VARSTVOSLOVJE,
let. 15
št. 3
str. 357–369

Socialno-psihološke implikacije kibernetskega terorizma

Kaja Prislan, Igor Bernik

Namen prispevka:

S prispevkom želimo predstaviti sinergijo učinkov nerealnih predstav o tehnologiji in terorizmu, realne sposobnosti in aktivnosti kibernetskih teroristov, hkrati pa opozoriti na grožnjo, ki je z vidika informacijske varnosti, predvsem na nacionalni ravni, ne smemo zanemariti.

Metode:

V prispevku je uporabljena deskriptivna metoda in metoda komparacije, s katerima smo analizirali predpostavke strokovnih in znanstvenih prispevkov na obravnavano tematiko. Z metodo sinteze spoznanj smo nadgradili trenutne teoretične pristope pri pojasnjevanju narave storilcev kibernetske kriminalitete in kibernetskega terorizma.

Ugotovitve:

Zaradi razvoja globalnega kibernetskega prostora je kriminaliteta pridobila povsem nove razsežnosti in priložnosti. Tako kot uporabniki sodobne tehnologije in klasični zlonamerni storilci v tem prostoru delujejo tudi kibernetski teroristi, katerih namen je s pomočjo tehnologije povzročiti čim večji strah in medijsko odzivnost. Psihološki učinki uporabe tehnologije prispevajo k temu, da kibernetski terorizem spremlja visoka stopnja nerazumevanja, posledično pa tudi strahu. Ker tovrstna kibernetska kriminaliteta nima urejene politične in pravne podlage, to skupaj z nerazumevanjem sodobne tehnologije, strahu pred njeno uporabo in možnimi zlorabami povzroča velik učinek zastraševanja. Čeprav kibernetski terorizem predstavlja resno grožnjo nacionalnim in organizacijskim informacijskim infrastrukturam, je njegovo udejanjanje v fizičnem okolju zgolj posredno. Teroristi sodobno tehnologijo za enkrat izkoriščajo predvsem kot orodje za pomoč pri načrtovanju napadov in ohranjanju lastnega obstoja.

Izvirnost/pomembnost prispevka:

Pomembnost prispevka se kaže v njegovi aktualnosti. Tako kot klasična kibernetska kriminaliteta tudi kibernetski terorizem postaja vse pogostejša tematika medijev in polemičnih razprav. S senzacionalnim poročanjem se velikokrat povzročajo dramatične in nerealne asociacije na kibernetski terorizem, v smislu možnih scenarijev in posledic. V prispevku predstavljamo njegove realne zmožnosti in temeljne značilnosti, izvirnost pa se kaže v njegovi pojasnjevalni in razlagalni vlogi.

UDK: 343.3/.7:004

Ključne besede: kibernetski terorizem, storilci, zastraševanje, psihološki vidiki

Socio-psychological Implications of Cyberterrorism

Purpose:

This paper intends to present the synergy between unrealistic notions about technology and terrorism and the cyberterrorists' real capabilities and activities. At the same time, the paper also points to the threat, which must not be neglected from the information security point of view, particularly at the national level.

Design/Methods/Approach:

The paper presents the use of descriptive and comparative methods, which were applied to analyse several assumptions found in professional and scientific publications in the relevant field. The synthesis method was then applied to consider the findings and upgrade current theoretical approaches in order to explain the nature of cybercrime and cyberterrorism perpetrators.

Findings:

Due to the development of global cyberspace, crime gained entirely new dimensions and opportunities. Apart from modern technology users and typical malevolent perpetrators, cyberterrorists, whose intention is to instigate as much fear and media attention as possible by using technology, are also operating in cyberspace. Psychological effects stemming from the use of technology contribute to the fact that cyberterrorism is characterised by a high level of misunderstanding and consequently fear. When considered in combination with the lack of understanding of modern technology, as well as the fear of its use and potential abuse, the fact that this type of cybercrime does not have a structured political and legal basis generates major intimidation effects. Although cyberterrorism represents a serious threat to information infrastructures owned by states and organisations, its actualisation in the physical environment is merely indirect. At the moment, terrorists mostly use modern technology as instrumentalities for planning attacks and preserving their own existence.

Originality/Value:

The importance of this paper is demonstrated by its up-to-date nature. Apart from traditional cybercrime, cyberterrorism is also becoming a subject of ever more frequent media attention and controversial debates. Sensationalist reporting often generates dramatic and unrealistic notions regarding cyberterrorism, as well as its potential scenarios and implications. This paper, however, presents the true capabilities and basic characteristics of cyberterrorism, while its originality is demonstrated by its explanatory and interpretative nature.

