doi: 10.56461/ZR_24.LAJT.08

Dr *Mirjana Glintić**

SAJBER-RAT KAO OSNOV ISKLJUČENJA OBAVEZE OSIGURAVAČA**

Apstrakt: *Sajber-napadi prouzrokovani NotPetya virusom pričinili su veliku imovinsku štetu kompanijama širom sveta. Kompanije koje su imale zaključene ugovore o različitim vrstama imovinskih osiguranja obratile su se svojim osiguravačima sa zahtevima za naknadu štete. Međutim, osiguravači su se pozvali na klauzule o isključenim ratnim rizicima, uz obrazloženje da su pomenuti napadi deo rusko-ukrajinskog sukoba i da stoga njihova obaveza prema drugoj ugovornoj strani ne postoji. Budući da su dve američke kompanije pokrenule sudske postupke protiv svojih osiguravača, autorka centralni deo rada posvećuje analizi krajem prošle godine donetih sudskih odluka o ovom pitanju. Pozitivnopravna analiza propisa međunarodnog javnog prava kao i opštih i posebnih uslova osiguranja ukazala je na nekoliko nedostataka u argumentaciji osiguravača o isključenosti njihove prestacije. Prvi nedostatak se tiče nemogućnosti osiguravača da dokažu da sajber-napad predstavlja ratnu akciju jedne države protiv druge. Drugi nedostatak se tiče činjenice da su sajber-napadi usmereni protiv kompanija, a ne protiv suverenih država. U radu su dati i određeni predlozi za izmene polisa osiguranja, a u pravcu preciziranja pojma sajber-napada i uslova za primenu klauzule o isključenim ratnim rizicima. U zaključnom delu rada autorka daje argumente u korist tvrdnji da se polisa uvek ima tumačiti u korist pokrića, a posebno onda kada ne postoje nikakve indicije da se o klauzuli o isključenju rizika uopšte pregovaralo i kada je u polisi korišćen standardni jezik.*

Ključne reči: osiguranje, isključeni ratni rizici, sajber-napad, sajber-rat, *NotPetya*.

1. UVOD

Pitanje sajber-rata gotovo da se nije ni postavljalo do 2007. godine kada je započela serija sajber-napada iz Talina.[1] Tada se po prvi put počelo govoriti uopšte o kovanici *sajber-rat*. Dotada su sajber-napadi bili koncentrisani oko povrede zaštite podataka i odgovornosti trećih lica. Ipak, sa geopolitičkom i ekonomskom nestabilnošću, uz sve veće oslanjanje društva na digitalne tehnologije,

* Naučna saradnica, Institut za uporedno pravo, Beograd; e-mail: m.glintic@iup.rs

** Rad je nastao kao rezultat naučnoistraživačkog rada Instituta za uporedno pravo koji finansira Ministarstvo nauke, tehnološkog razvoja i inovacija Republike Srbije prema Ugovoru o realizaciji i finansiranju naučnoistraživačkog rada NIO u 2023. godini (evidencioni broj: 451-03-47/2023-01/200049 od 3. 2. 2023).

1 O navedenim napadima može se više naći na McGuinness, D., 2017, *How a CyberAttack Transformed Estonia* (https://www.bbc.com/news/39655415, 13. 3. 2023).

porasli su i sajber-rizici. Razvoj tehnologije uveo je nove ratne tehnike koje ne uključuju bombe ili kopnene snage („*cyber Pearl Harbour*“),[2] iako se internet može posmatrati kao inferiornija zamena za kopnene sile korišćene za prinudu i osvajanje. Preko noći se javila zabrinutost zbog ove pretnje, koja se čak ocenjuje i kao opasnija od klasičnih i konvencionalnih vidova ratovanja.

Upozorenja o sajber-napadima pristigla sa svih strana sveta učinila su da privredna društva sve više nabavljaju različite vrste osiguranja koje će pružiti zaštitu njihovoj imovini za slučaj da bude meta sajber-napada. Statistički gledano, veoma mali broj kompanija je dugo vremena uopšte bio osiguran protiv sajber-rizika.[3] One kompanije koje su pak osigurane od sajber-rizika, tu zaštitu su postizale putem sajber-osiguranja,[4] putem osiguranja prekida rada,[5] ali i putem klasičnih imovinskih osiguranja – *all risk* insurance. Međutim, iako su kompanije verovale da poseduju bilo kakvu zaštitu od imovinske štete izazvane sajber-napadima, serija napada izazvana *NotPetya* virusom 2017. godine pokazala je da to zapravo i nije slučaj.

Kompanije širom sveta pogođene *NotPetya* virusom koje su imale zaključena *all risk* imovinska osiguranja obratile su se svojim osiguračima radi naknade štete pokrivene osiguranjem. Iznenađeni neočekivano velikim gubicima, osiguravači su nastojali da iznađu način kako da ne izvrše obaveze prema osiguranicima, koje su bile ogromnih novčanih razmera. Njihov odgovor je bio da ne postoji obaveza osiguravača po osnovu ugovora o osiguranju, s obzirom na to da je Ukrajina godinama bila meta hakerskih napada koji su povezani sa Rusijom, kao i da se *NotPetya* sajber-napad desio tokom trajanja rusko-ukrajinskog sukoba. Stoga se, prema mišljenju osiguravača, imala primeniti klauzula o isključenim ratnim rizicima. Pored toga, brojne izjave zvaničnika i predstavnika velikog broja zemalja predstavljale su dodatni argument u korist tvrdnji da je reč o ratnoj operaciji, bar iz vizure osiguravača. Nezadovoljne dobijenim odgovorom osiguravača, nekoliko američkih kompanija je pokrenulo sudske postupke koji su dobili svoje epiloge krajem prošle godine.

2. ISKLJUČENI RATNI RIZICI

Neke začetke klauzula o isključenim ratnim rizicima srećemo još u XVII veku, ali uglavnom u kontekstu pomorskog osiguranja, gde zapravo nije vršeno

2 Goldman, E., Warner, M., Why a Digital Pearl Harbour Makes Sense... and Is Possible, in: Perkovich, G., Levite, A. (eds.), 2017, *Understanding Cyber Conflict*, Washington, Georgetown University Press, pp. 147–157.

3 Swiss Re Institute, 2022, *Cyber Insurance: Strengthening Resilience for the Digital Transformation*, p. 2.

4 Tošić, I., Novaković, O., 2021, Osiguranje od internet rizika i nova regulativa u oblasti zaštite podataka o ličnosti, *Prouzrokovanje štete, naknada štete i nova regulativa u oblasti zaštite podataka o ličnosti*, Institut za uporedno pravo, Udruženje za odštetno pravo, Beograd, Mionica, str. 468.

5 Glintić, M., Schicksal der Betriebsschliessungsversicherung vor den deutschen und österreichischen Gerichten, in: Rohrbach, W. (Hrsg), 2022, *Wertewandel und Werterenaissance in Zeiten der Pandemie und Klimakrise*, Belgrad-Wien, s. 546–550.

eksplicitno razdvajanje morskih i ratnih rizika.[6] Međutim, o razvoju isključenih ratnih rizika u današnjem smislu i njihovoj obimnijoj upotrebi možemo govoriti tek u periodu između dva svetska rata.[7]

Razlozi za isključenje rata su njegova izuzetno razarajuća dejstva, nepredvidivo trajanje i pravac kretanja. Posledično se osiguravači ograđuju od pokrivanja šteta nastalih usled ratnih dejstava, jer ih ne mogu predvideti i kontrolisati, a uz to postoji opasnost od agregacije šteta.[8] Nijedno tržište osiguranja nije u stanju da snosi troškove nastale usled značajnih rizika.[9] Pored toga, smatra se da postoje i moralni razlozi da se isključi obaveza osiguravača u slučaju rata, jer bi pokrivanje tako nastalih šteta davalo legitimitet ratnim aktivnostima.[10]

Ispitivanje isključenja ratnih rizika je i dalje aktuelna tema i o njoj se nije toliko diskutovalo u kontekstu sajber-napada do pre neku godinu. Problemi sa kojima su se susrela privredna društva pogođena sajber-napadom *NotPetya* pokazali su da sajber-rizici nisu dovoljno dobro percipirani i procenjeni jer se očekivano javio problem agregacije šteta nastalih iz istog osiguranog slučaja ili povezanih događaja. Istovremeno, ako se isključi sajber-osiguranje za sve te napade koje su podržale države, onda su sve te kompanije na velikom udaru

6 Grande ordonnance de la marine, du mois d'aoûst 1681. Upor. sa slučajem *Carter v. Boehm* koji je za krajnji ishod imao isplatu sume osiguranja uprkos postojanju ratnih okolnosti. O značaju ovog slučaja za razvoj načela krajnje dobre vere, koje se razvilo upravo u kontekstu prijave ratnih okolnosti kao relevantnih za procenu rizika, vid. Glintić, M., 2021, Održivost načela krajnje dobre vere u ugovornom pravu reosiguranja, *Zbornik radova Kopaoničke škole prirodnog prava – Slobodan Perović Primena prava i pravna sigurnost*, 2, str. 458.

