogoča, da dosežejo ciljno občinstvo tudi, kadar drugi mediji niso učinkoviti, hkrati pa tako dosežejo tudi novo občinstvo (mlade in izobražene) (Whine 1999 in Edwards in Zanini 2001).

5 Kibernetični prostor

5.1 Zgodovinski razvoj pojma računalniške kriminalitete

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

Zaradi vedno novih in novih oblik računalniškega kriminala se je pojavila potreba po njegovi opredelitvi. Tako je že leta 1983 skupina strokovnjakov OECD (Organisation for Economic Co-operation and Development – Organizacija za gospodarsko sodelovanje in razvoj) opredelila izraz »računalniški kriminal« kot »*vsako nezakonito, neetično ali neavtorizi-*

rano vedenje, ki zajema avtomatsko obdelavo podatkov in/ali prenos podatkov« (Seiber 1998: 20). Poznejše razlage pojma pa so šle še dlje z razvojem obsežnejšega pojma »*podatkovni in/ali informacijski kriminal*« (Seiber 1998: 21).

5.2 Računalniška kriminaliteta

Ne glede na prvotni namen računalništva (znanstveni in raziskovalni) je svojo priložnost v njem kaj hitro našel tudi kriminal. Njegovo zanimanje za izrabo zmogljivosti računalniške tehnologije, njegove povezave s komunikacijskim okoljem in vedno bolj imaginarnim spletnim okoljem postajajo vedno večje (Thackrah 2004).

Čeprav je večina razlag pojma kibernetične kriminalitete oziroma kriminalitete, povezane z računalniki, dokaj splošna, pa je verjetno prav v njihovi splošnosti mogoče najti širok spekter kriminalnih dejanj, ki jih ta pojem obsega. Tako David Wall v svoji konceptualizaciji kibernetične kriminalitete pravi, da je to pojem, ki zajema škodljivo vedenje, ki je na neki način povezano z računalnikom (Wall 2001: 2). Armstrong in Forde pa za kibernetični kriminal pravita, da je to »kriminal, ki je zagrešen s pomočjo interneta« (Armstrong in Forde 2003: 209). Grabosky in Smith računalniško kriminaliteto opredeljujeta kot t. i. digitalni kriminal, to pa je kriminal, ki obsega informacijske sisteme kot sredstva ali tarče nezakonitega delovanja (Wall 2001: 29).

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

Danes organizirane kriminalitete in nekaterih drugih vrst kriminalitete, kot so goljufije, bančne prevare, kraje avtorskih pravic, kriminaliteta z znaki diskriminacije, tatvin patentov ipd., da pornografske industrije, zlorab otrok, otroške pornografije sploh ne omenjamo, verjetno sploh ne bi bilo toliko, če ne bi pri svoji kriminalni dejavnosti uporabljale računalniške tehnologije in kibernetičnega prostora. Organizirane kriminalne združbe in posamezniki z različnimi interesi internet izrabljajo za širjenje internetnega vandalizma, razširjanje virusov in črvov, povzročanje velikanske gmotne škode z uničevanjem podatkovnih zbirk, z vsem tem pa povzročajo pravi tehnološki kaos.

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

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

Poskusi področij, kot so psihologija, politika in ekonomija, skušajo združiti prizadevanja, da bi se družba ozavestila in spoznala pretečo nevarnost v njenem pravem obsegu. Izražata se predvsem dva vidika, psihološki in tehnološki; prvi, naključnost izbire ciljne skupine žrtve, ki povzroča nenehno stanje negotovosti, in drugi, za izvedbo uporabljena tehnološka dognanja (Weimann 2004).

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

Ugotavljajo, da bi samo enodnevni izpad spletnega medmrežja v ZDA povzročil izpad 6,5 milijarde dolarjev prometa. Blagovni promet na spletnem medmrežju, IT-komunikacije, bančne komunikacije in finančne transakcije, sistem avtorizacije kreditnih kartic ipd. so osnovno gibalo ekonomije. Pomembnost informacij in s tem dostopa do njih je nepredstavljiva, njihova pomembnost pa skokovito narašča. Te potrebe narekujejo nenehen razvoj tehnologije, ki omogoča hitrejšo in učinkovitejšo uporabo računalniške infrastrukture, s tem pa se povečuje tudi njena ranljivost. Ob finančnem vidiku ne smemo pozabiti na psihološki učinek, ki ga pomeni nenehen strah, da bo uporabnik zlorabljen (Coleman 2005).

