DOI: 10.5937/MegRev2102223K

Stručni članak

Primljen 16.04.2021.

Odobren 21.04.2021.

HAKERSKI NAPADI KAO OBLIK SAJBER TERORIZMA**

Apstrakt: *Kako smo upućeni intenzivno i nezaobilazno na sve sadržaje koji su nam od značaja upravo na internetu broj hakerskih napada je po logici stvari sve učestaliji. Ovaj fenomen upozorava da su svi bezbednosni sistemi država na stalnom udaru opasnosti sajber terorizma. U ovom radu biće analiziran hakerski napad kao pojava, kao posledica i uzrok, ali i kao instrument sajber terorizma. Svrha rada je da se ukaže na one elemente ovog vida terorizma koji nisu adekvatno predstavljeni, a samim tim ni prepoznati na način na koji bi trebalo shvatiti ih ozbiljno i suprotstaviti im se. U radu su izneta zapažanja koja imaju cilj da ukažu na put kojim bi hakerski napadi mogli biti suzbijani i presretani.*

Ključne reči: *hakerski napadi, sajber bezbednost, sajber terorizam, antiterorizam, bezbednost, haker, hakovanje, teroristi.*

* Pravni fakultet, Megatrend univerzitet, Beograd, Srbija; sanja_klisaric@yahoo.com

** Ovaj rad je rezultat projekta FPMIRS – Znanjem do integrisanja u društvene i ekonomske tokove. Projekat je pokrenut sporazumom Pravnog fakulteta sa Međunarodnim institutom za romološke studije.

1. Uvod

Kako danas jasno uviđamo da je svet zauzeo jednu novu dimenziju postojanja u sajber prostoru postavlja se pitanje jesmo li dovoljno pripremljeni za izazove koji nas čekaju tom svetu. Ako se sve što postoji sve intenzivnije izlaže i skladišti upravo na samom internetu, rizik od napada na sve sadržaje je nešto što treba da očekujemo. Izazov sa kojim se suočavaju sve države sveta predstavlja odbrana od hakerskih napada koji gotovo bez i jedne sekunde prestanka napadaju sve moguće sisteme kojima imaju mogućnost da pristupe. Samo značenje reči haker označava osobu koja je sadrži veoma napredne veštine u korišćenju računarskih sistema i tehnika, neretko koristeći svoje znanje za malverzacije ma kog softverskog ili informacionog tipa u sajber prostoru. Primarno su to bili samouki pojedinci koji su ovakve napade vršili iz ličnih razloga na korporacije i pojedince ali vremenom ovaj model nemoralnog postupanja u sajber prostoru preuzeli su teroristi formirajući dinamičnu hakersku terorističku snagu u sajber prostoru. Hakovanje ne mora da predstavlja negativan odnos prema sajber sistemima kakav je on to bio primarno kada je postao svetski fenomen. Vremenom smo naučili da hakovanje ne mora da bude isključivo protivzakonito jer imamo tu vrstu prakse i vidu bezbednosnih mera kada se sumnjivim licima ili organizacijama ulazi u sisteme kako bi se utvrdila ili presrela neka informacija od značaja za borbu protiv kriminala ili terorizma. Sa te strane države stoje iza hakera omogućavajući im legitiman rad unutar državnih institucija. Objektivno govoreći da države nemaju hakere sa svoje strane, bilo bi iracionalno diskutovati o sajber odbrani sistema. Unutar hakovanja je obavezno podrazumevano lažno predstavljanje kojim se maskira ne samo identitet hakera već i lokacija kao i uređaj sa kog vrši napad. Suštinski, sam hakerski napad je uvek upad na nedozvoljeno ili nepristupačno sajber polje sa kog se otuđuju informacije u cilju koji je značajan za hakera ili njegove nadređene. Onda kada smo svesni šta znači haker jasno nam je da je hvatanje u koštac sa zanimanjem koje istovremeno može da ima i pozitivnu u negativnu sajber ulogu, problem sajber terorizma postaje logično povezan sa njim. Zbog toga svaki hakerski napad treba posmatrati sa dosta opreza.

