INFORMACIJSKE RAZSEŽNOSTI SODOBNEGA TERORIZMA – TEORETIČNA VPRAŠANJA IN PRAKTIČNI VIDIKI

Information dimensions of contemporary terrorism-theoretical dilemmas and practical aspects

Uroš Svete* **UDK 323.28:659.4**

Povzetek

Kljub temu, da so se spori glede opredelitve terorizma prenesli tudi na njegov informacijski vidik, pa le-ta predstavlja za varnostni sektor (zahodnih) držav vse večji izziv in grožnjo. Zaradi odvisnosti (zahodnih) družb in njihovih podsistemov od informacijsko-komunikacijskih tehnologij naj bi namreč predstavljal najsodobnejšo in tehnološko najbolj sofisticirano obliko, kako med prebivalstvom sejati strah pred teroristično grožnjo, saj naj bi bilo mogoče z informacijskimi tehnologijami prebivalstvo fizično ogrožati. Vendar pa imamo v praksi izredno malo (dokazanih) primerov informacijskega terorizma, zato se med številnimi avtorji celo postavlja vprašanje, ali ne gre zgolj za še eno varnostno temo, ki jo določa vsesplošna vojna proti terorizmu. Kar zadeva fizično nasilje lahko vsekakor soglašamo s skeptiki, da o informacijskem terorizmu ne moremo govoriti dotlej, dokler ne bodo zaradi terorističnih napadov na kritično informacijsko infrastrukturo dejansko ogrožena življenja in premoženje prebivalstva ter moteno normalno delovanje temeljnih družbenih procesov. Po drugi strani pa je jasno, da brez medijev in danes še kako pomembnih interaktivnih informacijsko-komunikacijskih tehnologij tudi o terorizmu ni mogoče govoriti, saj so mediji tisti, ki v javnosti zbujajo občutek ogroženosti s terorističnimi napadi. Nenazadnje pa se je treba zavedati, da postaja internet vse pomembnejše sredstvo teroristov za pridobivanje informacij, širjenje propagande, medsebojno komuniciranje in načrtovanje operacij. Tako je postala informacijska tehnologija zaradi svoje splošne navzočnosti in nizkih vstopnih stroškov sredstvo in cilj terorističnega delovanja.

Abstract

Although there are also analytical and theoretical disagreements regarding the definition of terrorism as well the concept of information terrorism, terrorism and its information aspects have undoubtedly become increasingly important to the western security threat assessment. Western society's dependence on information technology and infrastructure is supposed to be exploited by contemporary terrorists to sow terror, fear and a feeling of threat. In a fundamental sense, (information) terrorists could even have so physical effects as well collateral damage should be caused. Is in consequence information terrorism hype or reality? In terms of physical violence, one would have to agree with the sceptics who say that we cannot talk of information terrorism until life or property, or the normal functioning of basic social processes, are actually threatened by a terrorist attack on critical information infrastructure. In terms of fear and the psychological aspects of the terrorist threat, it is clear that terrorism could not exist without (interactive digital) media coverage. Last but not least, we should also be aware that the internet is becoming an ever more important tool in the hands of terrorists for gathering information, spreading propaganda, fundraising and operation and coordination management. The cheapness and diffusion of information technology means that it has become simultaneously the tool and target of terrorist activities.

Uvod

Čeprav je terorizem v obdobju po hladni vojni gotovo postal najpomembnejša varnostnopolitična tema ne samo v zahodnih državah, temveč povsod po svetu tudi v državah, ki sicer neposredno niso ogrožene, se analitiki pri njegovem obravnavanju strinjajo zgolj v neobstoju