Ker gre pri virtualnem svetu in kibernetičnem okolju, ki bi lahko potencialno delovalo v njem ali proti njemu, za zelo kompleksno področje, na katerem se prepletajo različna področja elektronskih tehnologij, je treba opredeliti tudi do-

polnjujoče sisteme, prek katerih deluje računalniška kriminaliteta oz. terorizem. S tem se ukvarja t. i. Communication Intelligence. To je zelo občutljivo področje, ki ima bogato tradicijo v pretekli zgodovini nekaterih totalitarnih sistemov, ki so tako nadzirali vsak korak svojih državljanov, pa tudi v različnih kriznih obdobjih, kot je npr. hladna vojna, ko je bilo za nacionalno varnost ključnega pomena prestrezanje informacij, ki so jih vsebovala diplomatska sporočila (Vidic 2008).

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

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

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

6 Teroristična dejavnost v spletnem okolju

Teroristi informacijsko tehnologijo za svojo dejavnost uporabljajo na dva načina. Pri prvem gre za zlorabo informacijske tehnologije (svetovni splet in elektronska pošta na internetu) za podporo ali izvajanje teroristične dejavnosti. S pomočjo spletnih strani razširjajo ideološko propagando, novačijo nove pripadnike, pridobivajo finančna sredstva ter varno komunicirajo med seboj in med skupinami. Prav tako je internet izjemen pripomoček za pridobivanje podatkov, ki so pomembni za teroristično delovanje, pri tem pa omogoča anonimnost v različnih operacijah (Weiman 2004).

Druga oblika zlorabe informacijske tehnologije je uporaba tovrstne tehnologije za napad in vdor v informacijske sisteme različnih organizacij, varnostnih služb in vladnih organizacij, ki se borijo proti terorizmu. V tem primeru se informacijska tehnologija uporablja kot teroristično orožje ali kot objekt terorističnega napada. Poleg klasičnega napada na informacijske sisteme (uničevanje infrastrukture sistemov) teroristične skupine načrtujejo tudi informacijski napad z uporabo računalniških virusov, trojanskih konjev in logičnih bomb. Tako pri vdoru v informacijski sistem poskušajo uničiti čim več podatkov v kibernetičnem prostoru in s tem onemogočiti nemoteno delovanje dejanskega sveta. Tak napad gotovo pomeni veliko nevarnost, če bi nastal kaos v informacijskem sistemu, ki ureja zračni ali železniški promet, predvsem v trenutku, ko je varnost predvsem odvisna od informacijske tehnologije (vodenje letal ob pristanku, radarska zaznava letenja, usmerjanje prometa potniških vlakov …). Tarča tovrstnega terorizma pa so tudi poskusi blokad finančnih transakcij, bančnih sistemov in povzročanje zmede na svetovnih borzah (Vidic 2008).

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

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

Samo ZDA[5] so v preteklih nekaj letih zaznale številne poskuse vdora v računalniške sisteme ministrstva za obrambo in vladnih ustanov. V letu 1998 so zaznali 11 vdorov v ministrstvo za obrambo, v letu 2005 pa v povprečju ugotavljajo okoli 60 poskusov vdora oz. napada tedensko. Seveda gre večinoma za visoko usposobljene nadobudneže, pri katerih v ozadju ni terorizem ali kriminalna dejavnost, temveč osebni izziv ali lastno uveljavljanje. Je pa dovolj veliko opozorilo, da je treba računati tudi s t. i. informacijskim spopadom/napadom (*Information Warfare*), ki ga lahko izvedejo teroristi ali posamezne države (http://www.adl.org/terror/focus/16_focus_a2.asp).

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

6.1 Internetni terorizem

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

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

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

- zbiranje občutljivih podatkov o tarčah,
- zbiranje finančne podpore,
- povezovanje različnih skupin,
- izsiljevanje,
- propaganda,
- globalna svoboda,
- psihološki vplivi,
- goljufije in
- prikrite operacije (Thomas 2003).

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

- medsebojno komuniciranje,
- propagandna dejanja,
- zbiranje informacij,
- teroristični napadi z uporabo informacijskega orodja – orožja.

