*Анђелија Стевановић**

DOI: 10.51204/Zbornik_UMKP_24167A
Оригинални научни рад

САЈБЕР РАТОВАЊЕ – НОВИ ВИДОВИ СУКОБА У МЕЂУНАРОДНОМ ПРАВУ[1]

Апстракт: Иако је рат као такав забрањен Повељом Уједињених нација, сведоци смо да и даље долази до оружаних сукоба. Развојем технологије долази до појаве нових видова сукоба, који до пре пар деценија нису могли ни да се замисле. У овом раду се приказује сајбер ратовање као нови начин ратовања у међународном праву, као и каква је могућност примене постојећих правила међународног хуманитарног права на ове, нове видове сукоба између држава унутар самих оружаних сукоба. Упоређује се сајбер ратовање са класичним оружаним сукобима и и поставља се питање да ли је време за измену постојећих или доношење нових правила. Анализира се појам сајбер напада и шта чини радњу извршења. Затим, на крају се врши анализа Конвенције о високотехнолошком криминалу, која је донета под окриљем Савета Европе 2001. године, као и њених Протокола и Талинског приручника, који се односи на сајбер ратовање и коначно, анализа случајева из праксе, како би се извео закључак да ли је међународно право на добром путу ка регулисању, а самим тим и надајмо се, спречавању, ових сукоба.

Кључне речи: сајбер ратови, оружани сукоби, међународно хуманитарно право, Конвенција о високотехнолошком криминалу, Талински приручник.

1. УВОД

Појавом нових технологија неки сегменти живота јесу олакшани, међутим, нова открића и нове технологије се некада могу и злоупотребити. Као

* Истраживачица приправница у Институту друштвених наука у Београду, ORCID: 0009-0002-3157-515X, andjelija.stevanovic21@gmail.com.

1 Рад је написан у оквиру Програма истраживања Института друштвених наука за 2024. годину који подржава Министарство науке, технолошког развоја и иновација Републике Србије.

што је давних дана Алфред Нобел свој изум – динамит наменио за потребе рударства, друштво је тај изум почело да користи (односно злоупотребљава), због своје разорне моћи, и приликом ратовања. Данас можемо рећи да имамо сличну ситуацију, са појавом компјутерских система и интернета, појавили су се и нови начини да се ти системи искористе у сврхе којима не би требало да служе. Иако су предности интернета толике да се не могу упоредити са било којим другим „изумом" до сада, јавиле су се и одређене лоше стране тоталног умрежавања система, људи и држава. Управо због тога имамо једну парадоксалну ситауцију: савремене технологије стварају нове могућности, које једнако користе и извршиоци кривичних дела и агенције за спровођење закона, само у супротстављеним интересима.[2] Поред класичних оружаних сукоба, у модерно време јављају такозвани сајбер сукоби. Иако се сајбер напади разликују од класичних ратова у простом смислу што се не одигравају у стварности – на ратишту, између војника две државе, последице могу бити приближно исте. Из тих разлога неопходно је анализирати да ли се постојећа правила међународног хуманитарног права могу применити и на ове нове врсте сукоба.

Са друге стране правила међународног хуманитарног права настала су и примењивала су се на типичне оружане сукобе и тешко могу бити примењива на нове облике угрожавања безбедности држава. Ипак не би било исправно тврдити да су правила међународног хуманитарног права неприменљива на сајбер сукобе, а поготово се то може рећи за основна начела ове дисциплине.[3] Иако садашња правила међународног хуманитарног права не помињу посебно сајбер ратовање, Мартенсова клаузула, повезана са прихваћеним принципима међуанродног хуманитарног права, каже да кад год стање ствари није покривено глобалним споразума, „цивили и борци остају испод заштите и ауторитета принципа јуриспруденција која произилази из устаљеног обичаја, из принципа хуманости и из диктата јавна савест.[4]

Стога, можемо претпоставити да је сајбер простор може бити посматран на истоветан начин као и реалан простор у коме се одигравају оружани сукоби. Сваки облик ратовања мора бити подложан достигнутим цивилизацијским нормама савременог људског друштва. Те норме су утврђене заједнички дефинисаним и прихваћеним међународним правним актима, попут Повеље УН и оних који сачињавају међународно право оружаних сукоба.[5]

2 М. Шикман, „Трансформативне технологије и криминал (облици испољавања и мере сузбијања)", *Трансформативне технологије: Правни и етички изазови 21. век Зборник радова,* (ур. Игор Милинковић), Правни факултет Универзитета у Бањој Луци, Бања Лука, 2020, 234.