* Dr., Univerza v Ljubljani, Fakulteta za družbene vede, Katedra za obramboslovje, Obramboslovni raziskovalni center, Kardeljeva ploščad 5, Ljubljana, uros.svete@fdv.uni-lj.si

splošno sprejete opredelitve, kaj terorizem sploh je. Ne glede na to, da se pojem zgodovinsko povezuje predvsem s francosko revolucijo[1], pa večina opredelitev izpostavlja predvsem uporabo sile/nasilja z namenom ustrahovati prebivalstvo, ki naj bi na ta način spremenilo svoj odnos do posameznih (zlasti varnostnih, obrambnih in zunanjih) politik določene države. Vendar se glavna težava pojavi šele tedaj, ko je treba opredelitev praktično uporabiti v sodobnih konfliktih. Enako lahko ugotovimo tudi za informacijski terorizem, ki naj bi bil zlasti zaradi odvisnosti (zahodnih) družb od informacijsko-komunikacijskih tehnologij najsodobnejša in tehnološko najbolj sofisticirana oblika, kako med prebivalstvom sejati strah, v bistvu pa naj ne bi bilo mogoče z informacijskimi tehnologijami prebivalstvo fizično ogrožati. Toda ali to drži? Glede nasilja soglašamo s skeptiki, da o informacijskem terorizmu ne moremo govoriti vse dotlej, dokler ne bodo zaradi terorističnih napadov na kritično informacijsko infrastrukturo fizično ogrožena življenja in premoženje prebivalstva ter moteno normalno delovanje družbe, kar pa se na srečo še ni zgodilo (seveda neobstoj tovrstnih napadov ne pomeni, da tehnično niso mogoči in izvedljivi)[2]. Glede ustrahovanja pa je jasno, da brez medijev in danes še kako pomembnih interaktivnih informacijsko-komunikacijskih tehnologij tudi o terorizmu ni mogoče govoriti. Kajti šele medijsko posredovanje in prikaz terorističnih dejanj omogoči povzročitev občutka strahu in zaznavo ogroženosti, ki je mnogo večja kakor kažejo empirični podatki o številu žrtev ali poškodovanih v napadih. Zato soglašamo s tistimi analitiki, ki poudarjajo predvsem informacijsko-komunikacijske tehnologije, ki jih teroristi uporabljajo za izvajanje pritiska in propagando, namenjeno nasprotnikovi javnosti, in mobiliziranje ter rekrutiranje novih podpornikov. Za razliko od tradicionalnih, komunikacijsko enosmernih medijev, je internet kot najzmogljivejše komunikacijsko sredstvo vse pomembnejši tudi za medsebojno komuniciranje in načrtovanje operacij prostorsko in organizacijsko decentraliziranih terorističnih organizacij, ki so danes vse prej kot hierarhično in centralizirano organizirane (glej shemo 1). Ne glede na analitično izhodišče in odprta vprašanja, pa je nesporno dejstvo, da informacijsko-komunikacijske tehnologije postajajo sredstvo in hkrati cilj terorističnega delovanja.

[1] Sama beseda terorizem izhaja iz francoščine (terreur), kjer je označevala metodo eno 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: 154).

[2] Ameriško Ministrstvo za domovinsko varnost je sicer že večkrat objavilo sporočila, da teroristična mreža Al Kaida pripravlja napade na ameriške finančne ustanove (predvsem borzo), ki večinoma poslujejo elektronsko. Vendar zankrat ni dokazov, da je sodobni kibernetski kriminal povezan s terorizmom. Problem je namreč v tem, da je zloraba informacijsko-komunikacijskih tehnologij anonimna, terorizem pa nasprotno potrebuje odmevnost in javno pozornost.