Prve tri oblike niso nujno uvod v informacijsko izveden teroristični napad, lahko so le pripravljalne stopnje v klasično teroristično dejanje. Pri terorističnih napadih z informacijskim orodjem – orožjem pa je nujen jasen cilj napada (npr. elektroenergetski sistem, prometni sistem, borza ...). Glavni cilj takega napada je onesposobitev ciljnega informacijskega sistema (Belič 2001: 263).

6.2 Značilnosti radikalnih islamističnih spletnih strani

Spletne strani z radikalnimi islamističnimi vsebinami pogosto spreminjajo spletne naslove, vsebina strani pa praviloma ostaja nespremenjena. Spletne strani radikalnih islamističnih skupin lahko razvrstimo po več merilih:

- strani, ki vsebujejo sestavine psihološke vojne – zastraševanja prebivalcev zahodnih držav;
- propagandne strani – poveličevanje boja proti Zahodu;
- zbiranje informacij – nekatere spletne strani so namenjene zbiranju informacij in idej (zaznali so stran, ki je zbirala podatke o veleposlaništvih ZDA po Evropi);
- iskanje somišljenikov – strani s širjenjem različnih idej;
- rekrutiranje – predvsem iskanje kandidatov za džihad;
- informativne strani – teh je veliko in vsebujejo podatke o izdelavi različnih eksplozivnih naprav, podatke o orožju, navodila za streljanje;
- strani o različnih načrtovanjih – predvsem grožnje, kaj se lahko zgodi, če Zahod ne bo končal gonje proti muslimanom (Vidic 2008).

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

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

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

6.3 Spletno okolje, uporabnost in priložnosti

Med terorizmom in spletnim okoljem sta dve temeljni povezavi. Spletno okolje postaja vse pomembnejše komuni-

kacijsko okolje, v katerem oz. prek katerega teroristi, logisti, simpatizerji idr. vpleteni zagotavljajo:[6]

- komuniciranje,
- načrtovanje napadov,
- pripravljalna dejanja.

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

Pri tem je treba opozoriti predvsem na prikritost delovanja, ki jo omogoča spletno okolje, nesledljivost zaradi množice komunikacij in prepletenosti z drugimi vrstami digitalne komunikacijske tehnike. Skrb vzbujajoča je prav tako možnost širjenja diskriminacijskih vsebin, ki pozivajo k nestrpnosti. Tu pa se seveda srečamo s področjem nasilne radikalizacije in rekrutiranja (Vidic 2008).

Spletno okolje s svojo dostopnostjo, uporabnostjo in prilagodljivostjo omogoča informacijsko disperzijo za iskanje novih rekrutirancev, nasilno radikalizacijo, terorističnim organizacijam omogoča dostop do informacij in s tem do sredstev, potrebnih za izvedbo akcij, in ne nazadnje si tako lahko pridobijo pomoč strokovnjakov s posameznih področij, kot je npr. izdelovanje eksplozivnih naprav ipd., ter se s tem izognejo dodatnemu tveganju, ki ga pomeni tovrstno usposabljanje (Vidic 2008).

Druga povezava pa pomeni spletno okolje kot sredstvo za izvedbo napada oz. cilj napada, kot smo to opisali v predstavitvenih poglavjih. Predvsem gre za dostop do podatkovnih zbirk ali njihovo uničenje, onesposobitev sistemov za upravljanje kritične infrastrukture, upravljanje sistemov za izvedbo napada ipd. (Vidic 2008).

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

Ena od najbolje tehnološko opremljenih skrajnih skupin[7] so nedvomno južnoameriška gverilska gibanja. Dokaz za to so skupine Zapatista v Mehiki, The Revolutionary Armed Forces of Colombia (FARC) v Kolumbiji ali pa npr. Shining Path (http://www.adl.org/terror/focus/16_focus_a.asp).

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

Obstaja še veliko drugih skrajnih skupin, ki tako uveljavljajo radikalne ideje, širijo večvrednostne ideje, pozivajo k nepokorščini in spodbujajo k nasilnemu sprevračanju obstoječih politik ali družbeno sprejemljivih in uveljavljenih sistemov. Zanimivo pri tem je, da ima večina teh strani vzpostavljene aktivne povezave s stranmi,[8] katerih vsebina se nanaša na orožje, eksplozive. Vsebina mnogih med njimi je sporna, nedovoljena ali celo prepovedana. Skladno z veljavno zakonodajo, ki se med državami razlikuje, bi se sicer taka stran morala ukiniti. Nekatere od teh strani delujejo le kratek, lahko tudi dogovorjen čas. Po ukinitvi strani se njihova vsebina objavi na drugi strani, pod drugim skrbnikom (Vidic 2008).