2. Sajber terorizam kao oružje hakera

Još 1984.godine je bilo objavljeno da su hakeri kako je tada rečeno heroji kompjuterske revolucije.¹ U knjizi koja je tada objavljena kao značajan korak ka objašnjavanju same suštine hakovanja i hakera izneta su objašnjenja o ovoj pojavi ukazujući na sve one elemente hakovanja koji su tada bili zastupljeni. Tu se navode etički principi hakovanja i njihova zastupljenost u popularnoj kulturi. Interesantno je da autor navodi da hakeri obavljaju dužnost za opšte dobro

¹ Levy, S. (1984): *Hackers: Heroes of the Computer Revolution* Garden City, New York

na neki način ostvarujući ulogu "Robin Huda".² Ovako nešto sa sigurnošću možemo da kažemo da je jedan od pokretača hakera koji zauzimaju sajber prostor kao sajber teroristi. U njihovoj svesti stvari su postavljane tako da će njihov napad oštetiti one koje oni smatraju da treba da budu oštećeni, a na osnovu toga pomoći drugima čiju stranu predstavljaju. Upravo ovaj postulat koji je naveden u pomenutoj knjizi je inkorporiran u današnji sajber terorizam. Interesantno je da je autor tokom rada na ovoj knjizi razgovarao sa velikim brojem hakera koji su operisali od 1950. do 1980. Ako tome pridodamo činjenicu koju autor navodi da se na hakere gleda sa određenim divljenjem, da se oni tumače kao umetnici, slobodoumni vizionari, avanturisti, zaključujemo da se na njih gleda sa simpatijama.³ Međutim, treba naglasiti da je od pojave prvih hakera kako stoji u tekstu prošlo više od sedamdeset godina. Ovaj protok vremena uslovio je njihov razvoj usklađen razvojem tehnologija, ali i potrebama društva i grupacija unutar naše civilizacije koje su prepoznale svoju poziciju u sajber terorizmu kroz prizmu hakerskih operacija ili napada. U tom trenutku sam hakerski napad više nije umetničko delo, niti junački čin iako za počinioce to svakako jeste, već ima kriminalnu i terorističku implikaciju.

Isti autor je objavio više knjiga na ovu temu i pratio razvoj hakera kroz vreme. No, nakon evolucije hakera, hakerskim veštinama počinju da se koriste veoma drugačiji tipovi ljudi od onih koje su do tog određenog trenutka predstavljali hakeri. Polako, a zatim sve masovnije hakeri postaju sajber teroristi.⁴ Kodiranje na internetu i unutar sigurnosnih operativnih sistema je meta hakera koji razbijanjem tih kodova dolaze do željenih informacija. Na ovaj način raspoloživost informacija dovodi svaki targetirani sistem u stanje kompromitacije, labilnosti, izloženosti i svakako u ruke hakera koji su unutar sajber terorizma pokazali svoju osnovnu nameru zbog koje je i nastao pojam sajber terorizam. Ali upravo nekontrolisano narastanje sajber terorizma predstavlja krucijalni problem za sajber bezbednost jer ne postoji način da se čitav proces kontrole obavi tako da svaki napad bude sprečen. Jednostavno nastaje neretko veoma haotična situacija u praćenju određenih sumnjivih hakera dok sa druge strane neko može u deliću sekunde da upadne u sistem hakerskin napadom jer sajber teroristi ostavljaju utisak da su još manje predvidivi od tradicionalnih terorista.⁵ Ovoj činjenici u prilog ide i fakat da na dnevnom nivou na celom svetu se svakog dana beleži više stotina miliona hakerskih napada.⁶ Ovaj podatak nam jasno pokazuje koliko je zahtevan posao službi sajber bezbed-

² Ibid.

³ Ibid.