7 Ipak, tokom Prvog svetskog rata u Engleskoj su se prodavale polise osiguranja imovine od bombaškog napada od čega su osiguravajuća društva puno profitirala jer su očekivanja i strah od bombardovanja bili daleko veći od stvarne štete koja je tako nastala. Do izmene rezona osiguravača dolazi tokom Španskog građanskog rata, kada su nastupili veliki finansijski udari na osiguravajuća društva.

Neki od slučajeva pred američkim sudovima su *Queen Ins. Co. v. Globe & Rutgers Fire In. Co*., 263 U.S. 487 (1924); *Stinson v. N.Y. Life Ins.,* 167 F.2d 233 (D.C. Cir. 1948); *Vanderbilt v. Travelers' Ins. Co*., 184 N.Y.S. 54 (N.Y. 1920); *Stankus v. N.Y. Life Ins. Co.,* 44 N.E. 2d 687 (Mass. 1942). Detaljnije o razvoju ovog isključenja vid. Massmann, S., 2001, *War Risk Exclusion Legal History Outlined*, p. 45 (https://www.propertycasualty360.com/2001/09/30/war-risk-exclusion-legal-history-outlined/, 3. 2. 2023); Chopra, A., 2021, Cyberattack – Intangible Damages in a Virtual World: Property Insurance Companies Declare War on Cyber-Attack Insurance Claims, *Ohio State Law Journal*, 1, p. 129. Takođe, Haufler, V., 1997, *Dangerous Commerce: Insurance and the Management of International Risk*, London, Cornell University Press, p. 86.

8 Shniderman, A., 2019, Prove It! Judging the Hostile-or-Warlike-Action Exclusion in Cyber--Insurance Policies, *Yale Law Journal*, 129, p. 83. O problemu agregacije štete vid. Glintić, M., 2021, Agregacija štete u skladu sa Načelima o ugovornom pravu reosiguranja, *Prouzrokovanje štete, naknada štete i osiguranje*, Beograd, Mionica, Institut za uporedno pravo, str. 375–376.

9 Sa sličnim problemima su se osiguravači sreli tokom pandemije kovida 19 kada su brojni osiguranici hteli da aktiviraju svoje polise osiguranja prekida rada, vid. Glintić, M., Pokriće po osnovu ugovora o osiguranju prekida rada tokom pandemije kovida 19, u: Đurić, V., Glintić, M. (ur.), 2021, *Pandemija kovida 19: pravni izazovi i odgovori*, Beograd, Institut za uporedno pravo, str. 143–144.

10 Carter, R. A., Enoizi, J., 2020, *Cyber War and Terrorism: Towards a Common Language to Promote Insurability*, Geneva, Geneva Association, p. 6.

sajber-napada koji se ne mogu ni sprečiti, niti detektovati na vreme, a posledice budu velike.

Da li će se isključenje ratnih rizika primeniti na sajber-napade zavisi od više faktora i odgovora na više pitanja – da li se sajber-napad može shvatati kao rat u pravnom smislu i ako može, da li se može dokazati ko je pripremio napad, na koji način je napad bio povezan sa širim političkim ili vojnim ciljevima, koje državne vlasti su bile umešane u napad. Odluka o daljem postupanju osiguravača zavisiće od toga da li će uspeti da se dokaže i da se odgovori na sva pitanja. Na prvi pogled se može učiniti da takva konstalacija odnosa ide naruku osiguraniku, jer je teret dokazivanja na osiguravaču.

Danas, u vreme čestih sajber-napada, pojam ratovanja bi se mogao tumačiti na različite načine i vrlo široko. Autori su ukazivali na probleme sa definisanjem određenih pojmova kao što su „neprijateljski" ili „ratni" (*Asaaf Lubin*), neki su ukazivali na definicije rata u skladu sa međunarodnim propisima (*Adam Shniderman*), kao i na brojne druge probleme koji prate ovu temu. Stoga ostaje otvoreno pitanje kako će sudovi tumačiti klauzule o isključenim ratnim rizicima u kontekstu sajber-ratovanja. Ako prevlada usko tumačenje ovog isključenja, onda će sudovi morati da uspostave jasne razlike između neprijateljskih i ratnih sajber-operacija i onih koje to nisu.[11]

2.1. RAT U PROPISIMA MEĐUNARODNOG JAVNOG PRAVA

Kao što pojedine grupe imaju koristi od sprovedenih sajber-napada, u istoj poziciji se nalaze i države. Deo nacionalne strategije može biti prikupljanje podataka iz informacionih sistema i podataka druge države, preko onemogućavanja druge države da dobije sredstva, pa sve do naplaćivanja otkupnina.[12] Neki od incidenata koji se odvijaju između dveju država (ograničenje dostave gasa, špijunaža, sajber-napadi) mogu se odrediti i kao delovi hibridnog rata koji je sa prostora bojnog polja prešao u sajber-prostor, ali i kao legitimni incidenti koji se mogu odvijati između dveju država.[13] Takođe, činjenica da kao posledica sajber-napada

11 U tom smislu postoje i stavovi da se isključenje ratnih rizika ima tumačiti vrlo usko kada su u pitanju sajber-napadi u smislu da se ovo isključenje rizika ima primeniti samo na one osigurane slučajeve kod kojih postoji povezanost sa vojnim sukobima. Tako i McCabe, M., 2018, *NotPetya Was Not Cyber 'War'* (https://www.marshmclennan.com/insights/publications/2018/aug/notpetya-was-not-sajber-war.html, 22. 2. 2023). Osim toga, sudovi u SAD su ocenili da se sajber-napadi usmereni protiv građana neratujućih sila čija se imovina nalazi daleko od mesta ili predmeta ratovanja ne mogu shvatiti kao ratne operacije. *Pan American World Airways Inc. v. Aetna Casualty and Surety Co.*, 505 F.2d 989 (2nd Cir. 1974).

12 Prema nekim podacima, Severna Koreja je putem sajber-napada obezbedila dobit od preko dve milijarde dolara. Shackelford, S., 2021, Wargames: Analyzing the Act of War Exclusion in Cyber Risk Insurance Coverage and Its Implications for Cybersecurity Policy, *Yale Journal of Law and Technology*, Vol. 23, p. 368.