UDC: 343.3/.7:004

Keywords: cyberterrorism, perpetrators, intimidation, socio-psychological aspect

1 UVOD

Stalen tehnološki napredek in njegova splošna dostopnost oz. razširjenost sta v medsebojni kombinaciji privedla do različnih posledic, ki vplivajo na stanje in razvoj kriminalitete. Največja problematika, ki se je pojavila z vsakodnevno uporabo sodobne informacijsko-komunikacijske tehnologije (v nadaljevanju IKT) je zakonsko neurejen in geografsko neomejen kibernetski prostor, ki je glavni vzrok, da so poleg poslovne in socialne sfere kibernetski prostor odkrile tudi kriminalne skupine. Prvi poizkusi kibernetske kriminalitete[1] so bili primeri testiranja in preizkušanja lastnih sposobnosti posameznikov, z razvojem in napredkom tehnologije pa so se nevarno razvili tudi storilci v kibernetskem prostoru. Le-ti so danes največkrat organizirani v različne skupine, ki se povezujejo med seboj. Njihove aktivnosti so naravnane k skupnemu cilju skupine oz. združbe, najpogosteje pa gre za protipravno pridobivanje koristi ali javno odmevnost dejanj (United Nations Office on Drugs and Crime, 2010). V določenih skupinah je potreba po prevladi in načinu delovanja prerasla iz poslovne v politično motivacijo, da bi izzvala čim večjo medijsko pozornost in povzročila čim širšo družbeno škodo nasprotniku. V tem primeru govorimo o kibernetskem terorizmu. Politično in ideološko motivirana kibernetska kriminaliteta je pravzaprav ena izmed najbolj perečih področij sodobne družbe. Širša družbena motivacija, ki se uresničuje s pomočjo IKT, presega posamične interese, krši družbene norme, je v veliko primerih legalna, neopazna in v nekaterih kulturnih okoljih celo legitimna. Splošna dostopnost sodobne tehnologije je terorističnim organizacijam močno poenostavila načrtovanje lastnih aktivnosti in zagotavljanje življenjskega cikla. Anonimnost in komunikacijske prednosti tehnologije so privedle do razvoja novih in širitve obstoječih terorističnih celic. Kombinacija tradicionalnih terorističnih skupin s sodobno tehnologijo, organizirano kriminaliteto in hekersko subkulturo je privedla do drastičnega preoblikovanja delovanja in razvoja terorizma. Do selitve terorizma pa ni prišlo zaradi načrtovanja »elektronske vojne«, kot opozarjajo mediji, temveč zaradi neosebnosti uporabnikov in možnosti oddaljenega dostopa do informacijskih sistemov. Anonimnost, znotraj in zunaj teroristične organizacije, je članom poenostavila medsebojno komuniciranje, izogibanje organom pregona in rekrutiranje novih članov. Zaradi t. i. učinka deindividuacije[2] je širjenje in obstoj terorističnih organizacij veliko lažje, saj z zakrivanjem identitete pri uporabi tehnologije prihaja do porasta antisocialnega vedenja tudi v terorističnih vrstah. Ker kibernetski terorizem izziva veliko nejasnosti in nerazumevanja v smislu opredelitve, politične ureditve in zakonske podlage, ga tako v strokovni javnosti kot v širši družbi spremlja velika mera pod- in precenjevanja. Strah pred tehnologijo in terorizmom skupaj z dramatičnim poročanjem medijev povzroča v družbi veliko mero zastraševanja, kar pravzaprav uresničuje primarne cilje teroristov. Zanikanje in zavračanje njegovega obstoja, z neustrezno regulacijo in nadzorom, pa prav tako pripomore k obstanku terorističnih aktivnosti v kibernetskem prostoru.

1 *Kibernetska kriminaliteta pomeni uporabo informacijsko-komunikacijskih tehnologij za izvedbo kaznivih, škodljivih in nemoralnih dejanj v kibernetskem prostoru (Bernik in Meško, 2011).*

2 *Ali tudi »deindividualizacija«.*

1.1 Vzroki uporabe tehnologije v teroristične namene

Sodobno IKT so poleg klasičnih storilcev spretno izkoristile tudi teroristične organizacije, ki pri uporabi in zlorabi omenjene tehnologije ne zaostajajo za ostalimi storilci kibernetske kriminalitete. S selitvijo terorizma v kibernetski prostor in njegovo močno prisotnostjo na svetovnem spletu se je spremenila percepcija, razsežnost in agresivnost klasičnega terorizma, kot smo ga poznali. Glavna težava, s katero se srečuje mednarodna in strokovna javnost, je zaostanek varnostnih ukrepov in protiterorističnih aktivnosti za eksponentnim razvojem in preoblikovanjem terorističnih dejavnosti in njihovih pojavnih oblik. Odsotnost univerzalne oz. mednarodne definicije klasičnega terorizma in neustrezna normativna podlaga na tem področju takšen zaostanek še poglabljata. Trenutno imamo na voljo 18 univerzalnih mednarodnih pravnih aktov, ki se nanašajo na teroristične aktivnosti, nobeden izmed teh pa ne opredeljuje kibernetskega terorizma. Posledično pa pojav, ki ni pravno definiran, ni mogoče ustrezno kazensko in mednarodno preganjati ter obsoditi (Shiryaev, 2013). Kljub neenotni opredelitvi splošnega pojma »terorizem«[3] za njegovo pojavno obliko v kibernetskem prostoru, ob pregledu različnih definicij, predlagamo naslednjo definicijo: *»Kibernetski terorizem je naklepen, politično motiviran napad z uporabo IKT v kibernetskem prostoru za napad na druge informacijsko-komunikacijske sisteme (računalniški, informacijski sistemi, računalniški programi ali podatki) za nasilje nad cilji, ki se ne zoperstavljajo napadu. Pri tem se povzročajo panika, strah, javni odzivi velikih razsežnosti in potencialne smrtne žrtve.«*

Iz tega lahko razberemo, da teroristi pri zlorabi IKT uporabljajo enake tehnike in orodja kot storilci klasične kibernetske kriminalitete. Glavna težava, s katero se srečujejo pristojni organi, je torej prav razlikovanje med posameznimi oblikami kibernetske kriminalitete, ki je mogoče le na podlagi poznavanja identitete storilca in njegovega motiva. Ugotavljanje motiviranosti pa je izjemno problematično, saj so anonimnost, splošna razširjenost in dostop v kibernetski prostor z oddaljene lokacije glavni dejavniki sodobne tehnologije, ki storilcem omogočajo spretno zakrivanje identitete in izvora napada, prav tako pa so to glavni razlogi, zaradi katerih teroristi prisostvujejo v kibernetskem prostoru. Večina sodobnih terorističnih organizacij je sestavljena iz posameznih celic, ki so med seboj slabo povezane in so razpršene po večjem geografskem območju (US Army, 2007). Takšna struktura jim zagotavlja večjo varnost, vendar pa se zaradi tega pojavlja potreba po komuniciranju prek informacijskih medijev. Te razpršene skupine morajo biti medsebojno povezane, da lahko načrtujejo in izvedejo napade, pridobijo finančna sredstva in ponarejene dokumente. Obstoj in uspeh teh skupin je tako odvisen od dobre komunikacije, ki poteka mimo organov pregona, ki jih želijo odkriti (Rogers, 2003). In kibernetski prostor, predvsem internet, je orodje, s katerim lahko dosežejo te cilje. Je najverjetneje prvi množični medij, ki je omogočil zbiranje in povezovanje odtujenih oz. oddaljenih ljudi za izmenjavo mnenja in širjenje predsodkov. Zmožnost zaobiti