⁴ The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States (9/11 Report), (2004), p.88. <https://www.govinfo.gov/app/details/GPO-911REPORT>

⁵ Peter R., Trim, J. (2003): *Public and Private Sector Cooperation in Counteracting Cyberterrorism*, International Journal of Intelligence and Counterintelligence, 16: p.594–608

⁶ <https://threatmap.checkpoint.com/>

nosti i koliko je teško ući u trag hakerima. Ovom prilikom se čak ni ne naglašava sama tehnologija rada, specijalne alatke, programi i vještine hakera, kao zaštićen sajber prostor na kom hakeri realizuju sajber terorizam. To je ogromno polje, najčešće u neprekidnom narastanju i razvoju sa stalnim razvojem vještina koje hakere udaljavaju od njihovih sajber kolega koji pokušavaju da im uđu u trag. Apsolutno sve na internetu od mejla do IP adrese može biti lažni trag koji je podmetnut kako bi se zatro trag hakera. Zbog ovoga postoje neophodni protokoli koji moraju da se koriste kako bi se ne samo Vlade, već i kompanije, zaštitile od sajber terorizma.

Ranije je bilo teško formirati sliku zbog previše malo detalja, dok se danas dešava upravo suprotan fenomen. Preveliki broj informacija u sajber prostoru omogućava da se gubi trag počinocima. Danas je veoma teško preskočiti enorman broj prepreka i lažnih tragova kako bi se došlo do počinilaca što suštinski veoma komplikuje sistem odbrane.⁷ Kada znamo da je tako, pred bezbednosnim sistemima se postavlja gotovo nerešiv zadatak. Sa druge strane raspoložemo enormnim tehničkim mogućnostima praćenja svih uređaja na planeti koji su u stanju da detektuju pretnje po sajber bezbednosne sisteme.⁸ Sasvim je jasno da je internet u stalnom rastu i razvoju sklon opasnostima koje prate tu dramatičnu ekspanziju sadržaja, informacija i podataka koji se mogu naći na internetu. Upravo sve ono što je na internetu može da devastira sisteme koji su izložili te informacije u taj prostor i na taj način omogućili sopstvenu ranjivost. Ali sajber bezbednost je u poziciji da sačuva svoje sisteme protokolima koji su obavezni deo svakog sistema. Međutim, sajber svet se neprekidno usložnjava i raslojava i na taj način sajber teroristi imaju prostor da svojim hakerskim vještinama u nepreglednom moru svih mogućih sadržaja imaju čitave sisteme koji ih štite. Ova opasnost sistema koji su izloženi na internetu, iako ima snažnu zaštitu najznačajnijih meta sajber terorista, u stalnoj je opasnosti da bude probijena. Ne postoji garancija za očuvanje nekog sistema Ali, treba napomenuti da strahovito uvećavanje informacija na internetu ukazuje na neprekidnu opterećenost bezbednosnih sistema i stalno narastanje opasnosti koja im preti. Jer u tolikom broju informacija, vještina pronalazjenja pravih tragova za kojima se stremlje je izuzetna. i bezbednosne agencije koje se bave praćenjem opasnosti koja preti sa interneta suočavaju se sa činjenicom da se količina tih informacija koje su značajne za analizu neprekidno uvećava.⁹ Sajber terorizam zahteva neprekidnu i kontinuiranu ne samo borbu i suprotstavljanje bezbednosnih struktura nego o njihovu neretku mimikriju unutar hakerskih sajtova i udruženja radi provaljivanja u sisteme kojima bi se narušila bezbednost onih ustanova, institucija i organizacija koje zastupaju. U ovom poslu odbrana mora da bude ispred napada, jer kada uspostave ravnotežu strana, postiže se brz

⁷ Hollywood, J., Snyder, D., McKay, K., Boon, J. (2004): *Out of the Ordinary Finding Hidden Threats by Analyzing Unusual Behaviour*, RAND Corporation, Santa Monica, California, pp. 23

⁸ Winston, T. (2007): *Intelligence Challenges in Tracking Terrorist Internet Fund Transfer Activities*, International Journal of Intelligence and Counterintelligence, vol-20, p. 327-343.

