Др Драган Дакић, доцент
Правног факултета Универзитета у Крагујевцу

УДК: 004.738.5:347.7
DOI: 10.46793/XVIIIMajsko.389D

УСЛУГЕ У ДИГИТАЛНОМ ОКРУЖЕЊУ: НОВИ АСПЕКТ МЕЂУНАРОДНОГ СУБЈЕКТИВИТЕТА НЕДРЖАВНИХ СУБЈЕКАТА?

Резиме

Предмет истраживања у овом раду јесте могућност недржавних субјеката, корпорација, да пружају ius ad bellum услуге у дигиталном окружењу и то не само државама већ и другим недржавним субјектима. Ius ad bellum услуге у дигиталном окружењу се односе на могућност посматраних субјеката да путем њиховог пружања учествују у сајбер сукобима који се због своје разорне моћи на имовину и људске животе могу изједначити са оружаним сукобима. У наведеном налазимо основ да посматране услуге подведемо под активности из ius ad bellum домена. Разлог за овакво дефинисање предмета истраживања је у чињеници да је дигитално окружење омогућило овим недржавним субјектима предузимање аката који су традиционално сврстани у домен државног међународног субјективитета. Главни резултати истраживања су да се кроз пружање посматраних услуга другим недржавним субјектима заснивају међународни односи између ових субјеката међународног права и то са пуном правностварајућом способношћу. На овај начин дошло је до надоградње међународног субјективитета компанија из пасивне способности која подразумјева њихову директну обавезаност нормама међународног права али искључује њихову могућност стварања међународног права ка активном субјективитету који подразумјева међународноправну легислативну способност. Дакле, захваљујући развоју дигиталних услуга, корпорације су као носиоци пасивног субјективитета стекле и активни међународни субјективитет или су макар развиле нови аспект постојећег међународног субјективитета.

Кључне речи: *дигиталне услуге, ius ad bellum, недржавни субјекти, међународни субјективитет.*

1. Увод

Питање међународноправног субјективитета можемо посматрати у вестфалском контексту као способност држава – неспорних и основних субјеката међународног права, да кроз успостављање међународних односа са другим државама преузимају права и обавезе који су регулисани међународним правом. Схватајући појам међународног субјективитета као способност његовог титулара да, осим наведене правне способности посједује и пословну и процесну способност као и деликтну одговорност, јасно је да се овај појам не може ограничити искључиво на државе. Тако је данас у литератури присутна класификација субјеката међународног јавног права по којој у ту категорију спадају државе, међународне организације и недржавни субјекти. Сваку од наведених група карактеришу дистинктивна питања у вези одређивања садржине и обима њеног међународног субјективитета. Такође, и сам појам међународног субјективитета је варијабилан и у многоме зависи од околности.[1] У овом раду пажњу смо посветили недржавним субјектима, тј. посебном аспекту њиховог међународног субјективитета који се развија у дигиталном добу и то најчешће путем услуга. Разлог за овакво дефинисање предмета истраживања је у чињеници да је дигитално окружење омогућило недржавним субјектима предузимање аката који су традиционално сврстани у домен државног међународног субјективитета што у извјесној мјери представља повећан степен приватизације међународног јавног права односно међународних односа.

Овако постављен предмет истраживања захтјева одређено појмовно дефинисање у уводном дијелу како би се правилно схватила дискусија која слиједи. Појмови које је потребно дефинисати за потребе овог рада су „недржавни субјекти", „дигитално окружење" и „*ius ad bellum* услуге у дигиталном окружењу". Што се тиче недржавних субјеката прихваћен став је да у ову категорију спадају ентитети унутар држава, међународне компаније, невладине организације и појединци. Већ из самог списка субјеката из ове групе видно је да обим и садржина њиховог међународноправног капацитета варира како у међусобном поређењу тако и у поређењу са субјектима из других група. С обзиром да је предмет истраживања одређен услугама у дигиталном добу, у овом раду ћемо под недржавним субјектима подразумјевати прије свега приватне међународне компаније (не тзв. *public international companies*), које своју пословну међународноправну способност користе у дигиталном окружењу. У литератури постоје бројни критеријуми који се предлажу за потребе појмовног дефинисања међународних корпорација.[2] Овде ћемо указати само на неке од

[1] Shaw, M., *International Law,* (9th ed.), Cambridge: Cambridge University Press, 2021. doi:10.1017/9781108774802 pp. 154.

[2] Hamdani, K., Ruffing, L., *United Nations Centre on Transnational Corporations: Corporate Conduct and the Public Interest,* London, 2015; Wouters, J., Chané, A.-L., *Multinational Corporations in International Law,* in NonState Actors in International Law, (ed. Noortmann,

најосновнијих карактеристика ових субјеката. Основна карактеристика посматраних субјеката међународног права јесте то да они своју пословну дјелатност обављају на територији више држава. С обзиром да дигитално окружење омогућава да се пословна дјелатност обавља на тржиштима ван сједишта и мимо физичких пословница компаније, можемо сматрати да ову карактеристику данас посједују сва предузећа која послују у дигиталном окружењу. Наведено је нарочито изражено у области пружања услуга.