13 Potpuno je odvojeno pitanje da li u sajber-ratu uopšte dolazi do preraspodele snaga između sukobljenih strana, što će opet zavisiti od toga da li je jednoj strani posledično naneta značajna i trajna šteta, ili je za to nužno da sajber-napad bude praćen vojnim kopnenim akcijama ili pak nekim drugim aktivnostima usmerenim na kapitalizaciju privremene nesposobnosti postignute sajber-udarima protivničke strane. Korhonen, O., 2015, Deconstructing the Con-

ne postoje ljudske žrtve, da ne dolazi do materijalnog oštećenja imovine i da suprotstavljene strane ne upotrebljavaju oružje, osnovni je izvor nedoumice da li se o sajber-napadu može govoriti kao o vidu rata.[14]

Ipak, teoretičari su ustanovili brojne probleme prilikom pokušaja određivanja pravnog statusa sajber-rata, jer je nesumnjivo reč o sivoj zoni. Sajber-rat, pa čak ni hibridni rat, nikad nije zvanično objavljen. Problemi koji prate određivanje statusa sajber-rata potiču od pravljenja razlika između javnog i privatnog, između državnih subjekata i nedržavnih, između civila i onih koji učestvuju u sukobu.[15] Vrlo je nejasno, takođe, u kom trenutku bi se moglo smatrati da je sajber-napad prestao da bude inkriminisano krivično delo i postao sastavni deo rata ili kada je prerastao u terorizam, s obzirom na usmerenost ovakvog napada na civilno stanovništvo.[16]

Zaključak akademske rasprave je da se međunarodno pravo, a naročito Povelja UN imaju primeniti na sajber-prostor, jer je reč o neophodnom uslovu za održavanje mira i stabilnosti.[17] Tako se, prema jednom od poslednjih stavova Međunarodnog komiteta Crvenog krsta, međunarodno humanitarno pravo ima primenjivati i na sajber-napade i predstavljati im granicu tokom oružanog sukoba, kao što ograničava upotrebu bilo kog oružja, sredstva i metoda tokom oružanog sukoba.[18] I pored navedenog zaključka, i dalje ostaje pitanje u kom trenutku će se sajber-napad shvatati kao rat, odnosno kada će se smatrati da sajber-napad ispunjava uslove rata. Definicije rata iz međunarodnog javnog prava zahtevaju da država protiv koje se postupa prepoznaje te akcije kao izraz rata i nasilja.[19] Široko tumačenje međunarodnih *ius ad bellum*, prvenstveno Povelje UN, iako nastali mnogo pre kompjutera i sajber-prostora, ostavljaju prostor da se i sajber-napad shvati i kao nezakonita upotreba sile, koji stoga otvara prostor

flict in Ukraine: The Relevance of International Law to Hybrid States and Wars, *German Law Journal*, 3, p. 472. Takođe, Gartzke, E., 2013, The Myth of Cyberwar. Bringing War in Cyberspace Back Down to Earth, *International Security*, 2, p. 43.

14 Američki teoretičari smatraju da je potrebno postojanje sukoba između dvaju suverenih entiteta, koji bi bio ekvivalent oružanom napadu ili upotrebi sile u sajber-prostoru. Mazaraki, N., Goncharova, Y., 2022, Cyber Dimension of Hybrid Wars: Escaping a "Grey Zone" of International Law to Adress Economic Damages, *Baltic Journal of Economic Studies*, 2, p. 116. Takođe, Rid, T., 2013, *Cyber War Will Not Take Place*, Oxford University Press, p. 166.

15 Korhonen, O., 2015, pp. 454, 460.

16 Kao u slučaju *Universal Cable Prods., LLC v. Atl. Specialty Ins. Co.*, 929 F.3d 1143, 1158–59 (9th Cir. 2019). Za više detalja o terorizmu vid. Zirojević, M., 2014, *Terorizam – međunarodni pogled*, Beograd, Institut za međunarodnu politiku i privredu, str. 169. Takođe, Zirojević, M., 2011, Zloupotreba interneta u terorističke svrhe, *Međunarodni problemi*, 3, str. 417–448.

17 Mazaraki, N., Goncharova, Y., 2022, p. 117.

18 ICRC, 2020, International Humanitarian Law and Cyber Operations During Armed Conflicts, *International Review of the Red Cross*, 102, pp. 481–492.

19 Gargano, D., 2013, An Act of War: Finding A Meaning for What Congress Has Left Undefined, *Touro Law Review,* 1, p. 152. Takođe, ministri spoljnih poslova EU su podržali inicijativu za izradu propisa za zajedničku diplomatsku aktivnost EU za sajber-napade, uz naglašavanje da se međunarodno pravo ima primeniti i na sajber-prostor i na sajber-napade. Council of the European Union, Draft Implementing Guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities – Approval of Final Text, 13007/17, 9 October 2017 (http://data.consilium.europa.eu/doc/document/ST-13007–2017-INIT/en/pdf, 5. 3. 2023).

za samoodbranu.[20] Tako član 2(4) Povelje UN proglašava pretnju ili upotrebu sile bez prethodne saglasnosti Saveta bezbednosti nelegalnim. Ekonomske sankcije, špijunaža, nadzor predstavljaju primere gde ovo pravilo nije povređeno.[21] Zato je sporno u kojoj meri bi sajber-napadi činili pretnju ili upotrebu sile, s obzirom na to da se možemo zapitati da li povreda zaštitnih virtuelnih barijera predstavlja povredu člana 2(4). Istovremeno, pravilo 11 iz Talinskog priručnika predviđa da neće svi sajber-napadi značiti upotrebu ili pretnju upotrebom sile u smislu člana 2(4) Povelje UN, a posebno ne oni kojima nedostaje element prinude.[22] Naime, pravilo 11 Talinskog priručnika predviđa da će se sajber-operacija smatrati upotrebom sile kada su njeni obim i efekti uporedivi sa operacijama koje se nalaze na nivou upotrebe sile a nisu sajber-operacije. To znači da sajber--aktivnosti vrlo često neće ispunjavati ovaj visoko postavljen uslov, tako da su se neke zemlje odlučile da ovo pravilo tumače na različite načine.[23] Trend koji se pak uočava, a uglavnom po uzoru na SAD, jeste da se lestvica sve više spušta u pogledu uslova koji moraju biti ispunjeni da bi se jedan sajber-napad smatrao ratom.[24] To znači da se otvara prostor da države sve veći broj sajber-napada više neće tretirati kao sajber-napade niskog intenziteta, već kao upotrebu sile koja aktivira pravo na samoodbranu iz člana 51 Povelje UN.

2.2. PROBLEMI PRILIKOM ODREĐIVANJA SAJBER-NAPADA KAO RATA

Prilikom određivanja sajber-napada kao rata sa ciljem opravdavanja primene klauzule o isključenju obaveze osiguravača javlja se još nekoliko pitanja koja zahtevaju detaljnije razmatranje. Od odgovora na ta pitanja zavisi krajnji odgovor da li će osiguravač biti u obavezi da izvrši svoju obavezu prema osiguraniku.

Prvo pitanje se tiče pripisivanja sajber-napada jednoj državi, koja će, po pravilu, negirati svoju povezanost.[25] Razdvajanje političkih razloga zbog kojih jedna država optužuje drugu zasigurno predstavlja i predstavljaće otežavajuću okolnost. Međunarodna zajednica je pokušala da ustanovi neke parametre koji mogu pomoći prilikom pripisivanja sajber-napada jednoj državi: tehničke karakteristike napada, njegove razmere i obim, uticaj, širi kontekst, uticaj na međunarodni

20 Sanders, C., 2018, The Battlefield of Tomorrow, Today: Can a Cyberattack Ever Rise to an "Act of War"?, *Utah Law Review,* 2, p. 514. Upor. Ferland, J., 2019, Cyber Insurance – What Coverage In Case of an Alleged Act of War? Questions Raised by The Mondelez v. Zurich Case, *Computer Law and Security Review*, 4, p. 376.

21 National Research Council, 2009, *Technology, Policy, Law, And Ethics Regarding U.S. Acquisition and Use Of Cyberattack Capabilities*, Washington, p. 242.

22 International Group of Experts at the Invitation of the NATO Cooperative Cyber Defense Centre of Excellence, 2013, *Tallinn Manual on the International Law Applicable to Cyber Warfare,* Cambridge University Press, p. 45.

23 O izmenama koje su se dešavale u dokumentima Vlade SAD vid. Shackelford, S., 2021, pp. 33–35.

24 *Ibid*., pp. 378–381.