⁹ Tiboni, F., (12 June 2000): *Difficulty Grows for US Intelligence Gathering*, Space News, p.1

proboj suprotne strane, pošto onda kada popusti gard odbrane, hakeri imaju proboj dovoljan da se sistem dovede u stanje u kom će možda, ne sam napad po sebi, ali neretko posledice napada izazvati sajber terorizam.

3. Sajber terorizam kao poprište nesagledivih sukoba

Ako postanemo racionalni po pitanju sajber prostora možemo da naslutimo formiranje sajber nacija unutar sajber sistema koje bi bile interesno povezane. Hakeri sa obe strane funkcionišu tako da koriste alatke i veštine koje bi mogle da se nazovu oružjem sukoba koji vode, a sam interes bi objedinio ljude različitog porekla na osnovu iste ideologije ili interesa. U ovom kontekstu treba analizirati hakere kao ratne strane sajber prostora čije aktivnosti realizuju sajber terorizam kao manifestaciju svojih agendi. Da li je racionalno smatrati da ovakvi sukobi mogu ma na koji način da jenjavaju, naravno da nije. Sama struktura sajber prostora je jedan veoma složen sistem gotovo univerzum koji se neprekidno razgranava. Ako jedan svet ima stalnu inerciju ka rastu i razvoju, sasvim je logično očekivati jednak razvoj opasnosti koja sledi iz takvog jednog polja stvarnosti. Sam terorizam ima mogućnost praćenja u skladu sa protokom sadržaja koji su neophodni da bi se teroristički napad izveo. U sajber svetu pratiti sekvence terorističkog napada je daleko teže zbog neverovatno velikog broja informacija koje se neprekidno umnožavaju. Opšte je poznato da velike bezbednosne agencije prikupljaju ogroman broj informacija sa kojima ne znaju šta da rade i koje zapravo zagušuju analitički prostor.¹⁰ Suština raslojavanja stvarnosti u sajber prostoru deli se na opasnosti veće ili manje po sisteme i svaka sajber odbrana ovome pristupa sistematski. Ono što odlikuje sajber terorizam je drastična inventivnost koja nastaje gotovo u hodu dok tradicionalni terorizam ima svoje klasične vidove ispoljavanja i prikazivanje koje je praćeno drugim ustaljenim metodama.

Virtuelni svet omogućava veoma veliki stepen kreacija unutar svih sistema i na taj način slobodu vidljivih ali i nevidljivih sajber lica. Taj svet omogućava nesmetano istraživanje i ispoljavanje svojih namera jer je sam prostor kreiran tako da postoje realni ogranci samog sistema koji ne moraju biti vidljivi za sistem kao takvi, a visoko rizični i ranjivi kada se aktiviraju. Na otkrivanju opasnosti rade stručnjaci čije znanje se neprekidno nadograđuje i sam posao sajber inženjera ili sajber obezbeđenja je posao visoko stresan kako zbog samih opasnosti sa kojima se suočavaju na radnom sajber prostoru, tako iz zbog fizički i psihički gotovo nadrealne radne i intelektualne dinamike. Sasvim smo svesni da je sajber univerzum savršen svet za teroriste jer danas lakše nego ikad oni imaju pristup svim željenim informacijama koje se tiču njihovih meta.¹¹ Sama sajber bezbed-

¹⁰ Ackerman, K. Robert (October 1999): *Security Agency transformations From Backer to Participant*, Signal, note 152.