Varnostnopolitični pomen informacijsko-komunikacijske tehnologije

Sodobna družba je že med naftno krizo v 70. letih prejšnjega stoletja spoznala, da bistveno ogrožanje varnosti ni nujno povezano z vojaškim delovanjem in oboroženimi spopadi, kjer bi imele nosilno in odločilno vlogo oborožene sile nacionalnih držav. Omenjena ugotovitev je postala še aktualnejša po koncu hladne vojne, ko sta varnostna teorija in praksa vse pogosteje izpostavljali t. i. nove in netradicionalne varnostne akterje in njihova delovanja (primer terorističnih skupin, organiziranega mednarodnega kriminala ipd.). Čeprav gre sicer za zelo različne akterje, pa je v njihovem delovanju mogoče najti tudi skupne imenovalce. Prvi je nedvomno asimetričnost, kajti sodobni viri ogrožanja bodo vse bolj temeljili na prepoznanju šibkosti možnega nasprotnika, pri čemer bo napaden najšibkejši člen v verigi, katerega onesposobitev lahko povzroči največjo škodo (na način analize stroškov in koristi). Pomembno je opozoriti tudi na tendenco zniževanja stroškov in uporabljenih virov, pridobivanje napadalnega potenciala in sredstev za izvajanje operacij. Obratnosorazmerno z zniževanjem uporabljenih virov se povečuje težnja k povečanju učinkov, kolikor je seveda v dani situaciji uresničljiva, glavni povečevalec učinkov v sodobni družbi pa so (interaktivni) mediji, brez katerih tudi terorizma – ustrahovanja prebivalstva z namenom spremeniti njegovo podporo določeni politiki – ne bi bilo. Nenazadnje pa je treba izpostaviti tudi zaščitne mehanizme pred odkritjem in protiukrepe, ki bi jih izvedli napadeni (ta ugotovitev ne velja oz. velja samo v omejenem pomenu za samomorilske teroristične napadalce).

Zlasti po 11. septembru 2001 se je med varnostnimi strokovnjaki okrepilo mnenje, da bodo informacijski sistemi ena od naslednjih tarč teroristov (informacijski terorizem – Cyberterrorism) (Weimann, 2005). Po drugi strani se soočamo tudi z dinamično globalizacijo informacijskih družb, ki v povezavi s tehnološkimi izboljšavami (npr. lokalne brezžične povezave) povečuje možnosti medsebojnega povezovanja, množično širjenje storitev in uporabnikov pa povečuje tudi ranljivost in ogroženost, ki se je večina med njimi sploh ne zaveda. V poročilu ameriškega sveta za znanost in tehnologijo Federal Plan for Cyber Security and Information Assurance Research and Development so tako opredelili naslednje tehnološke trende, ki povzročajo skrbi in povečujejo ranljivost informacijske infrastrukture (http://www.nitrd.gov/pubs/csia/FederalPlan_CSIA_RnD.pdf (03.05.2006)):

- Vse večja kompleksnost informacijskih sistemov predstavlja varnostni izziv za razvijalce in uporabnike.
- Razvoj telekomunikacijske infrastrukture, ko se tradicionalni telefonski sistem in informacijska tehnologija vse bolj združujeta v enotno platformo.
- Vse hitrejša širitev brezžičnih komunikacijskih sistemov zelo povečuje možnosti zlorab. V tem primeru namreč tradicionalni obrambni pristop

(securing the perimerer) ni učinkovit, saj nimamo fizičnega nadzora nad uporabniki in napravami.
- Vse večja prepletenost in dostopnost na računalnikih temelječih sistemov, ki postajajo kritični oz. ključnega pomena za ekonomijo, logistiko, razširjanje dobrin in storitev.
- Globalnost informacijsko-komunikacijske tehnologije povečuje število nasprotnikov za uporabnike v domačem in mednarodnem prostoru.

Hutter (2002:7-8) v svoji analizi faktorjev tveganja na področju informacijske infrastrukture dodaja še zelo kratke inovacijske cikle razvoja informacijsko-komunikacijskih tehnologij, njihovo vsesplošno razširjenost in dostopnost, posebej pa je treba izpostaviti raznovrstnost možnih napadalcev (od terorizma do industrijskega vohunjenja in posameznikov z različnimi interesi). Pravna in zakonodajna podlaga sta v večini držav na trhlih in nedorečenih temeljih, prav tako pa so nejasne pristojnosti in odgovornosti ob napadu na kritično informacijsko infrastrukturo.