25 Eichensehr, K. E., (2020), The Law and Politics of Cyber Attack Attribution, *UCLA Law Review*, 3, pp. 527–529.

mir i bezbednost i rezultati konsultacija između država.[26] Međutim, navedene smernice nisu ni izbliza dovoljno sredstvo.

U okviru ovog pitanja još sedamdesetih godina pred američkim sudovima pokrenulo se pitanje da li je potrebno da je reč o suverenom entitetu da bi uopšte bio prihvaćen stav da se radi o ratu. U slučaju *Pan Am. World Airways, Inc. v. Aetna Cas. & Sur. Co*, osiguravač je tvrdio da je PFLP (*Popular Front for the Liberation of Palestine*) kvazivladino telo, koje prima finansijsku podršku Kine i Severne Koreje, što sud nije prihvatio. Zauzet je stav da je otimica aviona 1970. godine od strane PFLP-a bio akt radikalne političke grupe, a ne suverenog tela i da otmica aviona nije proizašla iz ratnog sukoba između priznatih država.[27]

Potom, ako se pođe od pretpostavke da je ispunjen prethodni uslov da je reč o napadu suverenog entiteta na drugi suvereni entitet, dolazi se do izazova utvrđivanja identiteta izvršioca sajber-napada.[28] Činjenica da je jedna od osnovnih karakteristika sajber-napada anonimnost ne olakšava zadatak osiguravača i sudova.[29] Celokupan postupak može da bude usložnjen jer nije neuobičajeno da postoje *proxy* snage u sajber-prostoru kako bi „zavarale tragove".[30] Takođe, dešava se da kompanije koje se bave bezbednošću u sajber-svetu ustanove poreklo napada, ali da ne mogu da utvrde tačan identitet izvršioca, već ga vode pod određenim pseudonimom,[31] što osiguravačima ne može biti dovoljan podatak. Pored toga, javljaju se i podaci sa kojima nije najjasnije kako postupati. Primer za to su tvitovi Anonimusa da podržavaju Ukrajinu u sukobu sa Rusijom i da će delovati u njihovo ime.[32] Sve nacionalne vlade u krajnjoj liniji ne poseduju dovoljne kapacitete da utvrde poreklo napada niti se mogu u potpunosti osloniti na privatne istražitelje.[33]

Potom je tu i problem otkrivanja motiva za izvršenje sajber-napada. Motivi se tokom vremena mogu menjati – lice koje je izvršilo sajber-napad može

26 Mazaraki, N., Goncharova, Y., 2022, p. 118.

27 Ovaj predmet je poslužio kao precedent prilikom odlučivanja da li se isključenje ratnih rizika primenjuje na akte terorizma.

28 Tokom razmatranja ovog aspekta ne treba zanemariti da različite države imaju različite tehničke mogućnosti kojima se imaju služiti tokom utvrđivanja porekla sajber-napada i identiteta izvršilaca. U delu literature se ukazuje na to da naprednije zemlje, kao što je SAD, imaju više uspeha u utvrđivanju porekla sajber-napada u odnosu na ostale zemlje, što može dovesti do brojnih problema i grešaka. Goodman, R., 2018, Cyber Operations and the U.S. Definition of "Armed Attack," *Just Security* (https://www.justsecurity.org/53495/cyberoperations-u-s-definition-armed-attack/, 7. 3. 2023).

29 Clark, D., Landau, S., 2011, Untangling Attribution, *Harvard National Security Journal*, 2, p. 33.

30 Maurer, T., 2018, *Cyber Mercenaries: The State, Hackers, and Power*, Cambridge, Cambridge University Press, p. 31.

31 Primera radi vid. https://attack.mitre.org/groups/G0067/.

32 Vid. https://www.theguardian.com/world/2022/feb/27/anonymous-the-hacker-collective-that-has-declared-cyberwar-on-russia; https://timesofindia.indiatimes.com/gadgets-news/anonymous-declares-cyber-war-against-russia-amid-ukraine-war-takes-down-government-websites/articleshow/89825529.cms, 8. 3. 2023.

33 Ono što je neobično ili interesantno jeste to da uglavnom SAD ima uspeha u prepoznavanju porekla sajber-napada, dok to nije slučaj sa drugim zemljama, što svakako može dovesti do velikih grešaka. Vid. Goodman, R., 2018.

prikupiti sve potrebne podatke, a onda tek odlučiti da li želi da ih iskoristi za sopstvenu dobit, da li želi da pregovara sa vladom o njihovom korišćenju i slično. Pristup mreži koji je korišćen za špijunažu tokom krize i sukoba može se koristiti i za destruktivnije ciljeve. Takođe, neki od učesnika ili rukovodilaca sajber-napada mogu delovati i po nalogu države, ali to ne znači da oni uvek rade isključivo u tom svojstvu.[34]

Politički zvaničnici su svesni da vrlo lako mogu biti upleteni u korporativne sporove, odnosno sporove osiguravača i privrednih društava, jer se osiguravačima otvara mogućnost da se pozovu na izjave političara i zvaničnika. Postoje navodi da je predsednik Obama o napadu na Sony iz 2014. govorio kao o „sajber-vandalizmu", a ne kao o ratu upravo da bi izbegao uticaj na odluke osiguravača povodom šteta koje su proizašle iz navedenog sajber-napada.[35] Tu su potom i zvanične izjave država koje podržavaju ideju da nije moguće utvrditi krivce za sprovedene sajber-napade, čime se svakako dovode u pitanje navodi o napadima sponzorisanim od strane države.[36] U stvarnosti je situacija takva da državne službe sa velikom sigurnošću mogu da utvrde poreklo napada, što je bio ključni faktor za razvoj mogućnosti da se sajber-napad pripiše nekoj državi ili organizaciji, ali se države ipak uzdržavaju od zvaničnih izjava iz političkih i diplomatskih razloga.

3. POSLEDICE *NOTPETYA* NAPADA

Tokom 2017. godine dogodila su se dva sajber-napada koja su imala velike ekonomske posledice. Prvo se u maju 2017. godine desio *WannaCry* napad, kada je grupa hakera iskoristila ukradeni NSA (*National Security Agency*) alat da hakuje 20.000 Windows kompjutera u 150 zemalja i da onemogući njihovu upotrebu dok im se ne isplati otkupnina u bitkoinu.[37] SAD je na kraju pripisao rat Severnoj Koreji, ali Trampova administracija, i pored sankcija uvedenih Severnoj Koreji, nije ovaj napad ocenila kao ratnu akciju. Potom se desio *NotPetya* napad,

34 Tako je firma FireEye, vodeća u oblasti sajber-obaveštajnih delatnosti, utvrdila da grupa APT41 sprovodi špijunažu koju sponzoriše kineska država, ali uz to obavlja određene sajber--aktivnosti koje su isključivo finansijski motivisane i nisu po nalogu kineske države. Tako, ako bi se utvrdilo da je APT41 odgovoran za sajber-napad protiv koga je postojala polisa osiguranja, sud će imati zadatak da ustanovi da li je konkretan incident bio u režiji države ili ne. S tim ne mogu na kraj da izađu ni obaveštajne službe, a kamoli osiguravajuća društva koja ne raspolažu ni delićem potrebnih tehnologija. Fire Eye, 2019, *Double Dragon: APT41, a Dual Espionage and Cyber Crime Operation* (https://content.fireeye.com/apt-41/rpt-apt41/, 7. 2. 2023).

35 Satariano, A., Perlroth, N., 2019, *Big Companies Thought Insurance Covered a Cyberattack. They May Be Wrong* (https://www.nytimes.com/2019/04/15/technology/cyberinsurance-notpetya-attack.html, 5. 2. 2023).

Takođe, Shahani, A., 2014, *Doubts Persist on U.S. Claims of North Korean Role in Sony Hack* (https://www.npr.org/sections/alltechconsidered/2014/12/26/373303733/doubts-persist-on-u-s-claims-on-north-korean-role-in-sony-hack, 5. 2. 2023).

