UDK 004.738.5:323.28
COBISS.SR-ID: 159843081
DOI: http://10.5937/ UBUR24283R

Ana Radovanović*
Fakultet bezbednosti, Univerzitet u Beogradu

Sajber terorizam kao pretnja bezbednosti u urbanom prostoru

SAŽETAK

Brz razvoj informaciono-komunikacionih tehnologija (IKT) poslednjih decenija proizveo je, pored pozitivnih promena, u vidu brže i lakše komunikacije i ukupnog napretka društva, i širok spektar negativnih pojava i razvoj novih oblika bezbednosnih pretnji i rizika. Među brojnim pretnjama u sajber prostoru izdvaja se sajber terorizam. Pandemija Kovida 19 dovela je do ubrzanog tehnološkog razvoja u oblasti IKT, gde je značajan deo komunikacije izmešten iz realne u virtuelnu stvarnost. Sajber prostor je pothranjen velikom količinom informacija, različitih kategorija i stepena tajnosti. Imajući u vidu da ovaj prostor ima veliki broj pojavnih formi i same karakteristike prostora, u vidu odsustva geografskih ograničenja i mogućnosti delovanja s velike distance, pružanje anonimnosti počiniocu i teške sagledivosti posledica, veliki su izgledi za odvijanje sajber terorističkog napada u bliskoj budućnosti. U literaturi ne postoji opšte prihvaćena definicija sajber terorizma, ali možemo prihvatiti definicije, koje ga predstavljaju kao kriminalni akt u sajber prostoru, zloupotrebom računarskih mreža, čiji je cilj ugrožavanje vitalne nacionalne infrastrukture, prinuda i zastrašivanje Vlade i/ili njenih građana. Posledice sajber terorizma prema svojoj težini mogu se podeliti u tri kategorije: prvu predstavlja izmena ili krađa informacija i privremeni prekid rada institucija, drugu kategoriju

* aradovanovic099@gmail.com

predstavlja serija koordiniranih napada, koja utiče na donosioce odluka, i treću predstavlja napad na kritičnu infrastrukturu, što prouzrokuje poremećaje u funkcionisanju kritične infrastrukture ili njeno oštećenje. U ovom radu dat je doprinos razumevanju sajber terorizma, sa posebnim osvrtom na analizu napada kritične infrastrukture, koja je uglavnom skoncentrisana u urbanim sredinama i mogućim posledicama za ključne uslužne sisteme vodosnabdevanja, transportne, komunikacione i sisteme snabdevanja hranom ili sisteme zdravstvene zaštite.

KLJUČNE REČI: *sajber prostor, sajber terorizam, kritična infrastruktura*

UVOD

Teroristički napad koji se dogodio 11. septembra 2001. godine na teritoriji Sjedinjenih Američkih Država stavio je lupu javnosti na ekstremističke organizacije i njihove pripadnike, ali i označio početak globalne borbe protiv terorizma. Izgledi za odvijanje sajber terorističkog napada su veliki imajući u vidu međuzavisnost tri faktora. Brz tehnološki razvoj i sve veću zavisnost društva od javnih informaciono-komunikacionih mreža i njihovih usluga, odnosno sve veće povezanosti fizičkog i virtuelnog sveta i karakteristike sajber prostora.

Istorijski osvrt na terorističke napade pokazuje da su česta meta bili urbani centri, od Ankare i Madrida, preko Osla, Pariza i Nice, do nedavnog napada u Mahačkalu i Derbentu. To se može objasniti činjenicom da gradovi predstavljaju kulturne, privredne i infrastrukturne centre, kao i to da je kritična infrastruktura locirana u gradu ili u neposrednoj okolini grada. Kritična infrastruktura ima krucijalni značaj za obezbeđivanje ekonomske stabilnosti, javnog blagostanja i društvene kohezije u urbanim prostorima. Imajući u vidu da njeno malo oštećenje ili kvar može dovesti do brojnih nezgoda po svakodnevne aktivnosti ljudi ili odneti stotine hiljada ljudskih života, predstavlja savršenu metu za sajber teroristički napad. Imajući u vidu ograničenja u pogledu obima, u ovom preglednom radu neću se baviti izuzetno značajnim pitanjem zaštite kritične infrastrukture, već isključivo posledicama koje sajber teroristički napad ostavlja po nju, a samim tim i na život u urbanim sredinama. No, pre nego predstavim ove posledice, neophodno je nešto reći o samom konceptu sajber terorizma, odnosno faktorima koji su doveli do njegovog uspona u 21. veku.