Следећа карактеристика субјеката из ове групе јесте та да они не функционишу по међународном праву.[3] Ову карактеристику не треба схватити у смислу имунитета међународних корпорација на обавезе које произилазе из норми међународног јавног права,[4] нарочито не оних које су когентног карактера.[5] Критеријум по којем се захтјева да субјекти међународног јавног права буду директни адресати међународних норми[6] је испуњен у погледу међународних корпорација. Ову тврдњу можемо доказати између осталог на основу следећих примјера. Појашњење међународних обавеза ових субјеката са аспекта људских права можемо пронаћи у Општим принципима (2011) формулисаним од стране радне групе коју је именовао УН-ов Савјет за људска права а који се односе на поштовање људских права од стране транснационалних корпорација и других пословних субјеката.[7] Према принципу бр. 13. посматрани субјекти међународног јавног права треба да ускладе своје пословање са

M., Reinisch, A., Ryngaert C.) Oxford, 2015, p. 225; Jenks, C. W., in *Transnational Law in a Changing Society* (ed. Friedman, W., Henkin, L., Lissitzyn O.), New York, 1972, p. 70; Baade, H., in *Legal Problems of a Code of Conduct for Multinational Enterprises* (ed. Horn, N.), Boston, 1980; Charney, J., *Transnational Corporations and Developing Public International Law*, Duke Law Journal, 1983, p. 748; Rigaux, F., *Transnational Corporations*, in Bedjaoui, International Law: Achievements and Prospects, p. 121; Henkin, L. *et al.*, *International Law: Cases and Materials*, p. 368. See also Muchlinski, P., *Multinational Enterprises*; Vazquez, C. M., *Direct vs Indirect Obligations of Corporations under International Law*, Columbia Journal of Transnational Law, no. 43/2005, p. 927; Johns, F., *The Invisibility of the Transnational Corporation: An Analysis of International Law and Legal Theory*, Melbourne University Law Review, no. 19/1993–4, p. 893; Eshanov, D., *The Role of Multinational Corporations from the Neoinstitutionalist and International Law Perspectives*, New York University Environmental Law Journal, no. 16/2008, p. 110; Ratner, S. R., *Corporations and Human Rights: A Theory of Legal Responsibility*, Yale Law Journal, no. 111/2001, p. 443 (преузето од Shaw, M., *нав. дело*).

[3] Димитријевић, В. и др., *Основи међународног јавног права*, Београд, 2012, стр. 128.

[4] UNHCR, The Corporate Responsibility to Protect Human Rights: An Interpretive Guide, New York, 2012.

[5] Kelly, J. M., *Prosecuting Corporations for Genocide*, Oxford Scholarship Online, 2016, DOI:10.1093/acprof:oso/9780190238896.001.0001

[6] Крећа, М., *Међународно јавно право*, Београд, 2020. стр. 121.

[7] The UN Human Rights Council established a Working Group on on the issue of human rights and transnational corporations and other business enterprises in 2011, A/HRC/17/4. www.ohchr.org/EN/Issues/Business/Pages/WGHRandtransnationalcorporationsandotherbusiness.aspx

обавезом поштовања људских права на тај начин да избјегавају активности које доприносе кршењу људских права или да кроз своје активности ублаже или отклоне негативне ефекте до којих долази усљед обављања пословне дјелатности.[8]

Што се тиче посматраног захјтева у погледу међународног кривичног права, теорија је понудила становиште по којем посматрани субјекти ипак јесу директни адресати његових норми. Заснивајући своју аргументацију на прецедентима кривичне одговорности корпорација *Kelly* тврди да је могуће извести основе за кривично гоњење корпорација за помагање у извршењу злочина геноцида, за удружене злочиначке (геноцидне) подухвате, вјероватно и за неке директније радње извршења злочина гноцида Ипак, имајући у виду процесна ограничења у Римском статуту као и изостанак процесуирања корпорација (нпр. И.Г. Фарбен, компаније која је производила гасове коришћене за убиство жртава Холокауста), у тзв. индустријским процесима у Нирнбергу,[9] оваква врста одговорности посматраних субјеката је радије *de lege ferenda.* Међутим, постоје извори међународног права који прописују кривичноправну одговорност корпорација (директни адресати),[10] те је предметни критеријум такође испуњен.

Дакле, када је ријеч о не функционисању по принципима међународног права, мисли се на то да посматрани субјекти не заснивају своје међународне односе на *jus imperii*, ради чега им потенцијално недостају одређена процесна права, попут страначке способности, пред међународним судовима. Оваква крња процесна способност може да представља битну мањкавост међународноправног субјективитета уколико прихватимо да субјективитет зависи од нечије способности да на овај начин оствари своја права.[11] За ово истраживање интересантно је становиште по којем *ius ad bellum* садржински дио ове способности и елемент „идеалног бића субјективитета".[12] Тачније, управо услуге које корпорације пружају у вези са *ius ad bellum* у дигиталном окружењу су идеја овог наслова.