36 Kopan, T. 2016, *Is Trump Right? Could a 400-Pound Couch Potato Have Hacked the DNC*? (https://edition.cnn.com/2016/09/27/politics/dnc-cyberattack-400-pound-hackers/index.html, 4. 2. 2023).

37 Trautman, L., Ormerod, P., 2019, WannaCry, Ransomware, and the Emerging Threat to Corporations, *Tennessee Law Review*, 2, pp. 524–525.

za koji se ocenjuje da je deo ratne strategije Rusije prema Ukrajini u okviru njihovog višegodišnjeg sukoba. Naime, svoje ocene ruskog porekla ovog napada dale su vlade i njihovi zvaničnici širom sveta,[38] a u jednom trenutku su objavljena i imena šestorice Rusa odgovornih za sajber-napade.[39]

Napadom su prvenstveno bili pogođeni ukrajinski mediji, železnica, elektrodistribucija, jer je napadnut *softwear update* ukrajinske kompanije MeDoc.[40] Potom je došlo do proširivanja dejstva *NotPetya* napada i van ukrajinskih granica, pa su pogođeni brojni akteri – od Pensilvanije, preko fabrike čokolade iz Tasmanije, sve do državne naftne kompanije u Rusiji, odakle se veruje da je napad i krenuo.[41] Fizička i pravna lica pogođena *NotPetya* napadom nalazila su se svakako van mesta stvarnog sukoba i bavila su se čisto civilnim aktivnostima, kao što su dostavljanje paketa, proizvodnja lekova i slično.

3.1. SPOROVI PRED AMERIČKIM SUDOVIMA

Neselektivno gađanje i civilnih meta pokrenulo je brojne zahteve prema osiguravajućim društvima jer su privredna društva želela da budu obeštećena. Kako je stav osiguravača bio da je u pitanju ratna akcija, koja za njih predstavlja aktuarsku noćnu moru, odbili su da izvrše svoje ugovorne obaveze.[42] Od toga su dva slučaja, *Merck* i *Mondelez*, pokrenuta pred američkim sudovima, tokom 2022. godine dobila svoj konačni ishod.

Obe kompanije, *Merck* i *Mondelez*, posedovale su i polise sajber-osiguranja. Međutim, kako su to bile polise sa prilično niskim sumama osiguranja, ove kompanije su više nade polagale u polise iz ugovora o osiguranju imovine koje su pokrivale sve rizike i koje su predviđale više sume osiguranja.[43] U oba slučaja su

38 Za saopštenje Bele kuće vid. Press Briefing, The White House, Statement from the Press Sec'y (Feb. 15, 2018). Takođe, američki predsednik je naložio Ministarstvu finansija (US Treasury), a po osnovu Countering America's Adversaries Through Sanctions Act (CAATSA– Countering America's Adversaries Through Sanctions Act, Pub. L. No. 115–44, 131 Stat. 886 (2017)), da uvede sankcije Rusiji kao odmazdu za *NotPetya* napad. Press Release, U.S. Dep't of the Treasury, Treasury Sanctions Russian Cyber Actors for Interference with the 2016 U.S. Elections and Malicious Cyber-Attacks (https://home.treasury.gov/news/pressreleases/sm0312, 7. 3. 2023). Slične izjave su stigle iz Australije, Velike Britanije, Kanade, Danske, Litvanije i Estonije. Wolff, J., 2022, *Cyberinsurance Policy: Rethinking Risk in the Age of Ransomware, Computer Fraud, Data Breaches, and Cyberattacks*, Massachusetts, p. 139.

39 U. S. Department of Justice, 2020, *Press Release, Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace* (https://www.justice.gov/opa/pr/sixrussian-gru-officers-charged-connection-worldwide-deployment-destructivemalware-and, 7. 3. 2023).

40 Greenberg, A., 2018, *The Untold Story of NotPetya, the Most Devastating Cyberattack in History,* (https://www.wired.com/story/notpetyacyberattack-ukraine-russia-code-crashed-the-world/, 15. 2. 2023).

41 Chopra, A., 2021, p. 124.

42 Response of Generali in *Merck and Co., Inc. and International Indemnity Ltd. v. ACE American Insurance Company et al*, Superior Court of New Jersey Law Division: Union County, October 12, 2018.

43 Iznosi štete koje su obe kompanije pretrpele bili su izuzetno visoki. Merck, farmaceutska kompanija, pretrpeo je štetu od preko 1,4 milijarde dolara, a Mondelez preko 100 miliona

osiguravači stali na stanovište da je njihova obaveza isključena u slučaju „ratne akcije ili neprijateljskih akcija u vreme mira ili rata", nezavisno od toga da li ih preduzima vlada jedne države ili njen „agent".[44] Takođe, ni u jednoj od tih polisa nije pominjan rizik od sajber-napada, jer su najverovatnije i pisane bez ideje da takav rizik postoji.

U slučaju *Merck*, sud Nju Džersija je 6. decembra 2021. godine doneo delimičnu presudu u korist te kompanije uz obrazloženje da je isključenje rizika u slučaju rata vrlo jasno definisano i da se ne može primeniti na konkretan slučaj.[45] Stav suda je bio da nema mesta primeni ove klauzule o isključenju rizika, jer pojam rata iz ove klauzule zahteva postojanje sukoba između dveju suverenih država (nacionalne države), a pridev *neprijateljski* se odnosi na karakteristike druge strane u sukobu, za šta u konkretnom slučaju nisu postojali dovoljni i potrebni dokazi. Kako nije bilo nikakvih indicija o pregovorima osiguravača i osiguranika o sadržini polise, sud je bio na stanovištu da se ima primeniti pravilo o razumnim očekivanjima osiguranika o pokriću.[46] To bi zapravo značilo da postoji obaveza osiguravača i u onim slučajevima koji nisu eksplicitno isključeni. Takođe, dodatni teg na tasu odluke u korist osiguranika je bilo i nepostojanje precedenata o primeni isključenih ratnih rizika u sličnim situacijama.

Slučaj *Mondelez* je pokrenut jer je ta kompanija bila žrtva dvaju odvojenih sajber-napada 2017. godine koji su potekli od *NotPetya* virusa, a rezultirali su krađom ličnih informacija i enkriptovanja preko 1.700 servera i 24.000 laptopova.[47] Kao posledica su nastupili problemi u lancu dostave usled nemogućnosti pristupa mejlu. Isto kao i *Merck*, i *Mondelez* je kod svog osiguravača *Zurich*-a hteo da aktivira imovinsko osiguranje od svih rizika (*all risk insurance*) čija je polisa predvidela pokriće za fizički gubitak ili štetu na elektronskim podacima, programima, softverima, uključujući i fizički gubitak ili štetu usled „zlonamernog uvođenja mašinskog koda". Spor je završen poravnanjem u oktobru 2022. godine. Budući da je spor okončan na ovaj način, sporazum strana nije objavljen, ali je, prema dostupnim informacijama, okosnicu spora takođe predstavljao spor oko toga da li se *NotPetya* napad može okarakterisati kao rat.

---

dolara. Griffin, R., Chiglinsky, K., Voreacos, D., 2019, Was It an Act of War? That's Merck Cyber Attack's $1.3 Billion Insurance Question, *Insurance Journal* (https://www.insurancejournal.com/news/national/2019/12/03/550039.htm, 20. 2. 2023). Takođe, Satariano, A., Perlroth, N., 2019.

44 *Merck and Co., Inc. and International Indemnity Ltd. v. ACE American Insurance Company et al,* Superior Court of New Jersey Law Division: Union County, October 12, 2018.

45 *Merck & Co. & Int'l Indem., Ltd. v. ACE Am. Ins. Co.,* Order on CrossMotions for Partial Summary Judgment, N. J. Super. Ct., Union Cty., December 6, 202.