3 *Na splošno pa povsod velja, da terorizem pomeni sistematično in organizirano nasilno dejavnost skupin ljudi, ki so nedržavno ali državno organizirane s ciljem uničenja ali poškodovanja oseb in/ali premoženja, in to s političnimi, verskimi ali gospodarskimi nameni. Teroristična dejavnost je javna dejavnost, saj je usmerjena predvsem na vplivanje in oblikovanje javnega mnenja in na ustrahovanje širše družbene skupnosti (Newman et al., 2010).*

nacionalno zakonodajo je skupaj z elektronsko pošto in svetovnim omrežjem postala največji in najboljši medij za teroriste, ekstremistične skupine in aktiviste. Ta metoda komunikacije omogoča uporabniku zakrivanje prave identitete in skrivanje za izmišljeno oz. lažno (Crilley, 2004: 69), kar povečuje možnosti širjenja terorističnih skupin z rekrutiranjem novih članov. Takrat, ko se posamezniki, ki komunicirajo med sabo, ne poznajo (so anonimni), pride do t. i. deindividuacije, posledica česar pa je porast antisocialnega vedenja. Pri deindividuaciji popustijo posameznikove notranje zavore, zmanjša se sposobnost nadziranja lastnega ravnanja, kar je posledica zaznane anonimnosti. Različne študije ugotavljajo, da je zaradi anonimnosti večja verjetnost, da se bodo ljudje vedli agresivno (Peršak, 2009). Najnovejša različica teorije deindividuacije[4] trdi, da se bodo posamezniki obnašali deviantno, če socialna ali skupinska identiteta sprejemata oz. spodbujata takšno obnašanje in obratno (Williams, 2008: 145–146). Uporabniki kibernetskega prostora se namreč zavedajo »relativne oddaljenosti od drugih in relativne imunosti pred identifikacijo in sankcijami«. Prav tako je posameznik v kibernetskem prostoru popolnoma »gluh« oz. se ne zaveda pomena svojega dejanja in njegovih posledic v resničnem svetu (Hinduja, 2008: 392). Iz tega sledi, da anonimnost in deindividuacija sama po sebi sicer nista vzroka za deviantno obnašanje, lahko pa spodbudita k takšnim dejanjem posameznike, ki so iz takšnih ali drugačnih razlogov že nagnjeni k temu, vendar se v realnem svetu zaradi moralnih ali drugih zadržkov deviantnih aktivnosti ne bi poslu̇ževali. Vsekakor je kibernetski prostor močno pripomogel k zakrivanju identitete pripadnikov terorističnih organizacij, kar je njihov glavni način obstoja, in s tem povečal pripravljenost ljudi k priključitvi takšnim skupinam, saj je možnost odkritja v kibernetskem prostoru veliko manjša kot v fizičnem. Poleg zunanje anonimnosti pa svetovni splet zagotavlja anonimnost tudi znotraj same teroristične organizacije. Za slednje je značilno, da je notranja struktura razdeljena na posamezne dele, tako med posameznimi celicami kot tudi znotraj njih, v smislu hierarhije njenih članov. Novi člani in posamezniki, izvršitelji napadov, so pogosto izolirani od voditeljev in ključnih posameznikov v organizaciji. Takšna struktura terorističnih organizacij otežuje organom pregona pridobivanje ključnih informacij od ujetih članov te organizacije. Prav tako jim to onemogoča infiltracijo v jedro teroristične skupine (Rogers, 2003). Napad v kibernetskem prostoru oz. napad na določen informacijski sistem pa za napadalce predstavlja zelo nizko tveganje, saj obstaja majhna verjetnost, da bodo odkriti, prav tako pa lahko vstopijo ali zapustijo točko dostopa, kadar koli želijo. Če ob tem omenimo še nizko zavzetost oblasti za preganjanje tovrstne kriminalitete, lahko ugotovimo, da je tudi strah pred morebitnimi sankcijami skoraj ničen.

Poleg anonimnosti internet terorističnim skupinam daje možnost psiholoških učinkov na javnost z navideznim ojačevanjem[5] lastnih moči. Teroristična skupina, prisotna v kibernetskem prostoru, lahko z ustreznim znanjem pripravi lastno spletno stran, povezano z drugimi zelo obiskanimi spletnimi stranmi, kar daje uporabnikom občutek, da je skupina velika in močna, ne glede na njeno dejansko pojavno obliko. Pogosta razširjenost oz. prisotnost na spletu ustvarja vtis, da je organizacija takšna tudi v realnosti. In ker se uporabniki in družba odzivajo na

4 *Social identity theory of deindividuation – SIDE.*

5 *Ojačevanje je vojaški termin za povečevanje števila enot in moči.*

takšen pojav teroristične skupine na omrežju, se ji dejansko povečuje moč. V takšnem primeru se lahko obstoječa oblast in z njo represivni organi odzivajo na teroristične skupine, kot da so velike in mogočne. Oblast lahko zaradi tega postane izrazito avtokratična in poskuša omejiti uporabo ter razširjenost interneta s poseganjem v posameznikovo zasebnost. V takšnem primeru pa teroristi pravzaprav že dosežejo svoj cilj (Embar-Seddon, 2004: 17).