¹¹ Weinman, G. (2004): "How Modern Terrorism Uses the Internet". USIP Special Report, n° 116, p. 3.

nost kada se zna na šta se tačno odnosi postavlja se pitanje može li da realizuje svoj zadatak. Ako znamo da sajber bezbednost ima za cilj da zaštiti kompjutere, servere, mobilne telefone, uređaje priključene na električno napajanje koji su praćeni modernom tehnologijom, mreže i podatke koji su ugroženi napadom pitamo se da li je objektivno verovati da sistemi koji imaju zadatak toliko toga da obezbeđuju mogu sve to da obavljaju kada znamo da tehnologija kako raste, tako se i broj hakerskih napada uvećava. Mi zapravo, imamo zvanične podatke koji svakodnevno govore o napadima koji su brojniji iz dana u dan.¹² Početkom 2021. godine konkretno, zabeleženo je u jednom danu 50 miliona napada, da bi taj broj napada skočio na preko 100 miliona napada krajem marta meseca, a da bi broj napada 6. aprila dostigao oko 300 miliona napada u 24h na celoj planeti.¹³ Na osnovu ovoga zaključujemo da hakeri imaju svoje taktike koje razrađuju jednako kako se razvijaju sajber tehnologije i odbrana. Poznato je da je komunikacija i deljenje informacija putem kriptovanih poruka u značajnom broju puta olakšalo organizaciju, planiranje i komunikaciju tokom pripreme terorističkih napada.¹⁴ Ako to znamo i ako znamo da u jednom danu imamo oko 300 miliona napada zabeleženih širom sveta, ne čudi li nas činjenica da hakeri predstavljaju ozbiljne snage sajber terorizma. Hakeri su tokom vremena evoluirali kako je tehnologija napredovala, ali i kako su se menjale političke okolnosti. Svet se oblikuje prema onoj stvarnosti koja ga definiše, a to su svakako istorijska, politička, tehnička i socijalna dešavanja. Svet hakera se usklađuje sa svim tokovima naše stvarnosti i onda kada je terorizam uočio da je sajber svet nova zona njihovog manifestovanja sajber bezbednost je doživela ozbiljan izazov u borbi protiv hakerskih napada. U pitanju nije zaštita samih sistema već i čitavih država jer hakeri koji su postavljeni u službu sajber terorizma imaju za cilj kao i svi drugi teroristi da nanesu štetu, unesu paniku, neizvesnost i strah, ali i da demonstriraju svoju nadmoć u sukobima koji su usklađeni sa njihovim ciljevima.

Jednu stvar treba naglasiti, a to je diferencijacija između hakera i sajber terorista. Naime, hakeri nisu automatski sajber teroristi. Oni mogu biti sastavni deo sajber terorizma, ali suštinski haker ne mora da bude terorista. Ova distinkcija je veoma značajna, Ali je činjenica da takozvani "beli hakeri" mogu preći na drugu stranu i postati "crni hakeri" koji su zaslužni za protivzakonite upade u sajber prostor, ali i obrnuto. Mi, iako znamo da hakeri fundamentalno nisu teroristi i da njihova priroda nije primarno fokusirana na terorizam, ne možemo, a da ne uzmemo u obzir svakodnevno povećavanje sajber napada koji imaju indicije da budu teroristički. Jer onda kada se hakuju vladine institucije jasno je da namera nije samo pokazati nadmoć nego i postići neki konkretan cilj. Targetiranje privatnih kompanija nema

¹² <https://threatmap.checkpoint.com/>

¹³ Ibid. (pristupljeno 7.4.2021.)

¹⁴ The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States (9/11 Report), (2004), p.88. <https://www.govinfo.gov/app/details/GPO-911REPORT>

terorističke motive ukoliko te kompanije nisu u uskoj sprezi sa vladama država i obavljaju za pitanja države značajne poslove. Hakerskim napadima na privatne firme motivi su uglavnom svodivi na trku na sajber tržištu, krađu informacija, tehnologija, platnih sredstava, kao i suzbijanje konkurencije. Hakovanjem državnih institucija uvek pretila opasnost od sajber terorizma i zbog toga hakeri sada više nisu neutralni provalnici sistema unutar sajber prostora već i veoma značajne snage potencijalnog ili očekivanog terorističkog napada.