3 Б. Милисављевић, *Међународно хуманитарно право,* Правни факултет Универзитета у Београду, Београд, 2024, 205.

4 R. Bokil, „Cyber Warfare: Taking War to Cyberspace and its Implications for International Humanitarian Law", *International Journal for Multidisciplinary Research,* 1/2023, 3.

5 Д. Младеновић, М. Дракулић, Д. Јовановић, „Међународно право и сајбер ратовање", *Војно дело,* 1/2021, 10.

Имајући у виду да су ова правила већ дуго установљена у међународном праву и имају своју примену потребно је анализирати која правила међународног хуманитарног права познајемо, да ли су та правила примењива на сајбер нападе, и која су то правила која се посебно односе на сајбер ратовање и сајбер нападе.

2. ПРАВИЛА МЕЂУНАРОДНОГ ХУМАНИТАРНОГ ПРАВА

Међународно хуманитарно право је скуп правила која, са једне стране, представљају оптимално регулисање захтева ратног циља и начела, и с друге стране, начела и принципе хуманости.[6] Правила међународног хуманитарног права су једна од најстаријих правила која су настала у међународном праву. Ако се жели пратити развој хуманитарног права од појаве првих његових обичајних правила и установа, онда је оно веома старо по свом постанку, те се његово порекло протеже на неколико миленијума пре нове ере. У сваком случају модерно међународно хуманитарно право настало је средином деветнаестог века, али његово корене треба тражити у далекој прошлости.[7]

С обзиром на порекло међународног хуманитарног права и развој, можемо слободно закључити да има широку примену данас, као и да прати развој и потребе друштва. Поред обичајних правила међународног хуманитарног права, најважнији међународни уговори који служе као извори међународног хуманитарног права јесу: Хашке конвенције из 1907. године[8], затим четири Женевске конвенције из 1949. године[9] донете након забрињавајућих

6 В. Јончић, *Међународно хуманитарно право,* Правни факултет Универзитета у Београду, Београд, 2015, 19.

7 З. Радивојевић, „Порекло међународног хуманитарног права", *Зборник радова Правног факултета у Нишу*, 58/2011, 87.

8 Конвенција о законима и обичајима рата на копну (IV Хашка конвенција од 1907. године), Конвенција о правима и дужностима неутралних сила и лица у случају рата на копну (V Хашка конвенција од 1907. године), Конвенција о статусу непријатељских трговачких бродова у почетку непријатељства (VI Хашка конвенција од 1907. године), Конвенција о претварању трговачких бродова у ратне бродове (VII Хашка конвенција од 1907. године), Хашка конвенција од 18. октобра 1907. године о постављању аутоматских подморских контактних мина (VIII Хашка конвенција од 1907. године), Конвенција о бомбардовању од стране поморских снага у време рата (IX Хашка конвенција од 1907. године), Конвенција о одређеним ограничењима вршења права узапћења у поморском рату (XI Хашка конвенција од 1907. године), Конвенција о правима и дужностима неутралних држава у рату на мору (XIII Хашка конвенција од 1907. године).

9 Женевска конвенција за побољшање положаја рањеника и болесника у оружаним снагама у рату, од 12. августа 1949. године (I Женевска конвенција), Женевска конвенција за побољшање положаја ратника, болесника и бродоломника оружаних снага на мору, од 12. августа 1949. године (II Женевска конвенција), Женевска

дешавања у току Другог светског рата, ради унапређења заштите одређених лица и два Допунска протокола од 1977. године.[10] Норме међународног хуманитарног права нису само пуки обичаји и правила, већ су то норме чије поштовање представља понашање у складу са правним и моралним начелима и чије кршење представља међународни злочин.[11]