Eden izmed razlogov zlorabe tehnologije in uporabe interneta v teroristične namene pa je tudi razsežnost z napadom povzročenih posledic. Pri fizičnem napadu so posledice omejene na točno določeno lokacijo, medtem ko preostala skupnost dejanje le opazuje. Prav tako pa nasilje ni vedno najboljši način za doseganje političnih ciljev, saj je medijska pozornost usmerjena v samo dejanje in ne toliko v sporočilo teroristov, ki so ga želeli z dejanjem predati. Z uporabo interneta lahko teroristi s sporočilom dosežejo širšo skupnost, posledice pa niso tako dolgoročne in katastrofalne, da bi zameglile bistvo napada (Furnell in Warren, 2004). Prednost kibernetskega terorizma je tudi v tem, da je dejanje lahko sproženo na daljavo, prav tako pa ni potrebno ravnati z eksplozivom ali uresničiti samomorilsko misijo (Denning, 2000). Tehnike kibernetskega terorizma se močno razlikujejo od klasičnih terorističnih aktivnosti, saj so bolj sofisticirane in prikrite ter delujejo v popolnoma drugačnem okolju kot v preteklosti.

Temeljne oblike kibernetskega terorizma so (Ballard, Hornik in McKenzie, 2004: 59):

- Napad na informacijski sistem.[6] Glavni cilj je sprememba ali uničenje vsebine elektronskih datotek, računalniških sistemov ali podatkov, ki ga ta vsebuje.
- Uničenje ali poškodovanje kritične informacijske infrastrukture.[7] Sem so vključeni napadi na strojno in programsko opremo, stranska posledica pri tem je uničenje podatkov, glavni namen pa je poškodovanje informacijskega sistema oz. sistema, ki nadzira podatke v računalniškem okolju.
- Uporaba interneta in informacijskih sistemov za izvedbo klasičnega terorističnega napada.[8]
- Uporaba interneta za zbiranje finančnih sredstev za izvedbo nasilnih politično motiviranih akcij, za podporo drugih nasilnih dejanj ali za oglaševanje nasilne skupinske ideologije.[9]

Kadar je govora o kibernetskem terorizmu v pravem pomenu besede, gre za izvajanje zlonamernih vdorov in kibernetskih napadov na informacijske sisteme z namenom uničenja, spremembe, okvare ali zlorabe podatkov. Informacijski sistemi so lahko za teroristične skupine zanimivi zato, ker so najšibkejša točka razvitih družb. Računalniki nadzirajo dobavo električne energije, komunikacijo, letalski promet in finančne storitve. Uporabljajo jih za shranjevanje vitalnih

6 *Za napad se lahko uporabijo različne tehnike kibernetske kriminalitete: od širjenja zlonamerne programske opreme, kraja podatkov, onemogočanje delovanja sistemov in DOS napadov.*

7 *Kibernetski napadi v obliki vdorov, zasičenja strežnikov ali okvare sistemov.*

8 *V ta namen se med teroristi uporablja steganografija kot način za prenos skritih sporočil med pripadniki teroristične skupine. Največkrat se ta uporablja za prenos načrtov, širjenje priročnikov za načrtovanje napadov ali drugih ključnih informacij za izvedbo napada (Ballard et al., 2004: 59).*

9 *Za zbiranje finančnih sredstev se uporabljajo načini elektronskih prevar v obliki pharminga, phishinga, zlorabe kreditnih kartic, kraje identitete ipd.*

informacij, od zdravniških kartotek, poslovnih načrtov do kazenskih evidenc. Čeprav jim zaupamo, so ranljivi, predvsem zaradi slabe zasnove in pomanjkljive kakovosti nadzora nad nesrečami in napadi. Vendar pa se je pri tem treba zavedati tudi resnične moči in vpliva računalnikov na fizični prostor in okolje. Računalniki delujejo zaradi ljudi ali naprav, ki so priključene nanje. Da lahko računalnike povežemo s terorizmom, moramo zato razumeti njihove meje. Računalniki ne morejo neposredno ubiti ali poškodovati ljudi, lahko pa se povežejo z napravami ali sistemi, ki lahko vplivajo na fizično okolje. Zatorej obstaja posredno tveganje fizičnih okvar in neposredno tveganje ekonomskih poškodb. Kadar računalnike uporabimo kot orožje, se moramo zavedati, da so njihova dejanja posredna (Pollitt, 1997). Coleman (2003) navaja, da se neposredni stroški največkrat kažejo v izgubi prodaje med prekinitvijo, spletnih zamudah, prekinjenem dostopu za poslovne uporabnike, povečanih stroških zavarovanja, izgubi intelektualne lastnine, cenitev, stroških forenzike, sporih in izgubi kritičnih komunikacij v izrednem stanju. Med posredne posledice napada pa uvršča izgubo samozavesti in kredibilnosti finančnih sistemov, skrhane odnose in slabo globalno javno podobo, napete poslovne odnose, izgubo dohodkov strank v prihodnosti in izgubo zaupanja v vlado ter industrijo. Posledice se torej najpogosteje kažejo v ekonomski škodi. Ta pa lahko sproži veliko drugih posledic, ki so naštete kot posredne. Kibernetski terorizem lahko povzroči neposredno, vidno škodo, vendar pa je največkrat najhujša posredna škoda.