Ius ad bellum услуге у дигиталном окружењу се односе на могућност посматраних субјеката да учествују у сајбер сукобима директно или путем пружања услуга другим учесницима ових сукоба који се због своје разорне моћи на имовину и људске животе могу изједначити са оружаним сукобима. Наиме, услуге у дигиталном окружењу подразумјева употребу информационих и

[8] *Исто*.
[9] Lustig, D., *The Nature of the Nazi State and the Responsibility of Corporate Officials at Nuremberg* at Lustig, D., Veiled Power: International Law and the Private Corporation 1886-1981, Oxford University Press (2020) DOI:10.1093/oso/9780198822097.003.0004
[10] Погледати Kelly, J. M., *нав. дело*, стр 500.
[11] Shaw, M., *нав. дело,* стр.154-157.
[12] Погледати Креһа, М., *нав. дело,* стр. 122.

комуникацијских технологија које су већ препознате као оружје,[13] које може утицати чак на међународни мир и безбједност.[14] Стога сматрамо да можемо прихватити становиште које предлаже *Roscini* а према којем је мјеродавна способност употребљеног оружја да доведе до страдања тј. губитка људских жртава, и до материјалне штете како би се могла успоставити аналогија између сајбер и оружаног напада.[15] На основу наведеног посматране услуге подводимо под *ius ad bellum*.

Корисно је да овде укажемо и на општу полемику која се тиче саме примјењивости међународног јавног права у дигиталном окружењу, тј. могућности да субјекти наступају користећи се са *jus imperii* прерогативима. Наиме, одређене карактеристике дигиталног простора као што је претпостављена безтериторијалност доводе у питање примјену међународног јавног права. Уколико би дигитално окружење заиста било лишено територијалности државе би у њему биле лишене суверенитета као и свега онога што из суверенитета произилази. Међутим, сајбер простор није конципиран као безтериторијална и безгранична димензија. Ово је јасно исказано у Извјештају (2013 па 2015) сачињеном од стране УН-ове групе владиних експерата о развоју информационих и комуникацијских технологија у контексту међународне безбједности, према којем држава има суверенитет над овим технологијама смјештеним на њеној територији.[16] На овај начин се успоставља државно подручје у дигиталном окружењу. Иако ове границе нису одредиве на традиционалне начине, ипак су видљиве путем тзв. националних домена (нпр. интернет адресе као и претраживачи из Републике Србије се завршавају доменом „*.rs*“) који се додјељују државама и оперативни су на њиховим територијама.

Што се тиче дигиталног окружења - другог појма чије одређење је неопходно, важно је да схватимо из чега се оно састоји. Поуздану одредницу у том смислу налазимо у Рјечнику термина коришћених од стране УН-овог Комитета о правима дјетета у Генералном коментару број 25 о дјечијим правима у дигиталном окружењу.[17] Поред ИКТ, дигитално окружење сачињавају дигиталне мреже, садржај, услуге и апликације, умрежени уређаји и окружења, виртуелна и проширена реалност, вјештачка интелигенција, роботика, аутоматизовани системе, алгоритми и аналитика података, биометрија и технологија имплантата.[18] Сваки од ових елемената би могао да буде предмет

[13] Dinstein, Y., *Cyber war and international law: Concluding remarks, at the 2012 Naval War College International Law Conference* (2013) 89 International Law Studies, 2013, p. 276, 280.
[14] UN Doc A/66/152/Add.1, 16 September 2011, p. 2
[15] Roscini, M., *Cyber operations as a use of force at International Law and Cyberspace*, Research Handbook, eds. Tsagourias and Buchan, Edward Elgar Publishing Limited, 2021, pp. 299.
[16] *Исто*.
[17] Treaty bodies Download (ohchr.org)
[18] A terminology glossary to the UN Committee on the Rights of the Child. (2021). General Comment No. 25 (2021) on children's rights in relation to the digital environment available at Treaty bodies Download (ohchr.org)

посебног техничког и правног елаборирања што би и по обиму и тематски изашло ван оквира овога рада. Умјесто тога, користићемо појам дигитално окружење као синоним за све његове елементе. Такође, поједине елементе који се директно тичу предмета истраживања као што су вјештачка интелигенција, аутоматизовани системи и алгоритми ћемо представити са правног аспекта.