O SAJBER TERORIZMU

Pojam sajber terorizam sastoji se iz dva pojma: sajber prostora i terorizma. Ova nova forma terorizma nastala je kao produkt integracije čoveka i računara. Sajber terorizam možemo definisati kao kriminalni akt u sajber prostoru zloupotrebom računarskih mreža, čiji je cilj ugrožavanje vitalne nacionalne infrastrukture, prinuda i zastrašivanje Vlade i/ili njenih građana. Da bismo određeni akt kategorisali kao sajber teroristički nužno je postojanje posledica napada. Posledice napada mogu biti oštećenja ili uništenja imovine, povrede i/ili smrti civila ili psiholoških poledica u vidu panike i straha (Weimann, 2004: 4). Za potrebe ovog rada i boljeg razumevanja istraživanog pojma, autorka analizira sajber terorizam kroz dvodimenzionalni model. Prvu dimenziju čine analize sajber terorizma kao pretnje bezbednosti 21. veka, a druga dimenzija se sastoji iz prikaza karakteristika sajber terorista i sajber terorističke zajednice. Analiza prve dimenzije pruža odgovor na dva pitanja. Kolika je verovatnoća za odvijanje sajber terorističkog napada i da li ovaj vid terorizma ima prednosti u odnosu na klasičnu formu terorizma. Ova dimenzija je predstavljena kroz analizu faktora karakteristika internet, sajber prostora, sajber napada i sajber oružja. Rogers ističe da su sajber prostor i internet komplementarni sa prirodom sajber terorizma i psihom terorista (Rogers, 2003). Internet pruža brojne mogućnosti teroristima, od jednostavnog pristupa, brzog protoka informacija, preko ostvarivanja bezbedne komunikacije i prikupljanja dostupnih informacija za potrebe planiranja budućeg napada, do mogućnosti uticaja na tradicionalne masovne medije (Damnjanović, 2009; Rogers, 2003; Dobovšek i Dimic, 2012). Pored navedenog, internet olakšava teroristima sprovođenje propagadnih aktivnosti i regrutovanje novih članova. „Sajber prostor je i više nego privlačan za teroriste koji svojim akcijama mogu da zaštite identitet, lokaciju napada, nanesu štetu, pošalju svoju poruku i dobiju medijsku popularnost" (Jonev, 2016: 212). Sajber terorizam predstavlja vrstu sajber napada. Sajber napadi su privlačni teroristima jer je zahtevno utvrditi da li je napad nastao kao rezultat kvara, kompjuterske greške ili je organizovan od strane ljudi (Jonev, 2016). Ključne karakteristike sajber napada su nepredvidivost i nemogućnost proste detekcije ljudskim čulima, odnosno ne može se čuti i videti. Sajber napad podrazumeva upotrebu sajber oružja, koje poseduje brojne pred-