Največjo skrb danes vzbuja tudi poskus teroristov za pridobitev gradiva in tehnologije za izdelavo orožja za množično uničevanje (jedrskega, kemičnega, biološkega, radiološkega). Sestavine in način izdelave poskušajo pridobiti prek ponudnikov na spletnih straneh, na katerih je mogoče najti veliko navodil za izdelavo umazane bombe.[9] Nadzor nad spletnimi

---

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

[7] Za primerjavo: maja 1997 so npr. kolumbijskemu kartelu zasegli komunikacijsko tehnično opremo v vrednosti 10 mio. dolarjev.

[8] Za primer lahko navedemo Terrorist's Handbook ali The Anarchist Cookbook.

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

stranmi, ki ponujajo različne sestavine za izdelavo nevarnega orožja, je zato še posebej pomemben.

6.4 Ranljivost kritične infrastrukture

Kritična infrastruktura[10] skrbi za zagotavljanje temeljnih pogojev, potrebnih za nemoteno vsakodnevno življenje, je del tega sistema. Čeprav se zavedamo nevarnosti, ugotavljajo, da je 95 odstotkov vse infrastrukture, ki skrbi za zagotavljanje nemotene dobave plina, elektrike, vode in za telekomunikacijei, neustrezno zaščitenih (Ashenden 2002).

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

- elektrosisteme – prekinitev oskrbe z električno energijo ali motnje v oskrbi z njo; v krajšem ali daljšem časovnem obdobju je tak napad veliko verjetnejši kot nočna mora zaradi neposrednega napada na elektrarno, katere proizvodnja energije bi ušla iz nadzora; odgovor se skriva v tehnični rešitvi, saj so distribucijski in proizvodni sistemi popolnoma fizično ločeni;
- sisteme za oskrbo z vodo – računalniško nadzorovan sistem nadzora nad kakovostjo vode, čiščenja, prečiščevanja bi zlahka postal cilj, in sicer tako, da bi s pomočjo informacijske tehnologije ponastavili parametre vsebnosti kemičnih snovi;
- zemeljski plin, naftne derivate in maziva – večinoma se preigravajo scenariji izpustitve, motenj pri črpanju, distribuciji, požari in eksplozije …;
- sisteme kriznega reševanja – ob hkrati uprizorjeni nesreči bi onesposobili sistem kriznega reševanja, ki temelji na IKT in računalniški tehnologiji;
- finančne sisteme – po vsej verjetnosti bi bile še najhujše posledice ob napadu na pomembnejše finančne ustanove;
- sisteme javne uprave – napad na medmrežje javne uprave med volitvami ipd.

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

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

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

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

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

Sodobna družba deluje na način ravno take razsrediščenosti, prožnosti in nestalnosti, kar pa je zelo ploden teren tudi za delovanje in ohranjanje sodobnega političnega in gospodarskega sistema. Sodobna oblast ni več skoncentrirana v eni točki, temveč je mrežna, razpršena in tudi s pomočjo informacijsko-komunikacijske tehnologije povsod prisotna (Foucault 2000: 99). Vsekakor ne trdim, da ni mogoče prepoznati ključnih oziroma osrednjih protagonistov sodobne vladavine. Želim poudariti, da je s tem, ko ni enega vrhovnega suverena, ko sta glavno gibalo družbe gospodarska rast in optimizacija proizvodnih dejavnikov, ko je čut za socialna vprašanja zamenjal grob in neusmiljen boj za dobiček, rast ter napredek in s tem ko neoliberalna globalizacija (re)producira nove modele neenakosti na globalni ravni, ustvarjeno izjemno negotovo in odprto polje sil kot prostor za nastanek nenehne (globalne) ogroženosti, nevarnosti in vojne. Tukaj je tudi prostor za t. i. terorizem. V skladu z zgornjimi spremembami na družbenopolitični ravni pa sta se spremenila tudi delovanje in razumevanje vojne.