Женевске конвенције предвиђају да ће се одредбе које садрже примењивати у случајевима објављеног рата или сваког другог оружаног сукоба који избије између двеју или више Високих страна уговорника, чак и ако једна од њих није признала ратно стање, затим у свим случајевима окупације целе територије једне Високе стране уговорнице или њеног дела, чак и ако та окупација не наиђе ни на какав војни отпор.[12] Поред тога предвиђају да ако једна од Сила у сукобу није учесник у овој Конвенцији, Силе учеснице у Конвенцији ипак ће остати везане њоме у својим међусобним односима. Оне ће поред тога бити везане Конвенцијом према тој Сили, ако та Сила прихвата и примењује њене одредбе.[13] Можемо одмах приметити да се наводи да ће бити применљиве у случајевима „објављеног рата или сваког другог *оружаног* (курзив ауторке) сукоба". Ову реченицу можемо схватити са једне стране на начин да се ратом сматра само сукоб који се одиграва употребом оружја, међутим треба имати у виду да у периоду у коме су писане Женевске конвенције интернет није постојао, а самим тим ни идеја да се напади могу спровести посредством истог. Стога можемо да закључимо да уколико једна држава нападне другу путем сајбер напада (у време трајања оружаног сукоба), такав напад можемо окарактерисати као сајбер једне државе на другу и признати правила Женевских конвенција и у том сукобу. Поред тога, наглашено је да су правила Женевских конвенција обичајне природе и да се односе и обавезујуће су за све државе, а не само за државе које су их потписале и ратификовале – што је значајно за могућност примене ових правила на сајбер сукобе, јер посебна правила о сајбер ратовању до данашњих дана нису развијена у мери у којој су остала правила међународног хуманитарног права.

Поред правила међународног хуманитарног права, треба поменути и да је у оквиру Савета Европе 2001. године усвојена Конвенција о високотехнолошком криминалу (у даљем тексту: Конвенција) као и допунски

конвенција о поступању са ратним заробљеницима од 12. августа 1949. године (III Женевска конвенција), Женевска конвенција о заштити грађанских лица за време рата од 12. августа 1949. године.

10 Допунски протокол уз Женевске конвенције од 12. августа 1949. године о заштити жртава међународних оружаних сукоба (Протокол I), Допунски протокол уз Женевске конвенције 8. јуна 1977. године који се односи на заштиту жртава у оружаним сукобима који немају међународни карактер (Протокол II).

11 В. Јончић, *op.cit.,* 270.

12 М. Старчевић, *Извори међународног хуманитарног права – Приручник за професионалне војнике, правнике и активисте Црвеног крста,* Међународни Комитет Црвеног Крста, Београд, 2002, 1.

13 *Ibidem.*

протоколи на њу нешто касније. Она обухвата и случајеве изазване сајбер нападима према државама чланицама, али и према лицима која су на њиховој територији.[14] Што нам говори да су сајбер напади препознати као важан сегмент у међународном праву и да постоји иницијатива за регулисање. Поред Конвенције, важан документ који се односи на сајбер ратовање јесте Талински приручник, који доноси нешто шири дијапазон правила о сајбер ратовима. На пример, овај приручник предвиђа да су правила међународног хуманитарног права потпуно применљива на сајбер сукобе.[15] Међутим, проблематика код овог приручника се састоји управо у његовој правној природи – то је приручник, а не правнообавезујућа међународна конвенција, стога још увек у том смислу не може директно бити извор права.

На крају, али не и најмање важно, треба се осврнути на Саветодавно мишљење Међународног суда правде о нуклеарном оружју, које подсећа да се међународно хуманитарно право односи на све облике ратовања и на све врсте оружја, оно из прошлости, оно из садашњости и оно из будућности.[16] Из наведеног видимо да међународно хуманитарно право може бити подобно за примену на нове врсте сукоба, а сајбер нападе можемо окарактерисати као „облик ратовања из будућности", у контексту цитираног мишљења Међународног суда правде, те закључујемо да се правила међународног хуманирарног права могу применити и на сајбер нападе и сајбер ратове.

3. ПОЈАМ САЈБЕР НАПАДА И САЈБЕР РАТОВА

Више него икада за коначан успех у рату скоро подједнаку важност као победа на бојном пољу имају одређени облици ратовања, који сами по себи не значе примену оружане силе. Неки међу њима настали су у наше време, упоредо са технолошким и научним напретком.[17] Управо такав облик ратовања је и сајбер ратовање – путем сајбер напада. Како бисмо могли наставити анализу ових појава потребно је дефинисати појам сајбер напада и сајбер ратовања. Професор Милисављевић наводи да је сајбер ратовање „врста непријатељске активности предузета против рачунарских мрежа, рачунарских система и база података са циљем деградирања или уништавања циљаних система".[18] Значајно је да се само сајбер напади на циљеве који непосредно или посредно зависе од сајбер простора могу сврстати у подручје сајбер ратовања. Напади конвенционалном силом на сајбер инфраструктуру облик су традиционалног ратовања које оставља последице на

14 Б. Милисављевић, *op. cit.,* 208.