nosti u odnosu na konvencionalno oružje, pre svega zbog niskih troškova proizvodnje i upotrebe, ima mogućnost brzog kreiranja i distribucije, a može izazvati veliku štetu (Jonev, 2016). Ovi napadi mogu ugroziti integritet i poverljivost informacija, dostupnost servisa i usluga informaciono-komunikacionih tehnologija, ali i procese zasnovane na informaciono-komunikacionim tehnologijama, koji kontrolišu fizičke procese u stvarnom svetu (Luknar, 2022). Druga dimenzija se bavi razumevanjem sajber terorizma na nivou pojedinca, kroz prikaz karakteristika teroriste, ali i šire zajednice, mapirajući karakteristike terorističke zajednice. Uglavnom su to agresivni pojedinci, orijentisani na akciju, koji traže uzbuđenje i stimulans. Poseduju osobine kao što su odanost i posvećenost ideološkom cilju i grupi. Imaju crno-beli pogled na svet, a svako shvatanje koje se razlikuje od njihovog znači da ste protiv njih, odnosno imaju uniformnu retoriku, koja omogućava identifikaciju članova sa grupom i njenim ciljevima, ali i koheziju same grupe (Post, 2005; Horgan, 2003; Rogers, 2003). Sve veća primena interneta i intezivni razvoj informaciono-komunikacionih tehnologija proizveli su promene u vidu brže i lakše komunikacije, odnosno doveli su do kreiranja otvorenog sveta, ali i do evolucije terorističkih grupa u virtuelnu zajednicu i promenu organizacionog oblika. Od malih, lokalnih i samoorganizovanih grupa, smeštenih u neprijateljskom staništu, koje odlikuje hijerarhijski model organizacije, do mrežnog oblika organizacije (Baltezarević, 2022: 162). Jer umreženo društvo proizvodi „umreženi terorizam" (Jevtović, 2016: 116). Sajber terorizam pokreće brojna pitanja kao što su: zašto kritična infrastruktura predstavlja „savršenu" metu sajber terorističkog napada, da li postoje ranjivosti u kritičnoj infrastrukturi koje omogućavaju realizaciju napada i koje su posledice napada? U nastavku rada autorka će se baviti navedenim pitanjima.

RIZIK OD SAJBER TERORIZMA I NJEGOVI EFEKTI NA KRITIČNU INFRASTRUKTURU

Prema Zakonu o kritičnoj infrastrukturi Republike Srbije, kritična infrastruktura je definisana kao „sistemi, mreže, objekti ili njihovi delovi, čiji prekid funkcionisanja ili prekid isporuke roba, odnosno usluga može imati ozbiljne posledice na nacionalnu bezbednost,

zdravlje i živote ljudi, imovinu, životnu sredinu, bezbednost građana, ekonomsku stabilnost, odnosno može ugroziti funkcionisanje Republike Srbije (čl. 4 Zakona o kritičnoj infrastrukturi Republike Srbije). Kritična infrastruktura se zasniva na sajber-fizičkim sistemima, a ovi sistemi se zasnivaju na implementaciji sistema industrijske kontrole i operativnih tehnologija. Postoje tri tipa sistema industrijske kontrole: sistem nadzorne kontrole i prikupljanja podataka (SCADA), distribuirani kontrolni sistem (DCS) i programabilni logički kontroleri (PLC) (Matti; Falco). SCADA sistemi generišu ranjivosti, na osnovu svoje namene, karakteristika i rasprostranjenosti, zbog čega predstavlja idealnu metu za sajber teroriste. Ovi sistemi kontrolišu veliki broj industrijskih objekata i sistema koji čine ključnu kritičnu infrastrukturu (Smith, 2014; Weimann, 2004; Charvat, 2009). SCADA sistemi su kompleksni i veliki, dizajnirani su za rad na velikim udaljenostima, zbog čega postoji manja kontrola na mrežama (Dawson, Bacius, Borges, Gouveia & Vassilakos, 2021). Sajber teroristi za napad mogu iskoristiti opšte ranjivosti, odnosno ranjivosti koje postoje u IT proizvodima ili sistemima, zatim tehnološke ranjivosti, kao što su bezbednosne rupe u sistemu, odnosno hardversku ili softversku ranjivost. Pod softverskom ranjivošću se podrazumeva greška u programskom kodiranju, konfiguraciji ili upravljanju, dok je hardverske ranjivosti teško identifikovati (Smith, 2014; Lehto, 2022). Napad na kritičnu infrastrukturu može se realizovati upotrebom trojanskog konja, crva i virusa. Kritična infrastruktura je veoma složena i kompleksna, jer se sastoji od velikog broja sektora. Ovi sektori su međupovezani i međuzavisni, a sektori zavise od proizvoda ili usluge drugog sektora. Gde bi događaj, kao što je oštećenje ili kvar u jednom sektoru, doveo do niza događaja, odnosno stvaranje kaskadnog efekta. Što znači da malo oštećenje ili kvar može dovesti do brojnih nezgoda po svakodnevne aktivnosti ljudi ili odneti stotine hiljada ljudskih života, odnosno može imati katastrofalne posledice (Ahmad & Yunos, 2012; Chu, et al., 2009; Lehto, 2022; Dawson, et al., 2021; Osei- Kye, et al., 2021; Bennett, 2018). U nastavku rada biće analizirane posledice sajber terorističkog napada na sisteme vodosnabdevanja, transportne, komunikacione i sisteme snabdevanja hranom i sisteme zdrastvene zaštite. Ovi sistemi našli su se u fokusu analize, pre svega jer njihovo uspešno funkcionisanje predstavlja kamen temeljac urbane sredine.