У првом дијелу рада ћемо представити регулисање услуга у дигиталном окружењу у оквиру Европске уније као међународне организације. С обзиром да Европска унија посједује легислативне компетенције у овој области,[19] међународни субјективитет овог субјекта међународног права евидентно спада у категорију активног субјективитета. У овом дијелу рада указано је на општа правна питања која се отварају, и у главном остају без одговора, усљед употребе вјештачке интелигенције. Дискусија се претежно односи на употребу вјештачке интелигенције у цивилне сврхе са фокусом на пружање услуга. Главно правно питање на које се директно или имплицитно односи дискусија јесте питање одговорности. Први дио рада је након представљања правних оквира за употребу вјештачке интелигенције у процесу одлучивања завршен представљањем текућих легислативних процеса у посматраној области на нивоу Европске уније. Други дио рада је фокусиран на питања употребе вјештачке интелигенције у извршењу војних задатака. Представљени су начини на које се користи вјештачка интелигенција те је указано на који начин се може засновати примјенљивост норми међународног права у овој области и то када се као пружаоци услуга јављају недржавни субјекти а као примаоци се јављају државе. Глвани дио овог рада, као и чланка у цјелини, бави се питањима пружања *ius ad bellum* услуга у дигиталном окружењу и то у ситуацији у којој се недржавни субјекти појављују и као пружаоци услуга и као њихови примаоци. Ова ситуација је изабрана са намјером, како би се показали формални и фактички услови који омогућавају корпорацијама стицање новог аспекта међународног субјективитета.

2. Регулисање услуга у дигиталном окружењу у Европској унији

Не тако давно Европска унија је разматра увођење појма „Електронске личности“[20] тј. електронског субјекта, како би одговорила на правна питања повезана са употребом и креирањем робота и вјештачке интелигенције. Теоријска расправа у вези употребе поменутих ентитета као и њихових правних способности је блиска становишту признања њиховог

[19] **Savin, A.,** ***EU Internet Law*****, Edward Elgar Publishing 2020.**

[20] Committee on Legal Affairs of the European Parliament, DRAFT REPORT http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML%2BCOMPARL%2BPE-582.443%2B01%2BDOC%2BPDF%2BV0//EN

субјективитета.[21] С тим у вези потребно је да знамо да техничке карактеристике битно одређују правну способност, односно капацитете ових потенцијалних субјеката јер акти које предузима вјештачка интелигенција могу бити у потпуности ограничени инсталираним програмом али и аутономно постављени уз способност софтвера да самостално учи (тзв. *machine learning*) и одлучује.[22] За употребу софтвера из ове друге групе готово да потпуно недостају правни оквири а према праву Европске уније евентуална његова (употребна) класификација би била могућа.[23]

Без обзира на ове недостатке који су и даље присутни, вјештачка интелигенција, аутоматизовани системи и алгоритми налазе веома широку употребу у готово свим аспектима модерног живота. Ови елементи дигиталног окружења широко се употребљавају у цивилне и војне сврхе што је праћено бројним правним изазовима. У том смислу можемо да уочимо да двије велике групе правних питања са бројним међусобно повезаним и условљеним аспектима карактеришу општу дебату о употреби вјештачке интелигенције. Прва група правно интересантних питања се односи на прикупљање, обраду и складиштење података (гориво за вештачку интелигенцију). Можемо сматрати да су главна питања у вези података покривена комплексном легислативом која је унификована на нивоу ЕУ.[24] Друга група питања се тиче саме вјештачке интелигенције, којој недостаје свеобухватан и унификован правни оквир на нивоу Европске уније (ЕУ).[25] Из тог разлога, нека од основних питања као што је дефиниција вјештачке интелигенције,[26] као и кључна правна питања која произилазе из њене примјене, као што су грађанскоправна одговорност,[27] деликтна одговорност, давање сагласности и очување приватности остају без одговора. Недостатак кохерентних законских оквира негативно утиче на употребу вјештачке интелигенције како у војне тако и у цивилне сврхе

[21] Behdadi, D., Munthe, C., *Artificial Moral Agency: Philosophical Assumptions, Methodological Challenges, and Normative Solutions*, 2018. This is a "postprint", the authors' submitted manuscript after peer review to a scientific journal. Citations should refer to the published version of the article, once that exists

[22] Погледдати Grant, D. T., Wischik, J. D., *On the path to AI Law's prophecies and the conceptual foundations of the machine learning age*, Springer Nature, 2020 https://doi.org/10.1007/978-3-030-43582-0

[23] Regulation (EU) 2017/745, Annex VIII Article 3.3.

[24] Directive 95/46/EC (General Data Protection Regulation).

[25] Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain union legislative acts, COM (2021) 206 final, Brussels, 21.4.2021.

[26] Identification and assessment of existing and (europa.eu), p. 45.

[27]The European Parliament Resolution with recommendations to the Commission on a civil liability regime for artificial intelligence (2020/2014(INL) Procedure File: 2020/2014(INL) | Legislative Observatory | European Parliament (europa.eu) (Resolution on liability)

нарочито у задацима доношења одлука.[28] Тренутно, само нека фрагментна правила која се односе на кључна правна питања употребе вјештачке интелигенције у цивилне сврхе би могла бити изведена из постојећег законодавства ЕУ и то оног које се директно не тиче вјештачке интелигенције.[29]

На примјер, у случају да је штета проузрокована неисправним софтвером који се користи у пружању услуге, штета ће бити надокнадива према Директиви о одговорности за производе (85/374/ЕЕЦ) [30], односно оштећени може поднијети тужбу према Директиви 85. /374 против произвођача софтвера.[31] Ово правило, међутим, не важи за такозвани бестјелесни софтвер – онај који функционише на мрежама или интернету. Истовремено, безбједност услуге је ван дјелокруга Директиве 2001/95 о општој безбједности производа која укључује сваки производ намјењен за потрошачку употребу или који ће вероватно бити коришћен од стране потрошача укључујући и у сврху пружања услуге.