15 M. Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge University Press, Cambridge, 2017, 182.

16 Међународни суд правде, Саветодавно мишљење о нуклеарном оружју, пара. 82.

17 Б. Кривокапић, „Појам рата и савремени ратови", *FBIM Transactions,* 2/2020, 88.

18 Б. Милисављевић, *op. cit.,* 206.

сајбер инфраструктуру и не сврставају се у сајбер ратовање.[19] Што нас наводи на закључак да је за постојање сајбер напада неопходно „напасти" државу и нанети јој штету у сајбер простору. Међународни комитет Црвеног крста дефинише сајбер ратовање на следећи начин: сајбер ратовање јесу средства и методе ратовања која се састоје од сајбер операција које достижу степен, или су учињене у контексту оружаног сукоба у смислу међународног хуманитарног права.[20] Можемо дакле дефинисати сајбер ратове као сукобе у сајбер простору који имају улогу оружаних напада у реалном простору и који могу да нанесу одређену штету нападнутој страни за време трајања оружаних сукоба и на које се може применити међународно хуманитарно право. То значи да би свака сајбер операција спроведена током оружаног сукоба могла бити се третирана као сајбер рат.[21]

Са војног аспекта сајбер напади су постали моћна, нискобуџетна опција ратовања која материјално оштећује друге једноставним кликом на дугме. Сајбер напад служи као асиметрично оружје које омогућава инфериорним групама и државама да наносе штету технолошки и војно супериорним непријатељима. У комбинацији са герилско-терористичким начином ратовања вероватно ће бити основни вид „асиметричног" супротстављања мањих и слабијих, војнички јачима у класичном смислу.[22]

За установљавање примене међународног хуманитарног права на сајбер нападе неопходно је да буду предузети у време оружаних сукоба, да нанесу одређену штету држави и да је могуће установити одговорност државе у смислу међународног права. Такве операције могу се састојати од напада на рачунарску мрежу („операције за ометање, порицање, деградирање, или уништавање информација које се налазе у рачунарима и рачунарским мрежама, или самих рачунара и мрежа") или експлоатација рачунарске мреже („могућност добијања приступа информацијама које се налазе на информационим системима и могућност коришћења самог система") без утицаја на функционалност приступаном систему.[23] Ове карактеристике хибридних ратова претпостављају да се налазе у „сивој зони" од међународног права[24] имајући у виду да није лако утврдити ко је предузео сајбер напад и тешко је приписати одређени напад одређеној држави.

19 Д. Младеновић, М. Дракулић, Д. Јовановић, *op. cit.,* 15.

20 ICRC, What limits does the law of war impose on cyber attacks? https://www.icrc.org/en/doc/resources/documents/faq/130628-cyber-warfare-q-and-a-eng.htm (приступљено 18.3.2024. године).

21 R. Bokil, *op. cit.*, 2.

22 З. Јефтић, *et al*., „Савремени конфликти и њихове тенденције" *Војно дело* 7/2018, 37.

23 M. Sassoli, *International Humanitarian Law: Rules, Solutions to Problems Arising in Warfare and Controversies (*Principles of International Law series), Edward Elgar Pub, 2019, 533.

24 N. Mazaraki, Y. Goncharova, „Cyber dimension of hybrid wars: Escaping a „grey zone" of international law to adress econimic damages", *Baltic Journal of Economic studies,* 8/2022, 117.