Postojanje ljudskog bića i preduzimanje aktivnosti uslovljeno je konzumiranjem vode i hrane. Što jasno ukazuje na povezanost sek-

tora vode i hrane, kao i neophodnost njihovog uspešnog funkcionisanja. Snabdevanje građana higijenski ispravnom vodom omogućava veliki broj vodovodnih preduzeća, koja se sastoje od izvora vode, postrojenja za prečišćavanje, pumpnih stanica, skladišta i obimnih sistema za sakupljanje, distribuciju i nadzor (Lehto, 2022: 33). Svi ovi elementi mogu biti potencijalne mete napada. Prekid vodosnabdevanja izazvan kontaminacijom vode ili nekontrolisanog ispuštanja velike količine otpadnih voda može izazvati brojne posledice i imati kaskadne efekte. Navedeni napadi bi imali najteže posledice po javno zdravlje, zbog nedostatka vode za piće i za higijenu, ali i životnu sredinu (Lehto, 2022: 32–33). Nedostatak hemijski ispravne vode može ugroziti zdrastveni sektor, kroz rapidno povećanje broja pacijenata i nemogućnosti odvijanja medicinskih zahvata. Energetski sektor može biti značajno ugrožen nedostatkom vode, kroz odsustvo mogućnosti proizvodnje električne energije. Ispuštanje velike količine otpadnih voda onemogućilo bi odvijanje železničkog i pomorskog saobraćaja, odnosno imalo bi uticaj na transportni sistem. Takođe, ispuštanje velike količine otpadnih voda imalo bi uticaj na poljoprivredni sistem, kroz kontaminaciju zemljišta ili poljoprivrednih useva, što bi moglo da izazove glad i ugrozi stanovništvo.

Sistem snabdevanja hranom povezan je sa sistemima proizvodnje i obrade hrane (Lehto, 2022: 22–23). Ključna pretnja sistemu snabdevanja hrane je njena kontaminacija. Postoje pretpostavke da je veća šansa za kontaminaciju hrane ukoliko je u tečnom obliku (Jurica i sar., 2019: 241). Metode napada za kontaminaciju hrane mogu se podeliti u dve kategorije: spoljašnji i unutrašnji napad. Kod spoljašnjeg napada kontaminacija se realizuje na mestu gde se hrana proizvodi, prerađuje ili transportuje. Dok kod unutrašnjeg kontaminacija hrane je izvršena u proizvodnom objektu, zboupotrebom legitimnog pristupa zaposlenog hrani (Jurica i sar., 2019). Posledice napada na ovaj sistem su brojne, od ugrožavanja javnog zdravlja, preko privrede, do izazivanja političke i društvene nestabilnosti, nastale kao rezulat pitanja o ispravnosti hrane i njenog nedostatka (Jurica i sar., 2019).

U sistemu zdravstvene zaštite, mete napada su medicinska dokumentacija, informacije o pacijentima i medicinski uređaji. Posledice ovih napada su ugrožavanje bezbednosti informacija, bezbednosti i zdravlja pacijenata, ali i logističkih sistema na koje se oslanjaju bolnice, poput sistema zaliha (Lehto, 2022; Ness & Khinvasara, 2024).