Razlog za ovo uverenje je u enormnom broju napada samo na dnevnom nivou koji targetira državne institucije i čiji napadi ne bi mogli biti realizovani bez takozvanih "crnih" hakera čiji je cilj da provali u sisteme sa ciljem koji je nametnut u njihovoj terorističkoj agendi. Brojeve o dnevnim napadima možemo, kao i same napade da posmatramo u realnom vremenu upravo na samom internetu.¹⁵ Činjenica da postoji mogućnost da se napadi registruju i postavljaju istovremeno na internet ukazuje na stalno porprište sukoba koji su aktuelni u svakom trenutku. Naime, političkim okolnostima uslovljeni događaji imaju osnova da indukuju sve više hakera u sajberterorizam na osnovu njihovih opredeljenja, stavova i ideologija. Postoji realna neodgovornost ukoliko iko postavi hakere po strani kao neutralne snage unutar terorizma koje su stvar incidentnosti, a ne pravila. Gotovo je jasno da sajber prostor ne može da bude ugrožen ni na koji drugi način u smislu kompromitovanja informacija, urušavanja ili targetiranja sistema, rušenja sajtova i krađe podataka i onesposobljavanje aktivnosti koje su podrazumevane. Sam sajber prostor je polje delanja hakera u svetlu one strane koju zastupaju.

Treba istaći činjenicu da će sajber terorizam biti kontinuirana i trajna pretnja.¹⁶ Na osnovu ovog stava i današnjeg života koji je gotovo celokupno prenet na internet i sajber prostor, kako lični, tako i poslovni sadržaji, ali i zdravlje i operativni sistemi koji to kontrolišu, jasno nam je da svet nije suočen sa aktuelnom, lokalnom i trenutnom pretnjom, već sa ozbiljnom planetarnom opasnošću po čitavu civilizacijsku bezbednost koja je stalna i ekspanzivna. Hakeri nisu više ostrva u sajber prostoru, već čitavi okeani čija plima poplavljuje sajber prostor preteći svim sistemima i primenljivim zaštitama jer je posao koji oni obavljaju upravo probijanje barijera zaštite. Onda kada se podaci jednom kompromituju lančanom reakcijom sajber terorizam ugrožava sve segmente stvarnosti povezane sa internetom od medicinskih zahvata koji se obavljaju preko interneta, do električnih i sigurnosnih sistema, kao i najznačajnijih bezbednosnih podataka državnih i vladinih institucija pohranjenih na internetu. U samoj knjizi, zapravo priručniku pod nazivom "Enciklopedija Al Kaide" koji se može naći na internetu, pored detaljnog uputstva za pravljenje eksplozivnih napada, organizaciju i realizaciju terorističkih napada, imate precizno i sadržajno iznete metode i načine prikupljanja podataka, njihove obrade i manipulacije, kao i uputstva za

¹⁵ <https://threatmap.checkpoint.com/>

¹⁶ <http://www.computerworld.com/securitytopics/security/story/0,10801,63965,00.html>

terorističke napade.¹⁷ Ako znamo da postoji priručnik sa uputstvima za terorističke napade, u kom se daju instrukcije za prikupljanje podataka, jasno nam je da u okviru te terorističke organizacije, a nesumnjivo i ma koje druge, hakeri imaju značajnu ulogu. Sama terorizam evoluira.¹⁸ Sajber terorizam je jedan od osnovnih pokazatelja za ovu tvrdnju. A unutar sajber terorizma sama problematika sajber terorizma se usložnjava kreirajući onoliko prostora koliko je neophodno da se utrka hakera svodi na sa ove tačke gledišta nikad nezavršiv sukob.