46 Navedeno pravilo je posledica statusa osiguranika kao potrošača u ugovorima o osiguranju. Vid. detaljnije Glintić, M., 2020, Zaštita prava slabije ugovorne strane u skladu sa Principima evropskog ugovornog prava osiguranja, *Strani pravni živo*t, 3, str. 59–60. Takođe, Wan, K., 2020, Notpetya, Not Warfare: Rethinking the Insurance War Exclusion in the Context of International Cyberattacks, *Washington Law Review*, 3, p. 1596.

47 *Mondelez Int'l, Inc. v. Zurich Am. Ins. Co*., No. 2018L011008, 2018 WL 4941760 (Ill. Cir. Ct. Oct. 10, 2018).

3.2. DA LI JE *NOTPETYA* NAPAD ZAPRAVO SAJBER-RAT?

Po pravilu, polise ne sadrže definicije rata, a kamoli sajber-rata, i na sudovima je da donesu konačnu odluku o tome da li je postojao rat. Tvrdnje osiguravača da je konkretan sajber-napad zapravo sajber-rat ili da je deo rata u klasičnom smislu moraju biti potvrđene dokazima s obzirom na važenje raspravnog načela u parničnim postupcima. Veliko je pitanje koji su to dokazi koje osiguravač uopšte može koristiti kao relevantne u postupku – da li su to samo oni dokazi koji su javno dostupni ili se smeju koristiti i oni dokazi koji su okarakterisani kao poverljivi?[48] U brojnim slučajevima će se ispostaviti da su tvrdnje osiguravača u suprotnosti sa zvaničnom državnom politikom, a sud će morati da oceni da li je to na štetu ili u korist osiguravača. Pitanje je, međutim, gde su granice ovlašćenja suda u takvim okolnostima. Da li će sudovima biti dovoljan novinski natpis da je reč o ratu u konkretnom slučaju ili će sudovi poći od pravno utemeljenih definicija rata?

Kao što je prikazano u prethodnom odeljku, brojni zvaničnici su osudili *NotPetya* sajber-napad i pripisali ga Rusiji. U navedenim sporovima pred američkim sudovima osiguravači su se oslanjali na navedene novinske natpise i izjave zvaničnika.[49] Njihova ideja i dodatni argument su bili da je tim napadom pričinjena ogromna šteta podacima, programima, softverima kompanija, ali i opremi i njenim komponentama koje su ostale trajno disfunkcionalne, što mogu biti posledice i klasične forme rata.[50]

Međutim, nijedan zvanični dokument nije izdat tim povodom, što ne iznenađuje budući da su privatne kompanije bile pogođene ovim napadima. To nameće pitanje na koji način će osiguravači dokazivati da je reč o ratnim akcijama jedne države protiv druge, čime bi bila opravdana primena klauzule o isključenim ratnim rizicima.[51] Osim toga, metode koje koriste države, vlade i istražitelji nisu predviđene da rešavaju zahteve iz osiguranja, pa se i ne mogu tako jednostavno preneti na taj teren.

Sledeći argument koji ide u korist teze da se konkretno *NotPetya* ne može smatrati ratnom akcijom jeste taj da je reč o napadu usmerenom protiv drugih kompanija, a ne protiv nekog drugog suverena. Prema rezultatima analize sudske prakse američkih sudova, moglo bi se reći da osiguravači polaze od starijih definicija rata iz međunarodnog javnog prava prilikom definisanja isključenih ratnih rizika, a u daleko manjoj meri se oslanjaju na poimanje rata u politici i u

48 U SAD sudovi imaju procedure oko izvođenja poverljivih i tajnih dokaza, a Vlada je u određenim slučajevima ponudila poverljive dokaze kako bi pomogla rešavanje sporova u vezi sa isključenim ratnim rizicima, što nije tako uobičajena praksa. Upor. *Pan American World Airways Inc. v. Aetna Casualty and Surety Co*., 505 F.2d 989 (2nd Cir. 1974).

49 Tako je, između ostalog, savetnica Centra za strateške i međunarodne studije Olga Oliker izjavila pred Komitetom za oružane snage Senata da ako je raniji napad na ukrajinsku elektrodistribuciju učinila Rusija, onda upravo to može biti primer sajber-operacije koja se može okarakterisati kao ratna operacija. Navedeno prema Wolff, J., 2022, p. 142.

50 Ferland, J., 2019, p 374.

51 *Ibid*., p. 372.

novinarstvu.[52] Možda bi se čak moglo reći da se rat u kontekstu prava osiguranja ograničava na sukobe između *de facto* i *de iure* suverenih entiteta.[53]

Kada dođe do sledećih sporova, bilo pred američkim, bilo pred bilo kojim drugim nacionalnim sudovima, sudovi će morati da nastoje da ustanove volju ugovornih strana iz ugovora o osiguranju. Ako su odredbe polise jasne i nedvosmislene, onda ih sud mora tako i tumačiti. To se posebno odnosi na klauzule o isključenju odgovornosti osiguravača, koje moraju biti jasne i oslobođene bilo kakvih dvosmislenih značenja.

4. ZAKLJUČAK

Predstavljeni primeri iz sudske prakse američkih sudova imali su za cilj da pokažu samo delić problema sa kojim će se suočavati i osiguravači i osiguranici u vezi sa sajber-napadima. Velika finansijska šteta neminovno će i dalje pogađati obe strane, pa će posledično rasti i broj sudskih sporova. U cilju iznalaženja optimalnog rešenja, biće neophodna reakcija obeju strana. Osiguravači će morati da izvrše preciziranje svojih opštih i posebnih uslova osiguranja, dok će kompanije morati da razmisle o dodatnim sredstvima i instrumentima zaštite svoje imovine.

Za osiguravače će svakako biti najveći izazovi precizno definisanje sajber-napada i pod kojim uslovima će biti legalna i legitimna primena klauzule o isključenim ratnim rizicima. Bez izvršenja tog zadatka, osiguravači neće imati nikakav prostor da se pozovu na isključene ratne rizike koji nisu precizno definisani. Ako je tekst polise nejasan, dvosmislen, ako osiguravač nije preduzeo ništa da izmeni zastarele polise i anahroni jezik, onda se polisa mora tumačiti u korist pokrića, odnosno zaštite slabije ugovorne strane.[54]

Okosnica budućih aktivnosti osiguravača će biti da u svojim uslovima osiguranja definišu da li je akt sajber-napada zavisan (njegovo postojanje) od fizičke objave rate ili postojanja neprijateljstva između dveju država. Dalje, potrebno je definisati da li je neophodno da sajber-napad sprovede priznata država, uz preciziranje da li sajber-napadi moraju biti potpomognuti ili organizovani od strane države.[55] Prilikom iznalaženja odgovora na navedena pitanja moraće da

52 Tako je u slučaju *Universal* (*Universal Cable Prods., LLC v. Atl. Specialty Ins. Co.*, 929 F.3d 1143, 1158–59 (9th Cir. 2019) iz 2019. godine američki sud stao na stanovište da je u kontekstu osiguranja potrebno da postoji posebno značenje rata koje zahteva postojanje neprijateljstva i neprijateljskih odnosa između vlada država. Takav je bio stav i njujorškog suda u predmetu *Holiday Inns, Inc. v. Aetna Ins. Co*., 571 F. Supp. 1460, 1461 (S.D.N.Y. 1983).

53 Wan, K., 2020, p. 1600. Svakako da postoje i suprotna stanovišta u skladu sa kojima sud prilikom tumačenja pojma rata treba da pođe od kolokvijalnog značenja ovog pojma, čime su ovlašćenja suda značajno proširena. Vid. slučaj *Holiday Inns, Inc. v. Aetna Ins. Co*., 571 F. Supp. 1460, 1461 (S.D.N.Y. 1983).

54 Petrović Tomić, N., 2015, *Zaštita potrošača usluga osiguranja, Analiza i predlog unapređenja regulatornog okvira*, Beograd, Pravni fakultet Univerziteta u Beogradu, str. 282–302.