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

6.4.1 Modus delovanja

Internetni terorizem pri napadu na kritično infrastrukturo poskuša:

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

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

6.4.2 Kdo so mogoči storilci

Vprašanje je torej, kdo bi bil lahko internetni terorist. Medtem ko si večina še vedno zatiska oči pred resnico in zanika možnost katastrof, povzročenih z internetnim terorizmom, dejanska nevarnost in možnost uporabe skokovito naraščata. Trenutne ocene kažejo, da se tovrstna grožnja uporablja le za izvajanje pritiska na posamezne vlade (ne toliko zaradi tega, da bi državo popolnoma ohromili) in s tem povzročanje posebnih stanj med množicami, ki se počutijo ob tem nelagodno, povzroča strah med ljudmi, nezaupanje v programsko in strojno opremo, nezaupanje v delovanje sistemov ipd. (Vidic 2008).

Globalno gledano, preseki stanj in ocene tveganja kažejo, da je treba prednostno obravnavati mogoče uporabnike, kot so marginalne skupine, ki jih v tako dejavnost vodijo užaljenost ali za širše množice nerazumljiva ideološka prepričanja, npr. protikapitalistične skupine, skrajne skupine protiglobalističnih gibanj, okoljevarstveniki, zaščitniki pravic različnih manjšin ipd. Tovrstne ciljne skupine imajo največkrat omejeno količino ustreznega kadra in potrebne informacijsko-komunikacijske tehnologije, zato se predvidoma raje odločajo za napad na ranljivejše in nezaščitene cilje (Vidic 2008).

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

6.4.3 Predvidevanja

Pretekle izkušnje, obveščevalni podatki in ocene tveganja kažejo, da so teroristične skupine spoznale, da lahko tako izvajajo pritisk in teror na širše množice brez smrtnih žrtev. To jim omogoča bistveno prednost, saj ne izgubijo, vsaj ne v tolikšni meri, naklonjenosti okolja. Seveda ne smemo zanemariti ocene tveganja in presekov stanj, ki npr. za območje EU pristojnim telesom še naprej nalagajo večjo skrb za zaščito kritične infrastrukture.[11]

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

Če vzamemo pod drobnogled le območje EU, na katerem si trenutno prizadevajo za soglasje, ki bi omogočalo vzpostavitev in vzdrževanje sistemov zgodnjega obveščanja, zagotavljanje takojšnje pomoči ob naravnih in drugih nesrečah, vzpostavitev različnih mrež in povezav za zagotavljanje zgodnjega obveščanja, zagotavljanje takojšnje pomoči ob katastrofah ipd., vidimo, da je samo tu kar nekaj ciljnih točk, ki bi lahko postale primerno ranljive tarče.

Poleg tega je treba omeniti oskrbo z vedno bolj omejenimi naravnimi viri, kot so zemeljski plin in nafta, kmalu pa bo to postala tudi voda. Napad na infrastrukturo, ki omogoča nemoteno oskrbo z že tako nezadostnimi zmogljivostmi, bi pomenil hud udarec na svetovni ravni in ne le v državi ali regiji. Vdor v sistem nadzora nad prometno infrastrukturo bi lahko vodil v kaos (Vidic 2008).

Teroristi sicer uporabljajo internet kot podporo tradicionalnim oblikam terorizma, kot je na primer iskanje načinov izdelave eksplozivnih teles ali izvedba terorističnih napadov z njimi. Internet izkoriščajo tudi za vzpostavljanje spletnih strani, ki širijo njihove politične ali družbene cilje, pridobivanje novih članov, medsebojno komuniciranje in usklajevanje napadov.

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

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

7 Sklepne ugotovitve

Za teroristične skupine je uporaba nasilja zadnje sredstvo za dosego ciljev. Nasilni cilji so usmerjeni v prihodnost, pomenijo pa odgovor na neko preteklo nepravilnost (razpad sistema vrednot, družbene krivice ipd.). Sam terorizem je redkokdaj zadosten za uresničitev političnih ciljev. Pokazal

[11] Glej dokument The European Union Counter-Terrorism Strategy (14469/4/05).

pa se je kot zelo učinkovit dodatek v političnem sporu. V 20. stoletju se je izkazalo, da je z njim mogoče doseči zastavljene cilje, kar je tudi razlog za uporabo terorizma kot načina boja. Tudi večji teroristični napadi v zadnjih letih so z malo stroški dosegli veliko gospodarsko in politično škodo, predvsem pa zelo veliko publiciteto.