Za izvedbo sofisticiranih vdorov in napadov na informacijske sisteme teroristi potrebujejo relativno veliko znanja in spretnosti, zato se večina terorističnih skupin v kibernetskem prostoru ukvarja z naslednjimi aktivnostmi (prirejeno po Cohen, 2004: 150–151; Embar-Seddon, 2004: 16; Rogers, 2003): načrtovanje (zbiranje obveščevalnih podatkov, izvajanje analiz, koordiniranje članov in opreme); financiranje (zbiranje in prenos denarja, največji del finančnih sredstev pridobivajo v trgovini z drogo, belim blagom in orožjem, na spletu pa se sredstva velikokrat zbirajo in prenašajo prek dobrodelnih organizacij, donacij in skozi kraje ter zlorabe kreditnih kartic); koordiniranje (izdaja ukazov za izvrševanje akcij, časovno usklajevanje, določanje sestankov, dogovori o prevzemih naročenih pošiljk); politične akcije (povečevanje prepoznavnosti in medijske pozornosti z ustvarjanjem spletnih strani in prodajo terorističnih pripomočkov); rekrutiranje (pričakovana doba teroristične organizacije brez pridobivanja novih članov je manj kot eno leto, zato teroristične organizacije uporabljajo IKT in internet, da so bolj privlačne za mlajše morebitne kandidate ali t. i. mehke podpornike, ki javno in očitno izkazujejo podporo tem organizacijam); propaganda (preko spletnih strani teroristične skupine širijo svoje ideale in napačne oz. selekcionirane informacije s tem opravičujejo svoje akcije in ljudem prikazujejo svoje videnje sveta), ojačevanje (povečevanje moči enote brez dejanskega povečevanja števila njenih pripadnikov, saj je z uporabo interneta možno prikazati, da so veliko močnejše kot v resnici).

V največji meri teroristi uporabljajo internet kot podporo pri načrtovanju ali izvedbi klasičnih terorističnih napadov, vendar teroristični kibernetski napadi kljub temu predstavljajo povsem realno možnost. Zatorej je prva in najpomembnejša naloga preiskovalcev v primeru napada na informacijsko infrastrukturo prepoznati motiv in namen storilca. Mnogi primeri napadov se pod pojem terorizem ne morejo uvrstiti zaradi odsotnosti političnega ali socialnega motiva. Kljub temu pa

se zaradi potrebe po senzacionalnem poročanju velikokrat tudi najmanjše klasične napade na informacijske sisteme predstavlja kot terorizem. Do konca leta 2012 je bilo mogoče skupno zaznati več kot 31.000 prispevkov z opozorili na kibernetski terorizem, medtem ko v realnosti nismo uspeli zaznati nobenega klasičnega primera, posledično pa zato ne moremo govoriti o morebitnih žrtvah (Singer, 2012). Takšna situacija terorističnim organizacijam pravzaprav ne povzroča nobene škode, saj je njihov glavni namen ravno vplivanje na javno mnenje in povzročanje strahu v družbi[10] (Newman et al., 2010). Glede na to, da negativne osebne izkušnje s kriminaliteto praviloma (ne pa nujno) vplivajo na povečanje zaznane verjetnosti viktimizacije (Meško, Šifrer in Vošnjak, 2012: 80), lahko upravičeno domnevamo, da je zaradi preteklih negativnih izkušenj, ki jih ljudje pridobijo tudi od medijev, strah ob grožnji terorističnega napada izjemno velik. Kadar pa se ob tem omenja še možnost kibernetskega napada pa so občutki tesnobe in panični odzivi toliko večji. IKT že sama po sebi pri neveščih in neusposobljenih ljudeh izziva strah. Imenujemo ga tehnofobija in je odvisen od anksioznosti posameznika in njegove ozaveščenosti/usposobljenosti varno ravnati s tehnologijo (Gilbert, Lee-Kelley in Barton, 2003). Nepoznavanje tehnologije, njenega delovanja, morebitnih zlorab in posledic lahko hitro privede do prevelikega strahu in odpora ali pa ravno nasprotno, do malomarnosti in večje izpostavljenosti.

2 STRAH PRED KIBERNETSKIM TERORIZMOM

Ena izmed trenutno pogosteje raziskovanih tem v kriminologiji je strah pred kriminaliteto (Meško, Petrovec, Areh, Muratbegovič in Rep, 2006). Raziskovalci ugotavljajo, da strah pred kriminaliteto navadno presega dejansko stopnjo kriminalitete v družbi (Meško in Šifrer, 2008). Ko pomislimo na kibernetski terorizem, si predstavljamo najhujše, velikokrat pa si zamišljamo nemogoče scenarije, kar je posledica napačnega razumevanja pojava in strahu pred njim (Embar-Seddon, 2004: 18), vse skupaj pa se poglobi še zaradi slabih, redkih, vendar odmevnih izkušenj v preteklosti. Zelo hitro ugotovimo, da posamezni medijsko izpostavljeni primeri povzročijo višjo stopnjo strahu, kot sta dejanski ogroženost in možnost viktimizacije. Young (2007) ugotavlja, da so množični mediji spektakularna mesta izključevanja: v javnost prenesejo zaporedje, pravičnost in vključenost (ozadje novice), pri tem pa nalašč poudarjajo napake, nepravičnosti in izključenost ter te elemente postavijo v ospredje.

Mediji s svojim poročanjem pogosto ustvarjajo splošno mnenje in z miti o kriminaliteti upravičujejo socialne ukrepe, ki temeljijo predvsem na čustvenem odzivanju na poročanje o kaznivih dejanjih. Ukrepe, predvsem represivne, utemeljujejo z izražanjem strokovnih mnenj o kriminaliteti (Meško, 2000), ki v primerih kibernetskih napadov ali terorizma niso vedno objektivni in utemeljeni. V medijih je pogosto možno zaslediti opozarjanja na primere kibernetskega terorizma, bližajoče se elektronske vojne ipd. (npr. Spillius, 2012; Strand, 2012), ki

10 Teroristi zato, da bi izzvali strah in druge psihične odzive, izkoriščajo odmevnost svojega dejanja in sredstva množičnega obveščanja s prevzemanjem odgovornosti za teroristična dejanja, da bi tako izzvali širšo in večjo želeno reakcijo (Ledinek, 2005).