Zaključak

Kako su hakerski napadi vremenom postajali sve intenzivniji, sam teroristički koncept uvrstio ih je u sektor svog oružja unutar sajber prostora. Iako je činjenica da sami hakeri ne moraju biti po inerciji teroristi, nego znamo da postoje i takozvani “beli” hakeri koji rade za državne i vladine institucije, nastanjem terorizma unutar sajber prostora, povećava se i broj hakera koji su imponentne snage sajber napada uvrštenih u agende terorističkih organizacija. Kako je svet sve kompleksniji i prisnije važan za internet i moderne tehnologije, treba da očekujemo sve više tih napada koji će za cilj imati trajno i konstantno targetiranje svojih neprijatelja, kao i destabilizaciju i urušenje haosa unutar država čije institucije budu ciljale u svojim sajber napadima. Imajući sve navedeno u vidu preporučuje se i očekuje da države izdvajaju sve veća sredstva za sajber bezbednost kao i ulaganje u “bele” hakere u cilju zaštite kako državnosti, tako i bezbednosti svojih građana i institucija od sajber terorizma.

¹⁷ Bakier, Abdul Hamied. (july 13, 2006): “*Jihadis Adapt to Counter Terror Measures and Create New Intelligence Manuals*”. Terrorism Monitor, vol. 4, n° 14, pp. 1-2.

¹⁸ Klisarić, Sanja (2019): “Žene teroristi u periodu od 1979.godine do 2016. godine.”, Doktorska disertacija

Literatura:

- Ackerman, K. Robert (October 1999): *Security Agency transformations From Backer to Participant*, Signal, note 152.
- Bakier, Abdul Hamied. (july 13, 2006): "Jihadis Adapt to Counter Terror Measures and Create New Intelligence Manuals". Terrorism Monitor, vol. 4, n° 14, pp. 1-2.
- Hollywood, J., Snyder, D., McKay, K., Boon, J. (2004): *Out of the Ordinary Finding Hidden Threats by Analyzing Unusual Behaviour*, RAND Corporation, Santa Monica, California, pp.23
- Klisarić, Sanja (2019): "Žene teroristi u periodu od 1979.godine do 2016.godine.", Doktorska disertacija
- Levy, S. (1984): *Hackers: Heroes of the Computer Revolution* Garden City, New York
- Peter R., Trim, J. (2003): *Public and Private Sector Cooperation in Counteracting Cyberterrorism*, International Journal of Intelligence and Counterintelligence, 16: p.594–608
- States (9/11 Report), (2004), p.88. <https://www.govinfo.gov/app/details/GPO-911REPORT>
- <https://threatmap.checkpoint.com/>
- Tiboni, F., (12 June 2000): *Difficulty Grows for US Intelligence Gathering*, Space News, p.1
- The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United
- Weinmman, G. (2004): "How Modern Terrorism Uses the Internet". USIP Special Report, n° 116, p. 3.
- Winston, T. (2007): *Intelligence Challenges in Tracking Terrorist Internet Fund Transfer Activities*, International Journal of Intelligence and Counterintelligence, vol-20, p. 327–343.
- <https://threatmap.checkpoint.com/>
- <http://www.computerworld.com/securitytopics/security/story/0,10801,63965,00.html>

DOI: 10.5937/MegRev2102223K

Expert article

Received 16.04.2021.

Approved 21.04.2021.

HACKER ATTACKS AS A FORM OF CYBER TERRORISM

Summary: *As we are referred intensively and inevitably to all the contents that are important to us on the Internet, the number of hacker attacks is by the logic of things, more and more frequent. This phenomenon warns that all state security systems are under constant threat from cyber terrorism. This paper analyzes the hacker attack as a phenomenon, as a consequence and cause, but also as an instrument of cyber terrorism. The purpose of this paper is to point out those elements of this type of terrorism that are not adequately represented, and thus not recognized in a way that should be taken seriously and opposed. The paper presents observations that aim to point out the way in which hacker attacks could be suppressed and intercepted.*

Keywords: *Hacker attacks, Cyber security, Cyber terrorism, Antiterrorism, Security, Hacker, Hacking, Terrorists.*