Informacijski terorizem — opredelitev pojma

Informacijski terorizem nekateri avtorji vključujejo v okvir informacijskega bojevanja, drugi pa menijo, da je informacijsko bojevanje popolno teroristično orožje (Shahar, 1997). Teroristi danes vse pogosteje uporabljajo IKT za organiziranje, motiviranje, komuniciranje, vpliv na domačo in mednarodno javnost ter za izkoriščanje ranljivosti informacijsko razvitih držav (glej sliko 1). Zato danes vse pogosteje govorimo o informacijskem terorizmu in informacijskih vidikih sodobnega terorizma. Izraz informacijski terorizem, ki se nanaša na zbliževanje kibernetskega prostora in terorizma, je v 80. letih prejšnjega stoletja prvi uporabil Barry Collin, raziskovalni sodelavec Inštituta za varnost in obveščevalno dejavnost v Kaliforniji (Institute for Security and Intelligence in California) (Denning, 1999).

Izraz informacijski terorizem ali kibernetski terorizem, kakor ga nekateri imenujejo, se torej nanaša na dva pojma, in sicer na kibernetski prostor in virtualni svet ter terorizem. Collin virtualni svet opredeljuje kot »kraj, kjer računalniški programi delujejo in se podatki premikajo« (Collin v Politt, 1997).

Kljub težavam pri opredeljevanju terorizma in je soglasje težko doseči, različnih opredelitev ne primanjkuje. 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 javnosti« (Ministrstvo za zunanje zadeve ZDA v Politt, 1997). S kombiniranjem zgornjih dveh opredelitev je Politt opredelil informacijski terorizem takole: »Informacijski terorizem (kibernetski terorizem) je naklepni, politično motivirani napad nedržavnih skupin in tajnih agentov, katerega cilj so informacije, računalniški sistemi, računalniški programi in podatki, rezultat tega napada pa je nasilje nad civilnimi tarčami (Politt, 1997). Politt tudi meni, da informacijski teroristi za doseganje svojih ciljev uporabljajo (vsaj zaenkrat) neubojno (ang. soft power) nasilje, ki deluje predvsem psihološko (Politt, 1997), to je na zavest ljudi.