55 Postavlja se pitanje da li su sajber-napadi motivisani od strane države (engl. *state motivated*) ili da li jedna država upravlja njima (engl. *state directed*), zavisno od stepena operativne kontrole koji jedna država mora imati nad napadom, što se mora i dokazati. Time se otvaraju vrata za pripisivanje državama brojnih sajber-napada koje nije organizovala i podržala država.

se precizira i razdvajanje različitih sajber-napada. Naime, sajber-napadi koji imaju velike ekonomske posledice, a nisu podržani ni od jedne države, ne bi trebalo da budu isključeni i za njih bi trebalo da osiguranici očekuju pokriće.

U tom duhu je reosiguravač *Capsicum Re* nedavno objavio predlog u kom je ponudio dva moguća modela kojima bi se mogle zameniti klauzule o isključenim ratnim rizicima.[56] U julu 2020. godine, Međunarodni forum za rizik od terorizma u osiguranju (IFTRIP), zajedno sa *Geneva Association*, objavio je nekoliko radova o sajber-ratu i sajber-terorizmu sa ciljem da promoviše osiguraciju ovih rizika i ujednačavanje terminologije.[57]

Takođe, krajem 2021. godine, Lojd je izbacio svoje nove klauzule koje se tiču isključenja sajber-ratnih rizika kod sajber-osiguranja i sa čijom primenom se počelo u martu 2023. godine. Reč je o četiri nove klauzule koje omogućavaju iznijansirani pristup pokriću zavisno od ekonomskih posledica datog sajber-napada:

- klauzula LMA 1 isključuje pokriće za sve gubitke koji nastaju usled ili kao posledica rata ili sajber-operacije;
- klauzula LMA 2 uspostavlja određena ograničenja za isplatu pokrića usled sajber-napada, ali u potpunosti isključuje pokriće za one operacije koje su pokrenute tokom rata, kao deo odmazde određene države ili koje izazivaju velike štetne uticaje na funkcionisanje države;
- klauzula LMA 3 se razlikuje u odnosu na LMA 2 jer ne sadrži ograničenja za isplate osigurane svote;
- klauzula LMA 4, kao i LMA 3, uz dozvoljavanje pokrića za sva ona sporedna dobra koja su oštećena ili pogođena sajber-napadom, a koja nisu bila cilj sajber-napada, pri čemu sajber-napad mora biti takav da izaziva velike štetne uticaje na funkcionisanje države.

Odlučujući faktor u primeni ovih klauzula, koji je ujedno i njihov najveći nedostatak, jeste pitanje da li su državne službe pogođene države sajber-napad pripisale drugoj državi. Kao što je prikazano u delu rada posvećenom problemima određivanja sajber-napada kao ratne akcije, upravo je to najveći izazov, često i nerešiv. Ostaje da se vidi u kojoj meri će ove klauzule biti uspešne, a to će se desiti onda kada se postave zahtevi za isplatom osigurane svote nakon sajber-napada.

Ono što je nesporno jeste da uloga suda ostaje da tumači ugovor o osiguranju, a ne izjave i stavove medija i vlade.[58] Pravna pitanja nisu politička i odluke suda neće imati isto dejstvo kao međunarodno pravo – „postojanje rata zavisi od pravnog konteksta u kome nastaje, a taj kontekst i značenje su generalno podložni sudskoj identifikaciji".[59]

---

56 Gallagher Re, 2020, *Cry Cyber and Let Slip the Dogs of War,* (https://www.ajg.com/gallagherre/-/media/files/gallagher/gallagherre/cyber-reinsurance-exploring-attribution-issues-war-and-cyber.pdf, 5. 3. 2023).

57 Carter, R. A., Enoizi, J., 2020, p. 6.

58 *Holiday Inns, Inc. v. Aetna Ins. Co*., 571 F. Supp. 1460, 1464 (S.D.N.Y. 1983). Upor. *Universal Cable Prods., LLC v. Atl. Specialty Ins. Co.*, 929 F.3d 1143, 1158–59 (9th Cir. 2019).

59 Pearlstein, D., 2014, Law at the End of War*, Minnesota Law Review*, 99, p. 167.

LITERATURA

1. Carter, R. A., Enoizi, J., 2020, *Cyber War and Terrorism: Towards a Common Language to Promote Insurability*, Geneva, Geneva Association.
2. Chopra, A., 2021, Cyberattack – Intangible Damages in a Virtual World: Property Insurance Companies Declare War on Cyber-Attack Insurance Claims, *Ohio State Law Journal*, 1, pp. 121–162.
3. Clark, D., Landau, S., 2011, Untangling Attribution, *Harvard National Security Journal*, 2, pp. 41–73.
4. Eichensehr, K. E., 2020, The Law and Politics of Cyber Attack Attribution, *UCLA Law Review*, 3, pp. 520–598.
5. Ferland, J., 2019, Cyber Insurance – What Coverage in Case of an Alleged Act of War? Questions Raised by The Mondelez v. Zurich Case, *Computer Law and Security Review*, 4, pp. 369–376.
6. Gargano, D., 2013, An Act of War: Finding a Meaning for What Congress Has Left Undefined, *Touro Law Review,* 1, pp. 147–171.
7. Gartzke, E., 2013, The Myth of Cyberwar. Bringing War in Cyberspace Back Down to Earth, *International Security*, 2, pp. 41–73.
8. Glintić, M., 2020, Zaštita prava slabije ugovorne strane u skladu sa Principima evropskog ugovornog prava osiguranja, *Strani pravni živo*t, 3, str. 57–73.
9. Glintić, M., 2021, Održivost načela krajnje dobre vere u ugovornom pravu reosiguranja, u: *Zbornik radova Kopaoničke škole prirodnog prava – Slobodan Perović Primena prava i pravna sigurnost*, str. 455–469.
10. Glintić, M., 2021, Agregacija štete u skladu sa Načelima o ugovornom pravu reosiguranja, u: *Prouzrokovanje štete, naknada štete i osiguranje*, Beograd, Mionica, Institut za uporedno pravo, str. 373–385.
11. Glintić, M., Pokriće po osnovu ugovora o osiguranju prekida rada tokom pandemije kovida 19, u: Đurić, V., Glintić, M. (ur.), 2021, *Pandemija kovida 19: pravni izazovi i odgovori*, Beograd, Institut za uporeno pravo, str. 143–154.
12. Glintić, M., Schicksal der Betriebsschliessungsversicherung vor den deutschen und österreichischen Gerichten, In: Rohrbach, W. (Hrsg), 2022, *Wertewandel und Werte Renaissance in Zeiten der Pandemie und Klimakrise*, Belgrad, Wien.
13. Goldman, E., Warner, M., Why a Digital Pearl Harbour Makes Sense... and Is Possible, in: Perkovich, G., Levite, A. (eds.), 2017, *Understanding Cyber Conflict*, Washington, Georgetown University Press.
14. Haufler, V., 1997, *Dangerous Commerce: Insurance and the Management of International Risk*, London, Cornell University Press.
15. International Group of Experts at the Invitation of the NATO Cooperative Cyber Defense Centre of Excellence, 2013, *Tallinn Manual on the International Law Applicable to Cyber Warfare,* Cambridge University Press.
16. ICRC, 2020, International Humanitarian Law and Cyber Operations During Armed Conflicts, *International Review of the Red Cross*, 102.
17. Korhonen, O., 2015, Deconstructing the Conflict in Ukraine: The Relevance of International Law to Hybrid States and Wars, *German Law Journal*, 3, pp. 452–478.
18. Maurer, T., 2018, *Cyber Mercenaries: The State, Hackers, and Power*, Cambridge, Cambridge University Press.