Што се тиче употребе вјештачке интелигенције у процесу доношења одлука у цивилним пословима релевантни правни оквири могу се наћи у Резолуцији о одговорности која предвиђа правила о пуштању у промет,[32] пуштању у употребу и коришћењу система вештачке интелигенције, као и у правилима која се односе на софтвер. Пошто у главне резултате процеса одлучивања спадају предвиђања, препоруке или одлуке, по том основу ће бити примјењиви и правни акти који прописују правила за модерирање алгоритамског садржаја, препоруке или доношење одлука.[33] Иначе, поступак нормирања дигиталних услуга на нивоу Европске уније је у току и нарочито је интензивиран почетком 2022. године. Ријеч је о Акту о дигиталним услугама и основним правима *(Digital Services Act and fundamental rights issues posed),*[34] за који се очекује да у коначној верзији текста буде усвојен 28.04.2022. односно 04.05.2022. године.[35]

[28] Artificial Intelligence in Medicine (Eds. Niklas Lidströmer, Hutan Ashrafian), Springer, 2022

[29] *Исто*.

[30] Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products. Directive 1999/34/EC extended the scope of liability to agricultural and fishery products

[31] C-203/99 Veedfald, and C-495/10, Dutrueux

[32] Уопштено говорећи, за медицинске уређаје су директно релевантни the Regulations on Medical Devices (Regulation (EU) 2017/745) and on In-Vitro Diagnostic Devices (Regulation (EU) 2017/746).

[33] Identification and assessment of existing and (europa.eu), p. 45

[34] Texts adopted - Digital Services Act and fundamental rights issues posed - Tuesday, 20 October 2020 (europa.eu)

[35] DMA: significant additions made it into the final text – EURACTIV.com

3. Вјештачка интелигенција и услуге *ius ad bellum*

Ситуација са коришћењем вјештачке интелигенције поступку одлучивања у војним задацима се нарочито не разликује у односу на претходно описано. Главно питање употребе вјештачке интелигенције у војне сврхе јесте питање одговорности за акте које предузму аутономни системи што представља изазов и са аспекта важећих правила међународног права. Ипак, вјештачка интелигнецција се користи било за извођење напада конвенционалним наоружањем било за извођење сајбер напада у дигиталној сфери. Посљедице употребе вјештачке интелигенције на било који од ова два начина свакако стварају посљедице по имовину и људске животе те их је нужно подвести под норме међународног јавног права, односно међународног кривичног права и међународног хуманитарног права.[36] Овај задатак није ни мало једноставан,[37] отвара нека од најзначајнијих питања из међународног хуманитарног права,[38] и додатно се компликује уколико су софтверске услуге овакве врсте пружене од стране приватних компанија.[39]

Наиме, без обзира (или можда баш због) недостајућих међународноправних оквира који би јасно дефинисали питања у вези војне употребе вјештачке интелигенције, она налази широку примјену почевши од система који чувају границе, система који штите ратне бродове, антиракетних система, антирадарских система, извиђачких и бојевих дронова и то у својој аутоматизованој, најчешће од човјека неконтролисаној, варијанти.[40] Многе од ових војних функција су приватизоване те квалификоване као услуге које државама пружају приватне компаније.[41] Бројни аутори су писали о овој појави, дискутујући о њој у контексту тржишта војне силе и посљедицама

[36] Погледати Ambos, K., *International criminal responsibility in cyberspace* at International Law and Cyberspace (Research Handbook, eds. Tsagourias and Buchan), Edward Elgar Publishing Limited, 2021.

[37] Погледати Дакић, Д., *Сајбер напади и међународно јавно право*, Зборник радова: Отворена питања међународног кривичног права и реформа кривичног законодавства Републике Србије, Златибор, 2022. (у штампи).

[38] Sparrow, R., *War Without Virtue?* in B. Strawser (ed.), Killing by Remote Control (Oxford: Oxford University Press, 2013; Strawser, B., *Moral Predators: The Duty to Employ Uninhabited Aerial Vehicles*, Journal of Military Ethics, 9(4)/2010, p. 342–68; McMahan, J., *The Ethics of Killing in War*, Ethics, 114(4)/2004, p. 693–733; McMahan, J., *On the Moral Equality of Combatants*, Journal of Political Philosophy, 14(4)/2006, p. 377–496 (референце преузете од Dickinson, L., *Drones, Automated Weapons, and Private Military Contractors*, in Land, M., Aronson, J., (Eds.), New Technologies for Human Rights Law and Practice, 2018, pp. 93-124. Cambridge: Cambridge University Press. doi:10.1017/9781316838952.005)

[39] Погледати Dickinson, L., *нав. чланак.*

[40] *Исто*.

[41] *Исто*.