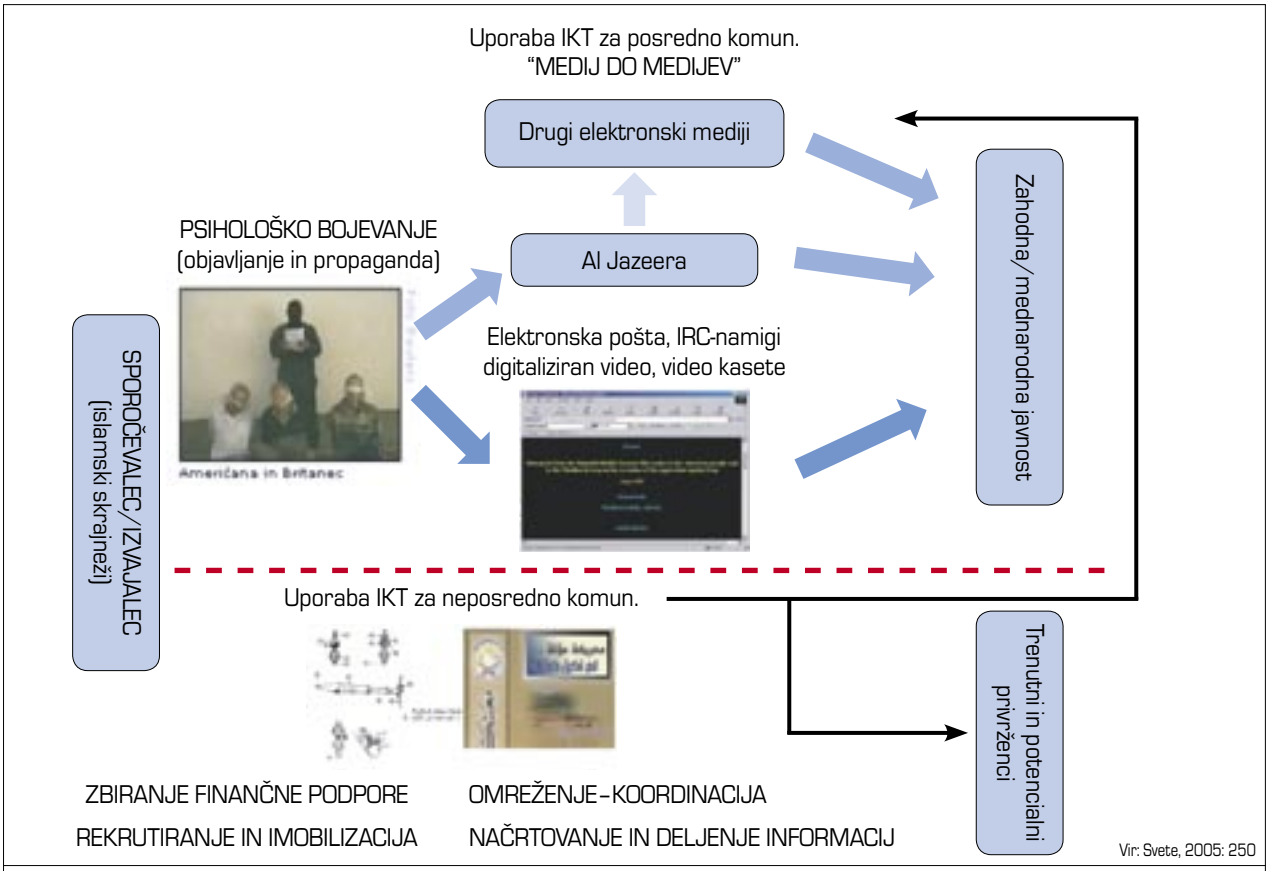
Podobno opredelitev uporablja Dorothy E. Denning (glej Denning 1999, 2000a, 2000b, 2001). Denningova meni, »da je kibernetski terorizem zbliževanje kibernetskega prostora in terorizma. Nanaša se na nezakonite napade ali grožnje z napadi na računalnike, omrežja in informacije, shranjene v njih, z namenom prestrašiti ali siliti vlado in ljudi v podporo političnim ali družbenim/ideološkim 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[3] so prav tako lahko dejanja informacijskega terorizma, vendar je to odvisno od njihovega vpliva. Medtem pa napadi, ki uničijo nebistvene službe ali

[3] Kritično infrastrukturo predstavljajo energetsko omrežje, komunikacijska infrastruktura, prometna infrastruktura in finančna infrastruktura (Lewis, http://www.fas.org/irp/eprint/snyder/infowarfare. htm).

		Cilj	
		fizičen	digitalen
orodje	fizično	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).
	digitalno	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?, v: Sun Tzu Art of War in Information Warfare.

Preglednica 1. Metode terorističnega napada
Table 1. Methods of terrorist attack



Slika 1. Informacijsko-komunikacijske tehnologije, ki jih uporabljajo teroristi
Figure 1. Use of information and communication technology by terrorists

povzročijo predvsem finančno škodo, niso dejanja informacijskega terorizma« (Denning 2001).

Devost, Houghton in Pollard informacijski terorizem opredeljujejo z metodami informacijskega napada. Avtorji menijo, da v družbah tretjega vala – t. j. informacijskih družbah, obstajata dve ključni metodi informacijskega terorističnega napada:

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

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

Druga metoda vključuje manipuliranje in izkoriščanje informacijskih sistemov, spreminjanje ali krajo podatkov ali prisiljenje sistema, da opravlja funkcije, za katere ni namenjen (Devost in drugi, 1997—1998).