to sploh niso. Mnogi avtorji so pravzaprav mnenja, da še vedno nismo bili priča dejanskemu primeru kibernetskega terorizma (Cavelty, 2007; Conway, 2011; Stohl, 2007; Weimann, 2004). Zavedati se je treba, da kibernetski terorizem ni samo napad na vojaške ali vladne institucije, temveč ti napadi predstavljajo dejanje, izvedeno s pomočjo računalnikov, omrežja in storilcev kibernetske kriminalitete. Da lahko napad klasificiramo kot kibernetski terorizem, mora biti zasnovan tako, da povzroči strah ter vpliva na družbo in njeno izvršno oblast. Do danes je bila večina takšnih zaznanih napadov produkt storilcev brez političnega motiva[11] (Rogers, 2003). Takšne zmote zaradi slabega poznavanja področja in pogosto nestrokovnega poročanja medijev o kibernetski kriminaliteti še dodatno zastrašujejo uporabnike.

Poleg medijev, ki največkrat napačno uporabljajo pojem kibernetski terorizem, pa k nerazumevanju tega pojava prispevata še strah pred neznanim in pomanjkanje informacij oz. napačne informacije. Pojem kibernetski terorizem torej združuje dve sodobni obliki strahu (Ballard et al., 2004):

- strah pred napredujočo tehnologijo in
- strah pred terorizmom.

Tako tehnologija kot terorizem sta v sodobni družbi relativni neznanki. Uporaba tehnologije od posameznika zahteva ustrezno znanje in sposobnosti. Tisti, ki se tehnologiji niso prilagodili, niso sposobni normalnega funkcioniranja v sodobnem času, podprtem s tehnologijo. Motivacijo teroristov pa je težko razumeti in brez tega razumevanja se njihovi napadi zdijo brezčutni in naključni, kar pomeni, da vsakdo lahko postane tarča. Zatorej ni čudno, da pojem kibernetski terorizem pri ljudeh vzbuja strah (Embar-Seddon, 2004: 12). Ta pa spremlja vsakršen pojav, vezan na terorizem v kibernetskem svetu, ne glede na kateri ravni in v kakšni pojavni obliki se pojavi. Kibernetska kriminaliteta, katere del je tudi kibernetski terorizem, postaja vse pogostejša in aktualna tema medijev in mednarodne strokovne ter politične javnosti. Zaradi odmevnosti je strah pred kibernetskimi prevarami, zlorabami ali uničenjem povsem razumljiv, vendar v veliko primerih tudi nerazumen. Kibernetski terorizem je en izmed takšnih pojavov, ki kljub relativno redki uresničitvi povzroča močne in čustvene odzive. Slednje pa je pravzaprav glavni cilj terorističnih organizacij. S prisotnostjo v kibernetskem okolju zastrašujejo internetno populacijo, dejanska ogroženost kritičnih infrastruktur in uporabnikov pa pravzaprav zaradi pomanjkanja sodelovanja in interesa strokovne javnosti na tem področju ni znana.

3 RAZPRAVA

Anonimnost z možnostjo izogibanja odgovornosti ter strah pred terorizmom, tehnologijo in kibernetsko kriminaliteto, so glavni psihološki dejavniki oz. učinki, ki omogočajo razvoj in obstoj kibernetskega terorizma. Nejasnosti, povezane z

11 *Leta 1998 je tamilska gverilska skupina dva tedna »bombardirala« ambasade na Šrilanki s po več kot 800 elektronskimi sporočili na dan. V sporočilu je pisalo: »Mi smo spletni črni tigri in to počnemo, da bi prekinili vašo komunikacijo.« Obveščevalne službe so to označile kot prvi znani napad teroristov na državni računalniški sistem (Coleman, 2003).*

ureditvijo in nadzorom kibernetskega prostora, ter nedoslednost kaznovanja storilcev pa so glavni atributi sodobne tehnologije, ki privlačijo politično in ideološko motivirane storilce v relativno novo in neznano okolje. Možnost zakritja identitete pri posameznikih s politično uporniškim potencialom zmanjšuje notranje (moralne) zavore, kar terorističnim organizacijam olajšuje ohranjanje obstoja z rekrutiranjem novih, mlajših in tehnološko podkovanih članov. Poleg lažje komunikacije in organizacije kibernetski prostor teroristom olajšuje tudi doseganje zastavljenih ciljev oz. vizije, to je zastraševanje družbe. Strah pred kibernetskim terorizmom je posledica sinergije različnih dejavnikov strahu in je zaradi tovrstne kombinacije toliko večji in širši, saj ga ljudje navadno precenjujejo. Strah pred terorizmom je zaradi negativnih preteklih izkušenj še vedno zelo živ, s pridevnikom »kibernetski« pa je zaradi nerazumevanja sodobne tehnologije še toliko močnejši. K nerazumevanju tovrstnega pojava prispevata tudi neurejena politika in zakonodaja ter neobjektivnost oz. dramatičnost medijev pri poročanju o kibernetski kriminaliteti. Slednje pa daje terorističnim organizacijam en razlog več za implementacijo sodobne tehnologije v lastne aktivnosti.