приватизације сектора безбједности, очувању јавних вриједности у свијету приватизованих међународних односа, модерног ратовања и развоју индустрије приватних армија.[42] У контексту овога рада наведена појава је означена појмом услуга у дигиталном окружењу или дигиталне услуге јер се фокусирамо само на војне услуге које подразумјевају употребу елемената дигиталног окружења. На овај начин истраживање је подведено под дискурс о међународном субјективитету недржавних субјеката као пружаоца посматраних услуга.

У том смислу, учешће приватних компанија у војним сукобима није новина. Историјски, познати су злочини које су починиле холандске и британске источноиндијске компаније.[43] Такође, међународно право кроз судску праксу може да понуди и одговоре на питања одговорности државе за акте које почине приватне компаније.[44] Међународноправни оквири могу да пруже одговор на питање одговорности држава за акте приватних субјеката на два начина и то[45]:

> (1) Када су акти недржавних субјеката у потпуности приписиви држави и тада користимо Чланове о државној одговорности за међународно незаконите акте (*Articles on the Responsibility of States for Internationally Wrongful Acts*);[46]
> (2) Када држава пропусти своју обавезу (дужне пажње) да не дозволи употребу властите територије за извршење аката који су супротни правима неке друге државе (*sic utere tuo ut alienum non laedas*) и тада се ослањамо на правила установљена кроз судску праксу попут оне у случају *Corfu*

[42] Avant, D., *The Market for Force: The Consequences of Privatizing Security*, Cambridge: Cambridge University Press, 2005; Dickinson, L., *Outsourcing War and Peace: Preserving Public Values in a World of Privatized Foreign Affairs*, New Haven, CT: Yale University Press, 2011; McFate, S., *The Modern Mercenary: The Rise of the Privatized Military Industry*, Oxford: Oxford University Press, 2014; Singer, P., *Corporate Warriors: The Rise of the Privatized Military Industry*, Ithaca, NY: Cornell University Press, 2007. референце преузете од Dickinson, L., *нав. чланак.*

[43] Luttikhuis, B., Moses, A. D., *Mass violence and the end of the Dutch colonial empire in Indonesia*, Journal of Genocide Research, no. 14:3-4/2012, p. 257-276, DOI: 10.1080/14623528.2012.719362

[44] Alabama claims of the United States of America against Great Britain, Award rendered on 14 September 1872 by the Tribunal of arbitration established by Article I of the Treaty of Washington of 8 May 1871, RIAA, Vol. XXIX.

[45] Дакић, Д., *нав. чланак.*

[46] International Law Commission, *Draft articles on Responsibility of States for Internationally Wrongful Acts, with commentaries*, Yearbook of the International Law Commission 2001, Vol. II. Part. 2

Channel Case,[47] или *Case Concerning United States Diplomatic and Consular Staff in Tehran*.[48]

Међутим, посматране дигиталне услуге које приватне компаније пружају нису ограничене само на државе као кориснике. Банелиер и Кристакис[49] указују на могућност да приватне компаније овакву врсту услуга могу пружати и другим приватним компанијама. Дакле, између ових субјеката међународног права долази до заснивања међународних односа, у сфери која традиционално припада домену државног субјективитета, независно од воље држава, и са пуном правностварајућом способношћу. Из уводне дискусије видјели смо да се међународни субјективитет компанија заснива првенствено на њиховој пасивној међународноправној способности која подразумјева њихову директну обавезаност нормама међународног права али искључује њихову могућност стварања међународног права.[50] Формални основ за аутономно, правностварајуће, регулисање међународних односа у дигиталном окружењу између ових носилаца међународног субјективитета, суштински деривира из чињенице да се на ове субјекте и њихове акте наведене врсте не могу примјенити одредбе чл. 2 ст. (4) Повеље уједињених нација.[51] Дакле, захваљујући развоју дигиталних услуга, корпорације су као носиоци пасивног субјективитета стекле и активни међународни субјективитет или су макар развиле нови аспект свог међународног субјективитета. Овим, корпорације су се приближиле стицању поменутог идеалног бића субјективитета.

Фактички основ за овакву кључну улогу приватних компанија у сфери дигиталних услуга Банелиер и Кристакис виде у чињеници да су управо компаније те које су прве и највише погођене сајбер криминалом и сајбер-нападима ради чега су са правом развиле системе самозаштите; као и у чињеници да дигиталне услуге доносе огроман потенцијал за раст за који су компаније витално заинтересоване.[52]

4. Закључак

Предмет истраживања у овом раду јесте могућност недржавних субјеката, корпорација, да пружају *ius ad bellum* услуге у дигиталном окружењу и то не само државама већ и другим недржавним субјектима. Након дефинисања кључних појмова, „недржавни субјекти“ и „дигитално окружење“, кроз текст је појам услуге у дигиталном окружењу или дигиталне за потребе овог рада су

[47] Corfu Channel Case, Judgment of 4 April 1949, ICJ Reports 1949
[48] United States of America v. Iran, Judgment of 24 May 1980, ICJ Reports 1980
[49] Bannelier, K., Christakis, T., *Cyber-Attacks – Prevention-Reactions: The Role of States and Private Actors*, Les Cahiers de la Revue Défense Nationale, Paris, 2017.
[50] Погледати Креча, М., *нав. дело*, стр. 123.
[51] Roscini, M., *нав. дело*, стр. 299.
[52] Bannelier, K., Christakis, T., *нав. чланак*, стр. 10.