Točka a v preglednici 1 predstavlja klasični (konvencionalni) terorizem (ugrabitve letal, zajemanje talcev, bombni napadi, umori, ipd). Točke b, c in d predstavljajo informacijski terorizem, točka d pa je po mnenju avtorjev t. i. »čisti ali fundamentalni« informacijski terorizem, ki ga je najtežje odkriti in se proti njemu boriti (Devost in drugi, 1997—1998). Denningova celo meni, da neobstoj takšnih terorističnih napadov zanika koncept informacijskega terorizma.

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

Uporaba informacijsko komunikacijske tehnologije pri terorizmu

Številne teroristične organizacije vse pogosteje uporabljajo IKT za boljšo organizacijo in uskladitev dejavnosti. Teroristi uporabljajo IKT zaradi različnih vzrokov, kakor so izboljšane komunikacije in podpora organizaciji, prav tako pa njenim članom dopušča hitro usklajevanje z velikim številom privržencev in predstavlja podlago za propagando in protipropagando ter prenos kodiranih sporočil,

pri čemer uporabljajo javno dostopno kodirno opremo in izvajanje napadov za ohromitev nasprotnikovih informacijskih sistemov (virusi in metode DoS[4]). IKT omogoča teroristom, da širijo svoje ideje in dosežejo krog možnih donatorjev ter novih privržencev povsod po svetu (Terrorism files org, 2002; Weimann, 2006), po drugi strani pa lahko vplivajo na mednarodno in nasprotnikovo javnost posredno in neposredno[5] (glej sliko 1).

Uporaba IKT teroristom omogoča številne prednosti, najpomembnejše pa so naslednje:

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

Zaninijeva in Edwards trdita, da IKT omogoča teroristom tri glavne načine dejavnosti, in sicer propagandne dejavnosti, napade na virtualne tarče z namenom motenja in ne uničenja ciljnega informacijskega sistema ter fizično uničenje tarče (klasični informacijski terorizem) (Zanini in Edvards, 2001).

Sklepne misli

Informacijski terorizem predstavlja varnostnemu sektorju (zahodnih) držav vse večji izziv in grožnjo. Najnižje oblike informacijskega terorizma po uničevalnosti so t. i. elektronske bombe in napadi prek elektronske pošte na uporabnike interneta. Višje oblike 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 merilom informacijskega terorizma. Vsi dosedanji informacijski napadi so kvečjemu prestrašili žrtve, nobeden pa ni vodil v nasilje ali poškodovanje ljudi, kakor predvideva zgoraj zapisana delovna opredelitev informacijskega terorizma. Najbližje merilu informacijskega terorizma je bil tako napad z elektronsko pošto teroristične skupine Tamilski tigri na veleposlaništvo Širilanke (Denning, 2000a).

Neobstoj empiričnih primerov dokazuje, da je grožnja informacijskega terorizma zgolj teoretična, vendar kljub temu vredna pozornosti. Za razumevanje možne grožnje informacijskega terorizma je treba upoštevati dva ključna dejavnika: ali obstajajo tarče, ki so ranljive za napad, ki vodi v nasilje ali resno škodo, in ali obstajajo sposobni in motivirani akterji za izvajanje dejanj informacijskega terorizma. Glede ranljivosti tarč lahko ugotovimo, da so številne študije in vaje kriznega upravljanja pokazale, da je kritična informacijska infrastruktura potencialno ranljiva za informacijski teroristični napad. Kar zadeva sposobne in motivirane akterje, je tako, da imajo mnogi hekerji znanje, veščine in orodja, primanjkuje pa jim motivacije za povzročanje nasilja in resne škode ekonomskemu ali socialnemu sistemu, medtem ko imajo teroristi motiv, vendar so, vsaj zaenkrat, še brez zadostnega znanja in veščin za takšen napad[6].