Zabeleženi su slučajevi simuliranih napada na medinske uređaje kao što su pesmejkeri, insulinske pumpe i infuzione pumpe (Ness & Khinvasara, 2024: 111). Sajberteroristički napad bi omogućio uvid u medicinsku dokumentaciju, izmene u zdrastvenim i apotekarskim kartonima, što bi dovelo do lekarskih greški i uzimanja pogrešne terapije. A to bi dalje prouzrokovalo ugrožavanje života ljudi, ali i smrtne ishode (Matusitz & Minei, 2009). U slučaju dužeg trajanja napada može doći do nemogućnosti pružanja zdravstvene zaštite, odnosno kolapsa sistema.

Transportni sistem čine putni, železnički i vazduhoplovni sistem. Ovaj sistem je veliki i kompleksan, tako da postoje brojne potencijalne mete napada. Napad na ovaj sistem mogao bi da ima za posledicu niz nesreća, povrede ili gubitak ljudskih života. S obzirom na to da ovaj sektor ima ulogu protoka ljudi i usluga, napad na njega mogao bi da dovede do ugrožavanja imovine, ljudi i životne sredine. Odnosno, izazvao bi posledice po bezbednost, zdravlje, ekonomsko i socijalno blagostanje stanovništva (Lehto, 2022; Tonn, et al., 2019). Postoji zavisnost transportnog sistema od komunikacionog sistema, koji ima izuzetan značaj jer omogućava komunikaciju i dobijanje pravovremenih informacija.

Usluge koje pruža komunikacioni sistem, u vidu interneta, telekomunikacija, poštanskih usluga i emitovanja, tvori osnovu društvenog funkcionisanja, poslovanja svih preduzeća i predstavlja integralni deo privrede (Lehto, 2022). Napad na ovaj sistem može se realizovati iskorišćavanjem ranjivosti komponenti sistema i potrošačkih uređaja, a koji im može omogućiti pristup podacima, izmenu podataka i komponenti sistema (Lehto, 2022). S obzirom na to da sistem skladišti velike količine osetljivih podataka o pojedincima i kompanijama, uspešan napad na ovaj sistem može ugroziti bezbednost pojedinaca ili poslovanje kompanije, odnosno imati teške bezbednosne i ekonomske posledice.

ZAKLJUČAK

Izgledi za odvijanje sajber terorističkog napada u budućnosti su veliki zbog sve veće povezanosti fizičkog i virtuelnog sveta, karakteristika sajber prostora, ali i formiranja nove generacije terorista, koje karakteriše informaciona pismenost i dobro poznavanje rada raču-

nara. Analiza napada i mogućih posledica na kritičnu infrastrukturu pokazuje da je potrebno raditi na smanjenju ranjivosti i unapređenju otpornosti kritične infrastrukture. Kroz unapređenje zakonodavnog okvira, koji reguliše ovu oblast, osmišljavanjem bezbednosnih rešenja i unapređenjem bezbednosnih procedura, ali pre svega razvojem sajber kulture.

LITERATURA

Ahmad, R., & Yunos, Z. (2012). A dinamic cyber terrorism framework. *International journal of computer science and information security*, 10(2), pp. 149– 158.

Bennett, B.T. (2018). Understanding, assessing, and responding to terrorism: Protect critical infrastructure and personnel. Second edition. New Jersey: John Wiley & Sons.

Charvat, J. (2009). A new dimension in battlespace. In: *The virtual battlefield: Perspectives on cyber warfare* (pp. 77–87). Amsterdam, the Netherlands: IOS Press.

Chu, H.C., Deng, D. J., Chao, H.C. & Huang, Y.M. (2009). Next generation of terrorism: Ubiquitous cyber terrorism with the accumulation of all intangible fears. *International jurnal of computer science and information security*, 15(12), pp. 2373–2386.

Damnjanović, I. (2009). Postoji li sajber terorizam? *Politička revija*, 8(1), str. 237–253.

Dawson, M., Bacius, R., Gouveia, L.B.& Vassilakos, A. (2021). Understanding the challenge of cybersecurity in critical infracture sectors. *Land Forces Academy Review*, 26(1), pp. 69–75.