дефинисане као војне услуге које подразумјевају употребу елемената дигиталног окружења прије свега вјештачке интелигенције. Овако постављен предмет истраживања је анализиран кроз два главна дијела рада и то првог дијела у ком је представљено регулисање услуга у дигиталном окружењу у оквиру Европске уније као међународне организације. Дискусија у овом дијелу рада је показала да иако нека од основних питања као што је дефиниција вјештачке интелигенције, укључујући и кључна правна питања која произилазе из њене примјене, као што су грађанскоправниа одговорност, деликтна одговорност, давање сагласности и очување приватности остају без одговора, ипак вјештачка интелигенција налази широку употребу. Одговори на правна питања која произилазе из употребе вјештачке интелигенције се евентуално могу извести из правила садржаних у актима који се не односе директно на вјештачку интелигенцију. Такође, регулисање дигиталних услуга заузима једно од централних мјеста у легислативним активностима Европске уније.

Други дио рада који се бави питањима употребе вјештачке интелигенције за потребе извршења војних задатака појаснио је начине на које се може засновати примјенљивост норми међународног права у дигиталној области, тачније на који начин се може засновати одговорност држава као корисника дигиталних услуга за акте недржавних субјеката као пружаоца услуга у дигиталном окружењу. Први начин је када су акти недржавних субјеката у потпуности приписиви држави. Други начин, није директно повезан са темом истраживања и односи се на ситуацију у којој држава пропусти дужну пажњу и не спријечи настанак штетне посљедице по другу државу. Међутим, посматране дигиталне услуге које приватне компаније пружају нису ограничене само на државе као кориснике. Приватне компаније овакву врсту услуга могу пружати и другим приватним компанијама чиме се између ових субјеката међународног права заснивају међународни односи, у сфери која традиционално припада домену државног субјективитета, независно од воље држава, и са пуном правноствараjућом способношћу.

Из уводне дискусије видјели смо да се међународни субјективитет компанија заснива првенствено на њиховој пасивној међународноправној способности која подразумјева њихову директну обавезаност нормама међународног права али искључује њихову могућност стварања међународног права. Формални основ за аутономно, правноствараjуће, регулисање међународних односа у дигиталном окружењу између ових носилаца међународног субјективитета, суштински деривира из чињенице да се на ове субјекте и њихове акте наведене врсте не могу примјенити одредбе чл. 2 ст. 4, Повеље уједињених нација. Дакле, захваљујући развоју дигиталних услуга, корпорације су као носиоци пасивног субјективитета стекле и активни међународни субјективитет или су макар развиле нови аспект свог међународног субјективитета. Овим, корпорације су се приближиле стицању поменутог идеалног бића субјективитета. Фактички основ за овакву кључну улогу приватних компанија у сфери дигиталних налази се у чињеници да су

управо компаније те које су прве и највише погођене сајбер криминалом и сајбер-нападима ради чега су развиле системе самозаштите; као и у чињеници да дигиталне услуге доносе огроман потенцијал за раст за који су компаније витално заинтересоване.

Dragan Dakić, Ph.D., Assistant Professor
Faculty of Law, University of Kragujevac

DIGITAL SERVICES: SUBJECTIVITY UPGRADE FOR NON-STATE ACTORS?

Summary

The subject of research in this paper is the possibility of non-state international subjects, corporations, to provide ius ad bellum services in the digital environment, but not only to the States but also to other non-state entities. Ius ad bellum services in the digital environment refer to the ability of the observed entities to get involved in cyberwarfare via services they provide. Cyberwarfare is considered to be equivalent of armed conflicts due to its destructive effects on property, critical infrastructure and human lives. This is the reason to to classify the observed services under activities from the domain of ius ad bellum. The research was framed as such because the digital environment enabled non-state subjects to undertake acts that were traditionally subsumed within the ambit of States subjectivity. The main results of the research elucidated suchlike services provision establishes international relations between non-state entities which is followed by full legislative capacity of the parties. In this way, the international subjectivity of companies was upgraded from passive, which provided them only with duties to respect but not to create international law, to to active subjectivity, which implies their international legislative capacity. Thus, the development of digital services enabled corporations as bearers of passive subjectivity to acquire active international subjectivity or at least developed a new aspect of it.

Key words: *digital services, ius ad bellum, non-state subjects, international subjectivity.*

Литература

A terminology glossary to the UN Committee on the Rights of the Child. (2021). General Comment No. 25 (2021) on children's rights in relation to the digital environment available at Treaty bodies Download (ohchr.org).