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

Kljub pomanjkljivostim informacijskega terorizma mu je vseeno treba posvečati pozornost. Nova generacija teroristov raste v digitalnem svetu, zato bo razpolagala z večjim informacijskim znanjem in veščinami in s še močnejšimi ter lažje uporabljivimi hekerskimi orodji, ki bodo pomenili več možnosti za informacijski terorizem kakor današnji teroristi. Lahko pričakujemo tudi, da se bosta v prihodnosti resnični in virtualni svet zelo zbližala z velikim številom naprav, povezanih v internet, in takrat bo informacijski terorizem postal privlačnejši.

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

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

[4] Denial of service – napadi za onesposobitev storitve.

[5] Neposredni vpliv imajo predvsem preko spletnih strani ter avdio in video objav, od izjav do napadov, v posredno pa gre za vpliv na tradicionalne medije, kakor so npr. televizijske postaje, ki kot vir za svoja poročila zelo pogosto uporabljajo spletna mesta, ki jih uporabljajo ali vzdržujejo teroristične organizacije in njihovi podporniki.

[6] Danes je vse več poročil o vedno bolj sofisticirani uporabi IKT, ki jih uporabljajo teroristične organizacije (tako naj bi Hesbollah med zadnjimi spopadi z Izraelom vdrl v komunikacijski sistem izraelskih oboroženih sil), prav tako pa se v islamskem svetu vse pogosteje govori o t. i. **infojihadu kot uporabi IKT za potrebe svete vojne** (Golpira, 2006).

podatkov o tarčah, zbiranje finančne podpore, povezovanje različnih skupin, izsiljevanje, propaganda, globalna svoboda[7], psihološki vplivi, goljufije in prikrite operacije (Thomas, 2002; glej tudi sliko 1). Podobno tudi Belič v informacijskem pomenu loči štiri oblike delovanja terorističnih organizacij: medsebojne komunikacije, propagandna dejanja, zbiranje informacij, teroristični napadi z uporabo informacijskih orodij – orožij. Prve tri oblike niso nujno uvod v informacijsko izveden teroristični napad, so lahko le pripravljalne stopnje v klasično teroristično dejanje. Pri terorističnih napadih z informacijskimi orodji—orožji pa je nujen jasen cilj napada (npr. elekroenergetski sistem, prometni sistem, borza,...) Osnovni cilj takšnega napada je onesposobitev ciljnega informacijskega sistema (Belič, 2001:263).

Teroristične organizacije kibernetski prostor uporabljajo predvsem za pospeševanje, olajševanje klasičnih oblik terorizma, kakor 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, usklajevanje dejavnosti, ipd. Internet torej teroristične organizacije uporabljajo predvsem za izvajanje propagande in protipropagande, za prenos kodiranih sporočil in izvajanje napadov za ohromitev nasprotnikovih informacijskih sistemov, kajti teroristom omogoča anonimnost, hkrati pa predstavlja učinkovito sredstvo poveljevanja in nadzora, usklajenost in možnosti povezanega napada.