Dejanska stopnja ogroženosti informacijskih sistemov pred terorističnimi skupinami, zaradi pomanjkanja interesa in volje ureditve tega področja, ni znana. Kljub neustreznemu razumevanju tovrstne teroristične dejavnosti pa grožnja hipotetično obstaja, zatorej predstavlja tudi dejavnik tveganja, predvsem za nacionalno informacijsko infrastrukturo. Pred tem ni izvzeta niti Slovenija, saj jo vključenost v mednarodno skupnost, politiko, organizacije in mednarodne akcije postavlja na seznam potencialnih tarč. Kibernetski terorizem je vsekakor pojav, s katerim se mora enotno in harmonično ukvarjati celotna mednarodna skupnost, ki naj uredi normativno in politično podlago za vsakršno nadaljnje preiskovanje, urejanje in nadzorovanje. Za učinkovitost pri doseganju takšnega konsenza pa je nujno potrebno sodelovanje različnih strok in področij, saj gre v primeru kibernetskega terorizma za izjemno kompleksen pojav, ki združuje največje družbene strahove. V boju proti tovrstni kriminaliteti morajo združiti svoje napore strokovnjaki z različnih področij, npr. psihologije, kriminalistike, informacijske varnosti itd. Dobro poznavanje narave problema in storilcev lahko pripomore k uspešnemu boju proti novi obliki terorizma. Treba je natančno analizirati razmišljanje storilcev, njihov način delovanja, način življenja, organizacijo in motive. Raziskava in analiza kibernetskega terorizma z namenom vpogleda v njegovo naravo je osnova vsakršnega nadaljnjega postopanja in urejanja tovrstne problematike. Nedavno je bil velik korak naprej storjen z mednarodnim projektom »Cyberterrorism project«, ki je izvedbo začel leta 2011 in poteka še danes. Njegov namen je raziskati stališča strokovnjakov, sprožiti multidisciplinarne razprave o problematiki in spodbuditi mednarodno ter medorganizacijsko sodelovanje. V nedavnih razpravah in raziskavah (mednarodna konferenca in raziskava med 118 strokovnjaki iz 24 držav, pri čemer so sodelovali tudi predstavniki iz Slovenije) o trenutnem stanju in mednarodni ureditvi kibernetskega terorizma, strokovnjaki ugotavljajo, da omenjen pojav spremljajo različne etične, politične, zakonske in tehnične ovire. S socialno-psihološkega vidika je največji problem v nerazumevanju narave tovrstne kibernetske grožnje, posledično pa je težko preprečevati in odkrivati grožnjo, ki ni enotno definirana. Zaradi odsotnosti ustrezne pravne

podlage pa je še težje identificirati potencialne storilce in določiti njihove motive. Večina strokovnjakov se strinja še, da je obstoj kibernetskega terorizma odvisen od stališč medijev oz. političnih razprav v določeni državi, saj omenjena dejavnika najbolj pospešujeta njegov razvoj (Cyberterrorism project, 2013). Iz tega sledi, da je odpravljanje strahu pred terorizmom pravzaprav protiteroristični ukrep, saj je strah gonilna sila vseh terorističnih organizacij. Na tem mestu je izobraževanje ljudi o rokovanju s tehnologijo, načinih zaščite in narave posameznih kriminalnih dejanj nujno potrebno za realizacijo takšnega cilja. Poznavanje lastnih ranljivosti in odgovorno vedenje v kibernetskem prostoru sta ključ do ustrezne informacijske varnosti posameznika. Pri sodobnem delu, kjer je stalna povezanost s kibernetskim prostorom nujna, večino zlorab »omogočata« ravno neznanje ali brezbrižnost ljudi, saj z informacijskimi sredstvi pogosto ravnamo nevestno (McCullagh in Caelli, 2005: 336). Boljše znanje, izkušenost, višja stopnja ozaveščenosti ter boljša zaščita računalnikov z elementarnimi programi in orodji za zaščito pomenijo manjše tveganje. Izobraževanje in usposabljanje glede nevarnosti kibernetske kriminalitete mora na vseh ravneh družbenega življenja postati del vsakdana za usposobitev ozaveščenega posameznika, ki premišljeno in odgovorno uporablja internet brez strahu pred zlorabo. Nekaj strahu je sicer koristno, saj se s tem poveča pazljivost uporabnika pri delu z računalnikom, s tem pa se zmanjša ogroženost, zato tudi ni smiselno preveč zmanjševati strahu, saj lahko pride do nasprotnega učinka (Meško in Areh, 2003: 257).

Na nacionalni in organizacijski ravni je potrebno poskrbeti za sprejem in implementacijo celovite varnostne strategije: od tehnične zaščite do natančno določene osebne odgovornosti posameznikov in podjetij. Kibernetski storilci postajajo iz dneva v dan bolj izkušeni, uporabljajo številne tehnike, o katerih še nismo poučeni, zaradi česar je tudi obramba vedno korak za napadalci. Prav celovitost in pazljivost ter obravnavanje informacijske varnosti kot nedokončanega procesa je lahko edina obramba pred informacijsko-varnostnimi incidenti. V takšnem primeru bo informacijska varnost učinkovita, stroški okrevanja in prekinitve poslovanja pa minimalni. V primeru uresničitve dobro načrtovanega terorističnega napada na informacijski sistem se le-temu v celoti ne moremo uspešno zoperstaviti, zato je vse, kar lahko storimo to, da optimiziramo stanje varnosti, spoznamo grožnjo in smo nanjo pripravljeni. Kakršenkoli strah pred incidentom pa pri zoperstavljanju pomaga bolj malo.

LITERATURA

Ballard, J. D., Hornik, J. G. in McKenzie, D. (2004). Technological facilitation of terrorism. V A. O'Day (ur.), *Cyberterrorism* (str. 39–66). Aldershot: Ashgate.

Bernik, I. in Meško, G. (2011). Internetna študija poznavanja kibernetskih groženj in strahu pred kibernetsko kriminaliteto. *Revija za kriminalistiko in kriminologijo*, *62*(3), 242–252.

Cavelty, M. D. (2007). Cyber-terror: Looming threat or phantom menace. *Journal of Information Technology and Politics*, *4*(1), 19–36.

Cohen, F. (2004). Terrorism and cyberspace. V A. O'Day (ur.), *Cyberterrorism* (str. 149–151). Aldershot: Ashgate.