Vprašanje grožnje internetnega terorizma obstaja na dveh ravneh: ali so kritične infrastrukture, ki so mogoča tarča takih napadov, ranljive, in koliko so teroristi usposobljeni za tako vrsto terorizma. Kritične infrastrukture, kot so vojaška, letalska, medicinska, energetska itd., so ranljive do neke mere.

Teroristične skupine sicer uporabljajo internet kot podporo tradicionalnim oblikam terorizma, pri katerih se naučijo različnih načinov izvedbe terorističnega napada, kot so navodila za izdelavo eksplozivnih teles. Vzpostavljajo spletne strani, ki širijo njihove politične ali družbene cilje, pridobivajo nove člane, med seboj komunicirajo in usklajujejo napade. Trenutno preiskovalci v večini varnostnih organov priznavajo, da je internetni terorizem za zdaj samo teoretični pojem, da možnosti uresničitve niso velike.

Do zdaj se še ni zgodilo, da bi terorist kogar koli ubil s pomočjo uporabe računalniške tehnologije. Tudi pri svetovno najbolj znani teroristični organizaciji Al Kaidi ameriški vojaki med odkritjem baze, opremljene z visoko računalniško tehnologijo, niso odkrili dokazov, da bi organizacija s pomočjo računalnikov pripravljala resno uničevalno akcijo. Še več, računalniški strokovnjaki so prepričani, da je z uporabo interneta dejansko nemogoče povzročiti smrt posameznika, kaj šele večje skupine ljudi. Dorothy Denning (Schmit 2001: 70–105), ameriška profesorica in strokovnjakinja za kibernetično varnost, pravi: »Ponoči spim in me ni strah napadov iz navideznega sveta, ki bi mi lahko uničili življenje. Ne samo da se internetni terorizem ne uvršča med kemične, biološke ali jedrske napade, ampak ni niti približno podoben drugim mogočim fizičnim grožnjam, kot so avtomobilske bombe ali samomorilski bombni napadi.«