Viri in literatura

1. Belič, I., 2001. Informacijski terorizem. V: Varstvoslovje let. 3/št. 4. Ministrstvo za notranje zadeve RS, Visoka policijsko-varnostna šola, 262–268.
2. Denning, D. E., 1999. Information warfare and security. Berkeley, Sidney, Bonn: addison-wesley.
3. Denning, D. E., 2000a. Cyberterrorism. V: Global Dialogue, dostopno tudi: http://www.cs.georgetown.edu/~denning/infosec/cyberterror-GD.doc (9. 11. 2004).
4. Denning, D. E., 2000b. Testimony before the Special Oversight Panel on Terrorism. U.S. House of Representatives, Committee on Armed Services (23 May), dostopno: http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html (09. 11. 2004).
5. Denning, D. E., 2001. Is Cyber Terror Next? New York: U.S. Social Science Research Council, (1. novemeber 2001) dostopno: http://www.ssrc.org/sept11/essays/ denning.htm (9.11.2004).
6. Devost, M. G., 1995. National Security in the Information Age, dostopno: http://www.devost.net/papers/national_security_in_the_information_age.html (09. 10. 2006).
7. Devost, M., Houghton, B. in Pollard, N., 1997–1998. Information Terrorism: Can You Trust Your Toaster? V: Sun Tzu Art of War in Information Warfare.
8. Golpira, H., 2006. Info jihad. Tehran Times.com, 08. 04. 2006. http://www.tehrantimes.com/Description.asp?Da=4/8/2006&Cat=14&Num=001 (15. 4. 2006).
9. Golubev, V., 2003. Cyberterrorism - the new side of terrorism. Computer Crime Research Center, 21. jul., dostopno: http://www.crime-research.org/news/2003/07/Mess2102.html, (25. 09. 2006).
10. Hutter, R., 2002. Cyber Terror- eine realistische Gefahr? Dostopno: http://www.aksis.de/CyberTerror.pdf (19. 08. 2006).
11. Krunić, Z., 1997. Strategija posrednega nastopanja. Ljubljana: Unigraf.
12. Politt, Mark M., 1997. Cyberterrorism – Fact or Fancy? FBI Laboratory, Washington D. C., dostopno: http://www.cs.georgetown.edu/~denning/infosec/pollitt.html (09. 10. 2006).
13. Savino, A., 2002. Cyber-Terrorism, Introduction, dostopno: http://cybercrimes.net/Terrorism/ct.html (25. 09. 2006).
14. Shahar, Y., 1997. Information warfare. International Policy Institute for Counter-Terrorism, dostopno tudi na: http://www.iwar.org.uk/cyberterror/resources/CIT.htm (04. 06. 2006).
15. Svete, U., 2005. Varnost v informacijski družbi. Ljubljana, Fakulteta za družbene vede.
16. Terrorists Use of Information Technology. Terrorism files org, http://www.terrorismfiles.org/weapons/information_technology.html (02. 10. 2006).
17. Thomas, T., 2003. Al Qaeda and the Internet: The Danger of »Cyberplanning. V: Parameters, Spring 2003, 112–123, dostopno tudi: http://carliste-www.army.mil/usawc/Parameters/03spring/thomas.pdf (01. 12. 2004).
18. Thomas, T., 2002. 30 Informationa-Age »De-Terror-Ance«, dostopno: http://www.leavenworth.army.mil/milrev/English/JanFeb02/thomas.htm (01. 12. 2004).
19. Weimann, G., 2005. Cyberterrorismus ist eine große, schwarze Wolke am Horizont. Dostopno http://www.sicherheit-heute.de/index.php?cccpage=readtechnik&set_z_artikel=200 (26. 11. 2005).
20. Weimann, G., 2006. Terror on the Internet: The New Arena, The New Challenges. Washington D.C.: United States Institute of Peace Press.
21. Whine, M., 1999. Cyberspace, A New Medium for Communication, Command and Control by Extremists. V: Studies in Conflict and Terrorism, 5. maj 1999, RAND, dostopno tudi: http://www.ict.org.il/articles/articledet.cfm?articleid=76 (18. 04. 2005).
22. Zanini, M. in Edwards, S., 2001. The Networking of Terror in the Information Age. V: Arquilla, J. in Ronfeldt, D. (ed.), 2001. Networks and Netwars: The Future of Terror, Crime and Militancy. RAND, dostopno tudi: http://www.rand.org/publications/MR/MR1382/MR1392.ch2.pdf (15. 06. 2004).

[7] Informacijski terorizem ne pozna fizičnih meja, kakor so kontrolne točke, državne meje, ipd.