Alabama claims of the United States of America against Great Britain, Award rendered on 14 September 1872 by the Tribunal of arbitration established by Article I of the Treaty of Washington of 8 May 1871, RIAA, Vol. XXIX.

Artificial Intelligence in Medicine (Eds. Niklas Lidströmer, Hutan Ashrafian), Springer, 2022.

Ambos, K., *International criminal responsibility in cyberspace* at International Law and Cyberspace, (Research Handbook, eds. Tsagourias and Buchan), Edward Elgar Publishing Limited, 2021.

Bannelier K., Christakis, T., *Cyber-Attacks – Prevention-Reactions: The Role of States and Private Actors*, Les Cahiers de la Revue Défense Nationale, Paris, 2017.

Behdadi, D., Munthe, C., *Artificial Moral Agency: Philosophical Assumptions, Methodological Challenges, and Normative Solutions*, 2018. This is a "postprint", the authors' submitted manuscript after peer review to a scientific journal. Citations should refer to the published version of the article, once that exists.

Thomas D. Grant, D. T., Wischik, J. D., *On the path to AI Law's prophecies and the conceptual foundations of the machine learning age*, Springer Nature, 2020.

Dickinson, L., (2018). *Drones, Automated Weapons, and Private Military Contractors*, in Land, M., Aronson, J., (Eds.), New Technologies for Human Rights Law and Practice, Cambridge: Cambridge University Press, 2018.

DMA: significant additions made it into the final text – EURACTIV.com.

International Law Commission, *Draft articles on Responsibility of States for Internationally Wrongful Acts, with commentaries*, Yearbook of the International Law Commission, 2001, Vol. II. Part. 2.

Dinstein, Y., *Cyber war and international law: Concluding remarks at the 2012 Naval War College International Law Conference*, International Law Studies, no. 89/2013.

Димитријевић, В. и др., *Основи међународног јавног права*, Београд, 2012.

Дакић, Д., *Сајбер напади и међународно јавно право*, Зборник радова: Отворена питања међународног кривичног права и реформа кривичног законодавства Републике Србије, Златибор, 2022. (у штампи).

Директива 95/46/ЕЦ (Општа уредба о заштити података).

Identification and assessment of existing and (europa.eu).

Kelly, J. M., *Prosecuting Corporations for Genocide*, Oxford Scholarship Online, 2016.

Крећа, М., *Међународно јавно право*, Београд, 2020.

Luttikhuis, B., Moses, A. D., (2012), *Mass violence and the end of the Dutch colonial empire in Indonesia*, Journal of Genocide Research,, no. 14:3-4/2012.

Lustig, D., *The Nature of the Nazi State and the Responsibility of Corporate Officials at Nuremberg*, at Lustig, D., Veiled Power: International Law and the Private Corporation 1886-1981, Oxford University Press, 2020.

Предлог Уредбе Европског парламента и Савета о утврђивању усаглашених правила о вештачкој интелигенцији (Закон о вештачкој интелигенцији) и изменама појединих законских аката синдиката, ЦОМ (20 21) 206 финал, Брисел, 21.4.2021.

Regulation (EU) 2017/745, Annex VIII Article 3.3

Regulations on Medical Devices (Regulation (EU) 2017/745) and on In-Vitro Diagnostic Devices (Regulation (EU) 2017/746).

Roscini, M., *Cyber operations as a use of force at International Law and Cyberspace*, (Research Handbook, eds. Tsagourias and Buchan), Edward Elgar Publishing Limited, 2021.

Savin, A., *EU Internet Law*, Edward Elgar Publishing, 2020.

Shaw, M., *International Law* (9th ed.). Cambridge: Cambridge University Press, 2021.

Texts adopted - Digital Services Act and fundamental rights issues posed - Tuesday, 20 October 2020 (europa.eu)

The UN Human Rights Council established a Working Group on on the issue of human rights and transnational corporations and other business enterprises in 2011, A/HRC/17/4. www.ohchr.org/EN/Issues/Business/Pages/WGHRandtransnationalcorporationsandotherbusiness.aspx

Treaty bodies Download (ohchr.org)

The European Parliament Resolution with recommendations to the Commission on a civil liability regime for artificial intelligence (2020/2014(INL) Procedure File: 2020/2014(INL) | Legislative Observatory | European Parliament (europa.eu) (Resolution on liability)

UN Doc A/66/152/Add.1, 16 September 2011.

UNHCR, The Corporate Responsibility to Protect Human Rights: An Interpretive Guide, New York, 2012.

United States of America v. Iran, Judgment of 24 May 1980, ICJ Reports 1980.

C-203/99 Veedfald, and C-495/10, Dutrueux

Committee on Legal Affairs of the European Parliament, DRAFT REPORT http://www.europarl.europa.eu/sides/getDoc.do?pubRef=//EP//NONSGML%2BCOMPARL%2BPE-582.443%2B01%2BDOC%2BPDF%2BV0//EN

Corfu Channel Case, Judgment of 4 April 1949, ICJ Reports 1949.

Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products. Directive 1999/34/EC extended the scope of liability to agricultural and fishery products).