Dobovšek, B., & Dimc, M. (2012). Cyber terrorism: transference of virtual world threats to the psysical world. U: *Terorizam kao globalna pretnja* (str. 340–352). Novi Sad: Pravni fakultet za privredu i pravosuđe Novi Sad i Centar za bezbednosne studije Beograd.

Jevtović, Z. (2016). Uloga društvenih mreža u promociji sajber terorizma. *Politika nacionalne bezbednosti*, 10(1), str. 99–119.

Jonev, K. (2016). Sajber terorizam i upotreba sajber prostora u terorističke svrhe. *Bezbednost*, 58(2), str. 206–222.

Jurica, K., Vrdovljak, J., & Brčić Karačonji, I. (2019). Food defence system as an answer to food terrorism. *Arhiv za higijenu rada i toksikologiju*, 70(4), str. 232–255.

Lehto, M. (2022). Cyber-attacks against critical infrastructure. In: *Cyber security: Critical infrastructure protection* (pp. 3–42). Cham: Springer International Publishing.

Luknar, I. (2022). *Sajber terorizam: mere za suzbijanje i prevencija*. Beograd: Institut za političke studije.

Matusitz, J., & Minei, E. (2009). Cyberterrorism: Its effects on health-related infrastructures. *Journal of digital forensic practice*, 2(4), pp. 161–171.

Ness, S., & Khinvasara, T. (2024). Emerging threat in cyberspace: implications for national security policy and healthcare sector. *Journal of engineering research and reports*, 26(2), pp. 107–117.

Osei-Kyei, R., Tam, V., Ma, M., & Mashiri, F. (2021). Critical review of the threats affecting the building of critical infrastructure resilience. *International Journal of Disaster Risk Reduction*, 60, 102316.

Post, J. M. (2005). The socio-cultural underpinning of terrorist psychology: "When hatred is bred in the bone". In: *Root causes of terrorism* (pp. 72–87). New York: Routledge.

Smith, R. (2014). *The cyber terrorism threat to critical infrastructure*. Master thesis. New York: Utica college.

Tonn, G., Kesan, J., Zhang, L., & Czajkowski, J. (2019). Cyber risk and insurance for transportation infrastructure. *Transport policy*, 79, pp. 103–114.

Weimann, G. (2004). *Cyberterrorism How Real Is the Threat?*. Washington: United states institute of peace.

Zakon o kritičnoj infrastrukturi Republike Srbije („Službeni glasnik RS"), br. 87/18.

CYBER TERRORISM AS A SECURITY THREAT IN URBAN SPACE

SUMMARY

The rapid development of information and communication technologies (ICT) in recent decades has produced, in addition to positive changes, in the form of faster and easier communication and the overall progress of society, a wide range of negative phenomena and the development of new forms of security threats and risks. Among the numerous threats in cyber space, cyber terrorism stands out. The Covid-19 pandemic has led to accelerated technological development in the field of ICT, where a significant part of communication has been moved from real to virtual reality. Cyber space is nourished by a large amount of information, of various categories and degrees of secrecy. Bearing in mind that this space has a large number of manifestations and the very characteristics of the space, in the form of the absence of geographical restrictions and the possibility of acting from a great distance, providing anonymity to the perpetrator and difficult visibility of the consequences, there are great prospects for the development of a cyber terrorist attack in the near future. There is no generally accepted definition of cyber terrorism in the literature, but we can accept the definitions, which present it as a criminal act in cyberspace, by misusing computer networks, the aim of which is to endanger vital national infrastructure, coercion and intimidation of the Government and/or its citizens. The consequences of cyber terrorism according to their severity can be divided into three categories, the first is the alteration or theft of information and the temporary interruption of the work of institutions, the second category is a series of coordinated attacks, which affects decision-makers, and the third is an attack on critical infrastructure, which causes disruptions in functioning critical infrastructure or its damage. This paper contributes to the understanding of cyber terrorism, with special reference to the analysis of attacks on critical infrastructure, which is mainly concentrated in urban areas, and the possible consequences for key service systems of water supply, transport, communication and food supply systems or health care systems.

KEYWORDS: *cyber space, cyber terrorism, critical infrastructure.*