8 Literatura

1. Ashenden, D. (2002): Cyber terrorism & Threat to Critical National Infrastructures. **INTERSEC** 12. (11/12).
2. Armstrong, H.; Forde, P. (2003): Internet Anonimity Practices in Computer Crime. **Information Management & Computer Security** 11(5), 209–215.
3. Belič, I. (2001): Informacijski terorizem. **Varstvoslovje** 3(4), 262–268.
4. Cohen, F. (2003): **Cyber-Risk and Critical Infrastructures. Strategic Security Intelligenece, Cyberterrorism, The National Library of Essays in Terrorism**. London: Ashgate Publishing Limited.
5. Coleman, K. (2005): Cyber Terrorism. Dostopno na http://www.crime-research.org/library/Cyberterrorism.html (1. maj 2006).
6. Denning, D. E. (2000): Cyberterrorism. Dostopno na http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html (20. november 2003).
7. Denning, Dorothy E. (2001): Activism, Hacktivism, and Cyberterrorism: The internet as a Tool for Influencing Foreign Policy. Dostopno na http://www.rand.org/publications/MR/MR1382/MR1382.ch8.pdf (20. november 2003).
8. Deluze, G.; Guattari, F. (2000): **Micelij.** Koper: Hyperion.
9. Dolinar, K. (1998): **Leksikon Cankarjeve založbe – dopolnjena 5. izdaja**, 1078. Ljubljana, Cankarjeva založba.
10. LIBICKI, Martin (1995): *What is Information Werfare*? Dostopno na http://www.iwar.org.ukIiwar/resources/nduIinfowar/contents (24. marec 2007).
11. Littlejohn Shnider, D. (2002): **Scene of the Cybercrime: Computer forensics Handbook**. Rocklan, Rockland Syngress.
12. Foucault, M. (2000): **Zgodovina seksualnosti 1 – volja do znanja**. Ljubljana, ŠKUC.
13. Haraway, D. (1999): **Opice, kiborgi in ženske – reinvencija narave**. Ljubljana, ŠOU, Študentska založba.
14. Hohler, B. (2005): Problem definicije terorizma, **Pravna praksa** 33, 6–15.
15. Korošec, D.; Bavcon, L. (2003): **Mednarodno kazensko pravo – Posebni del**. Ljubljana: Pravna fakulteta.
16. Martonoši, P. (1993): Kriminaliteta v zvezi z računalniki v novi slovenski kazenski zakonodaji. **Podjetje in delo** 1993 (5/6), 489–500.
17. Pollit, M. M. (1997): Cyberterrorism – Fact or Fancy? Dostopno na http://www.cs.georgetown.edu/~denning/infosec/pollit.html (20. november 2007).
18. Prezelj, I. (2006): Teroristično ogrožanje nacionalne varnosti Republike Slovenije. Dostopno na http://www.sos112.si/slo/tdocs/ujma/2006/prezelj.pdf (12. december 2007).
19. Schmit, A. P. (2001): **Countering Terrorism through International Cooperation**. Dunaj, Transnational.
20. Seiber, U. (1998): **Legal Aspects of Computer-Related Crime in the Information Society** – COMCRIME – Study. Prepared for the European Commision by University of Wurzburg.
21. Thomas, D. (2003): Al Qaeda and the Internet: The Danger of »Cyberplanning«. Dostopno na http://carlistewww.army.mil/usawc/Parameters/03spring/thomas.pdf (1. december 2004).
22. Thacjrah, J. R. (2004): **Cyber-terroris***m*. Dictionary of Terrorism. London, Routledge.
23. Toplišek, J. (1998): **Elektronsko poslovanje**. Ljubljana, Založba Atlantis.
24. Ulčar, M. (2001): Mednarodna pristojnost in kiberprostor. **Pravna praksa** 2001 (8), 21–34.
25. Vidic, M. (2008): **Uporaba interneta v teroristične namene**. Diplomska naloga, FDV.
26. Wall, S. David (2001): **Crime and the Internet**. London, Routledge.
27. Whine, M. (1999): Cyberspace, A New Medium for Communication, Command and Control by Extremists. Dostopno na http://www.ict.org. il/articles/articledet.cfm?articleid=76 (6. julij 2008).
28. Weimann, G. (2004): Cyberterrorism: How Real Is the Threat? Dostopno na http://www.usip.org/pubs/specialreports/sr119.html (1. maj 2006).
29. Zanini, M.; Edwards, S. (2001): The Networking of Terror in the Information Age. Dostopno na http://www.rand.org/publications/MR/MR1382/MR1392.ch2.pdf (6. julij 2008).

30. Anti-Defamation League (2007). Terrorist Activities in the Internet. Dostopno na http://www.adl.org/terror/focus/16_focus_a.asp (21. marec 2007).
31. **ODS:** «Hacker's guide to protect your Internet Network« (Hekerjev vodnik za zaščito interneta). Dostopen na www.ods.com.ua/win/eng/security/max_security (26. februar 2007).

The use of the internet for terrorist purposes

Matjaž Vidic, A Graduate of Political Science, 1000 Ljubljana, Slovenia

The internet can be used as a tool for terrorist attacks. The development of the information society as well as our dependence on computers, information systems and rapid connections, have paved the way to terrorism and cyber terrorism. Technological progress has allowed terrorist groups the access to almost all kind of weapons and they have also begun to use cyber space. They use it basically for the dissemination of information and making global links between terrorist group cells. The internet is used above all as a medium for the transmission of information. Information is a kind of power for terrorist groups and with effective use of the media, they can have an impact on the general public. The internet, with its characteristics, enables terrorist organisations to spread contemporary threats. It enables an immediate global spread of threats, the promotion of their organizations and the recruitment of "fighters". Internet terrorism means basically attacks on computer systems with the purpose of harming individuals and not computers. Countries trying to increase security have already adopted a range of legal regulations with a view to restricting internet crime and terrorism.

In the majority of security agencies, investigators admit that internet terrorism has been until now only a theoretical concept and that the possibilities of its realization are not at this moment large. Nobody has yet been killed by a terrorist using computer technology. Even in the world's best known terrorist organization, Al Kaida, no evidence has been found that the organization has prepared serious destructive action, when their bases, equipped with high computer technology, have been discovered. Furthermore, computer experts are almost certain that it is practically impossible to cause the death of an individual by the use of the internet, and even less the death of a large group of people.

Keywords: internet, terrorism, technology, safety, threats

UDC: 004.738.5 : 323.283