19. Mazaraki, N., Goncharova, Y., 2022, Cyber Dimension of Hybrid Wars: Escaping a "Grey Zone" of International Law to Adress Economic Damages, *Baltic Journal of Economic Studies*, 2, pp. 115–120.
20. National Research Council, 2009, *Technology, Policy, Law, And Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*, Washington.
21. Pearlstein, D., 2014, Law at the End of War*, Minnesota Law Review*, 99, pp. 143–220.
22. Petrović Tomić, N., 2015, *Zaštita potrošača usluga osiguranja, Analiza i predlog unapređenja regulatornog okvira*, Beograd, Pravni fakultet Univerziteta u Beogradu.
23. Red, T., 2013, *Cyber War Will Not Take Place*, Oxford University Press.
24. Sanders, C., 2018, The Battlefield of Tomorrow, Today: Can a Cyberattack Ever Rise to an "Act of War"?, *Utah Law Review*, 2, pp. 503–522.
25. Shackelford, S., 2021, Wargames: Analyzing the Act of War Exclusion in Cyber Risk Insurance Coverage and Its Implications for Cybersecurity Policy, *Yale Journal of Law and Technology*, Vol. 23, pp. 362–413.
26. Shniderman, A., 2019, Prove It! Judging the Hostile-or-Warlike-Action Exclusion in Cyber-Insurance Policies, *Yale Law Journal*, 129.
27. Swiss Re Institute, 2022, *Cyber Insurance: Strengthening Resilience for the Digital Transformation*.
28. Tošić, I., Novaković, O., 2021, Osiguranje od internet rizika i nova regulativa u oblasti zaštite podataka o ličnosti, *Prouzrokovanje štete, naknada štete i nova regulativa u oblasti zaštite podataka o ličnosti*, Institut za uporedno pravo, Udruženje za odštetno pravo, Beograd, Mionica.
29. Trautman, L., Ormerod, P., 2019, WannaCry, Ransomware, and the Emerging Threat to Corporations*, Tennessee Law Review*, 2.
30. Wan, K., 2020, Notpetya, Not Warfare: Rethinking the Insurance War Exclusion in the Context of International Cyberattacks, *Washington Law Review*, 3.
31. Wolff, J., 2022, *Cyberinsurance Policy: Rethinking Risk in the Age of Ransomware, Computer Fraud, Data Breaches, and Cyberattacks*, Massachusetts.
32. Zirojević, M., 2014, *Terorizam – međunarodni pogled*, Beograd, Institut za međunarodnu politiku i privredu.
33. Zirojević, M., 2011, Zloupotreba interneta u terorističke svrhe, *Međunarodni problemi*, 3, str. 417–448.

SUDSKA PRAKSA

1. *Holiday Inns, Inc. v. Aetna Ins. Co*., 571 F. Supp. 1460, 1461 (S.D.N.Y. 1983).
2. *Mondelez Int'l, Inc. v. Zurich Am. Ins. Co*., No. 2018L011008, 2018 WL 4941760 (Ill. Cir. Ct. Oct. 10, 2018).
3. *Merck and Co., Inc. and International Indemnity Ltd. v. ACE American Insurance Company et al*, Superior Court of New Jersey Law Division: Union County, October 12, 2018.
4. *Pan American World Airways Inc. v. Aetna Casualty and Surety Co.,* 505 F.2d 989 (2nd Cir. 1974).
5. *Queen Ins. Co. v. Globe & Rutgers Fire In. Co*., 263 U.S. 487 (1924).
6. *Stankus v. N.Y. Life Ins. Co.,* 44 N.E. 2d 687 (Mass. 1942).
7. *Stinson v. N.Y. Life Ins.,* 167 F.2d 233 (D.C. Cir. 1948).

8. *Vanderbilt v. Travelers' Ins. Co.*, 184 N.Y.S. 54 (N.Y. 1920).
9. *Universal Cable Prods., LLC v. Atl. Specialty Ins. Co.*, 929 F.3d 1143, 1158–59 (9th Cir. 2019).

IZVORI SA INTERNETA

1. Fire Eye, 2019, *Double Dragon: APT41, a Dual Espionage and Cyber Crime Operation* (https://content.fireeye.com/apt-41/rpt-apt41/, 7. 2. 2023).
2. Gallagher Re, 2020, *Cry Cyber and Let Slip the Dogs of War,* (https://www.ajg.com/gallagherre/-/media/files/gallagher/gallagherre/cyber-reinsurance-exploring-attribution-issues-war-and-cyber.pdf, 5. 3. 2023).
3. Goodman, R., 2018, Cyber Operations and the U.S. Definition of "Armed Attack," *Just Security* (https://www.justsecurity.org/53495/cyberoperations-u-s-definition-armed-attack/, 7. 3. 2023).
4. Greenberg, A., 2018, *The Untold Story of NotPetya, the Most Devastating Cyberattack in History,* (https://www.wired.com/story/notpetyacyberattack-ukraine-russia-code-crashed-the-world/, 15. 2. 2023).
5. Griffin R., Chiglinsky, K., Voreacos, D., 2019, Was It an Act of War? That's Merck Cyber Attack's $1.3 Billion Insurance Question, *Insurance Journal* (https://www.insurancejournal.com/news/national/2019/12/03/550039.htm, 20. 2. 2023).
6. Kopan, T., 2016, *Is Trump Right? Could a 400-Pound Couch Potato Have Hacked the DNC*? (https://edition.cnn.com/2016/09/27/politics/dnc-cyberattack-400-pound-hackers/index.html, 4. 2. 2023).
7. Massmann, S., 2001, *War Risk Exclusion Legal History Outlined*, (https://www.propertycasualty360.com/2001/09/30/war-risk-exclusion-legal-history-outlined/, 3. 2. 2023).
8. McCabe, M., 2018, *NotPetya Was Not Cyber 'War'* (https://www.marshmclennan.com/insights/publications/2018/aug/notpetya-was-not-cyber-war.html, 22. 2. 2023).
9. McGuinness, D., 2017, *How a Cyber Attack transformed Estonia* (https://www.bbc.com/news/39655415, 13. 3. 2023).
10. Satariano, A., Perlroth, N., 2019, *Big Companies Thought Insurance Covered a Cyberattack. They May Be Wrong* (https://www.nytimes.com/2019/04/15/technology/cyberinsurance-notpetya-attack.html, 5. 2. 2023).
11. Shahani, A., 2014, *Doubts Persist on U.S. Claims of North Korean Role in Sony Hack* (https://www.npr.org/sections/alltechconsidered/2014/12/26/373303733/doubts-persist-on-u-s-claims-on-north-korean-role-in-sony-hack, 5. 2. 2023).
12. U. S. Department of Justice, 2020, *Press Release, Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace* (https://www.justice.gov/opa/pr/sixrussian-gru-officers-charged-connection-worldwide-deployment-destructivemalware-and, 7. 3. 2023).
13. https://www.theguardian.com/world/2022/feb/27/anonymous-the-hacker-collective-that-has-declared-cyberwar-on-russia, 8. 3. 2023.

CYBER WAR AS AN EXCLUSION CLAUSE IN INSURANCE CONTRACTS

Mirjana Glintić

ABSTRACT

NotPetya cyber-attacks have caused major damage to companies around the world. Those that had signed contracts on various types of property insurance turned to the insurers hoping to have the damage compensated. However, the insurers invoked the war exclusion clause, due to the fact that they considered given cyber-attacks to be a part of the ongoing Russian-Ukrainian conflict. Since the two American companies initiated the court proceedings against their insurers, the author devotes the central part of the paper to the analysis of the court decisions on this issue. Comparative legal analysis, of both international public law regulations and of the general and special conditions of insurance policy, signaled several shortcomings of the insurers' argumentation on invoking the war exclusion clause. The first one concerns the inability of insurers to prove that a cyber-attack represents a war action between two states. Another shortcoming concerns the fact that cyber-attacks are directed against companies and not against sovereign states. The paper also contains certain proposals for necessary changes of insurance policies, regarding the term cyber-attack and the conditions for applying war exclusion clause. The author concludes that the policy should always be interpreted in favor of coverage, especially when there are no indications that the war exclusion clause was a matter of negotiation and if standard language was used in the insurance policy.

Key words: insurance, war exclusion clause, cyber-attack, cyber war, NotPetya.