Coleman, K. (2003). Cyber terrorism. *Directions Magazine*. Pridobljeno na http://www.directionsmag.com/article.php?article_id=432

Conway, M. (2011). Against cyberterrorism. *Communication of the ACM, 54*(2), 26–28.

Crilley, K. (2004). Information warfare: New battlefields terrorists, propaganda and the internet. V A. O'Day (ur.), *Cyberterrorism* (str. 67–81). Aldershot: Ashgate.

Cyberterrorism project. (2013). Wales: Swansea University. Pridobljeno na http://www.cyberterrorism-project.org/about/

Denning, D. E. (2000). *Cyberterrorism: Testimony before the special oversight panel on terrorism committee on armed services U.S. House of Representatives*. Pridobljeno na http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html

Embar-Seddon, A. (2004). Cyberterrorism. V A. O'Day (ur.), *Cyberterrorism* (str. 11–21). Aldershot: Ashgate.

Furnell, S. M. in Warren, M. J. (2004). Computer hacking and cyber terrorism: The real threats in the new millennium. V A. O'Day (ur.), *Cyberterrorism* (str. 111–117). Aldershot: Ashgate.

Gilbert, D., Lee-Kelley, L. in Barton, M. (2003). Technophobia, gender influences and consumer decision-making for technology-related products. *European Journal of Innovation Management, 6*(4), 253–263.

Hinduja, S. (2008). Deindividuation and internet software piracy. *Cyberpsychology & Behavior*, *11*(4), 391–398.

Ledinek, I. (2005). Terorizem. *Varnostnik*, (8), 25.

McCullagh, A. in Caelli, W. (2005). Who goes there? Internet banking: A matter of risk and reward. V C. Boyd in J. M. Nieto Gonzalez (ur.), *Information security and privacy: 10th Australasian conference, ACISP 2005* (str. 336–357). Berlin Heidelberg: Springer-Verlag.

Meško, G. (2000). Miti o kriminaliteti v ZDA. *Revija za kriminalistiko in kriminologijo*, *51*(4), 305–313.

Meško, G. in Areh, I. (2003). Strah pred kriminaliteto v urbanih okoljih. *Revija za kriminalistiko in kriminologijo*, *54*(3), 144–152.

Meško, G. in Šifrer, J. (2008). Fear of crime in urban settings – an inquiry. *Varstvoslovje*, *10*(4), 550–560.

Meško, G., Šifrer, J. in Vošnjak, L. (2012). Punitivnost, viktimizacija in strah pred kriminaliteto pri študentih varstvoslovja – rezultati spletne ankete. *Varstvoslovje, 14*(1), 75–96.

Meško, G., Petrovec, D., Areh, I., Muratbegovič, E. in Rep, M. (2006). Strah pred kriminaliteto v Sloveniji in Bosni in Hercegovini – izidi primerjalne študije. *Revija za kriminalistiko in kriminologijo*, *57*(1), 3–14.

Newman, G. R., Clarke, R. V., Dobovšek, B., Ivanuša, T., Podbregar, I., Sotlar, A. et al. (2010). *Policijska dejavnost proti terorizmu: učbenik za vodilno osebje na policijskih postajah*. Ljubljana: Fakulteta za varnostne vede.

Peršak, N. (2009). Virtualnost, (ne)moralnost in škodljivost: normativna vprašanja nekaterih oblik kibernetične kriminalitete. *Revija za kriminalistiko in kriminologijo*, *60*(3), 191–198.

Pollitt, M. M. (1997). *Cyberterrorism – fact or fancy?* Pridobljeno na http://www.cs.georgetown.edu/~denning/infosec/pollitt.html

Rogers, M. (2003). The psychology of cyber-terrorism. V S. Andrew (ur.), *Terrorists,victims and society: Psychological perspectives on terrorism and its consequences* (str. 77–91). Chichester: Wiley.

Shiryaev, Y. (2013). *Cyberterrorism in the context of contemporary international law*. Warwick: Warwick school of law.

Singer, P. W. (2012). The cyber terror boogeyman. *Armed Forces Journal.* Pridobljeno na http://www.brookings.edu/research/articles/2012/11/cyber-terror-singer

Spillius, A. (12. 10. 2012). US at risk of 'cyber-Pearl Harbor'. *The Telegraph*. Pridobljeno na http://www.telegraph.co.uk/news/worldnews/northamerica/usa/9604794/US-at-risk-of-cyber-Pearl-Harbor-Leon-Panetta-warns.html

Stohl, M. (2007). Cyber terrorism: A clear and present danger, the sum of all fears, breaking point or patriot games? *Crime, Law and Social Change, 46*(4–5), 223–238.

Strand, P. (3. 10. 2012). America's cyber defenses: A digital Pearl Harbor? *CBN.News*. http://www.cbn.com/cbnnews/us/2011/december/americas-cyber-defenses-a-digital-pearl-harbor-/

United Nations Office on Drugs and Crime. (2010). *Cybercrime.* Pridobljeno na http://www.unodc.org/documents/data-and-analysis/tocta/10.Cybercrime.pdf

US Army. (2007). *A military guide to terrorism in the twenty-first century*. Kansas: TRADOC.

Weimann, G. (2004). *Cyberterrorism: How real is the threat? Special report*. Washington: United States Institute of Peace.

Williams, K. S. (2008). Using tittle's control balance theory to understand computer crime and deviance. *International Review of Law Computers & Technology*, *22*(1–2), 145–155.

Young, J. (2007). *The vertigo of late modernity*. London: Sage.

O avtorjih:

Kaja Prislan, mag. var., doktorska študentka na Fakulteti za varnostne vede Univerze v Mariboru.

Dr. Igor Bernik, docent, predstojnik Katedre za informacijsko varnost in prodekan za izobraževalno dejavnost na Fakulteti za varnostne vede Univerze v Mariboru. E-mail: igor.bernik@fvv.uni-mb.si