Да би се прихватило међународно право у сајбер простору, мора се знати идентнтитет лица која су одговорна за чињење назаконите радње – било да је држава у питању, било да се ради о субјекту под покровитељством државе, или се ради о приватном лицу, које спроводи активности у сајбер простору ван оквира међународног права.[25] Кључна карактеристика сајбер напада је јединствена потешкоћа у откривању њихових покретача (и учиниоца), што произилази из могућности програмирања сајбер-багова тако да не само замагљују трагове, већ и воде до погрешних извора.[26] Што подразумева потешкоће, јер се не може прецизно утврдити ко стоји иза сајбер напада – за разлику од класичних оружаних сукоба где једна држава шаље своје трупе како би се сукобиле на ратишту са снагама друге државе. Некада је могуће и да појединац стоји иза одређеног сајбер напада – хакер, који може да изазове штету истог интензитета као и војни оружани напад државе, те се може јавити и проблем приписивости таквих аката одређеној држави - да ли је таква особа радила за државу или по сопсвеном нахођењу и на који начин доказати једно или друго, што може даље да закомпликује утрвђивање одговорности државе за сајбер нападе. Ово је карактеристика сајбер ратова која прави битну разлику између класичних оружаних сукоба и сајбер ратова. Некада сајбер напад може да предузме само једна особа или група особа, као што смо поменули, док код класичних оружаних сукоба то није могуће.

Коначно, следи приказ најчешћих примера сајбер напада, и то су: шпијунажа, фишинг (phishing)[27], ботнет[28], сајбер напади на електричне мреже градова или читавих регија (electrical power grid), ДоС напади (denial of service)[29] , пропаганда, економска дисрупција...[30] Ови примери показују нам да сајбер напади могу да изазову последице по државу у којој се изводе, сличног интензитета као и оружани сукоби, као и да је тешко утврдити ко је учинилац, и у наредном делу приказаћемо неку праксу сајбер напада, као и инструменте којима се ближе регулише ова материја.

---

25 Ј. Гордниђ, „Сајбер напади са аспекта међународног и унутрашњег права", *Баштина,* 57/2022, 278.

26 M. Szyłkowska, „Attributes of cyber conflict in the context of armed conflict – an outline of the problem", *Defence science review*, 11/2021, 139.

27 Фишинг представља покушај крађе података корисника интернета путем фалсификоване веб странице. Обично се таква лажна страница нуди путем посебно припремљене е-поруке или ћаскања

28 Ботнет је неколико уређаја повезаних на Интернет, од којих сваки покреће један или више ботова. Ботнети се могу користити за обављање дистрибуираног напада ускраћивањем сервиса, крађу података, слање нежељене поште, и омогућава нападачу приступ уређају и његовој вези.

29 ДоС напад је опструкција приступу важних веб страница које користе грађани, војска, научници и други, тако да оптерећује страницу великим бројем захтева који су лажно створени како корисници не би могли да је користе.

30 Cyber ratovanje - potpuno novi oblik ratovanja, *https://duplico.io/cyber-ratovanje-potpuno-novi-oblik-ratovanja/*, приступљено 30.03.2024. године.

4. РЕГУЛИСАЊЕ САЈБЕР НАПАДА И ЊИХОВА МАТЕРИЈАЛИЗАЦИЈА У ПРАКСИ

Претходном анализом установили смо да је став међународне заједнице да се правила међународног хуманитарног права примењују на све видове сукоба, па и на нове видове као што су то сајбер сукоби. Штавише, члан 36. Допунског протокола I уз Женевске конвенције из 1949. године захтева од страна да, „у проучавању, развоју, набавци или усвајању новог оружја, средства или метода ратовања треба утврдити да ли би његова примена, у неким или свим околностима, била забрањено овим Протоколом или било којим другим правилом међународног (хуманитарног) права.[31] Чак и државе које нису чланице Протокола препознају потребу да се обезбеди да оружје, укључујући сајбер оружје, испуњава захтеве постојећих норми међународног хуманитарног права.[32] Нема разлога да се сајбер оружје не подведе под „ново оружје" и да се његова примена ограничи нормама постојећег међународног права.

Поред правила општег међународног и међународног хуманитарног права Талински приручник је најзначајнији документ који се бави регулисањем сајбер ратовања, међутим, Талински приручник нема правнообавезујућу снагу сам по себи јер није донет у форми међународног уговора – конвенције. Међутим, имајући у виду да се одређена правила која садржи односе на већ постојећа правила међународног обичајног права, може се рећи и да постоје делови који су правнообавезујући – јер се у смислу члана 38 Статута Међународног суда правде обичај сматра извором права.[33] Осим приручника, 2001. године је донета и Конвенција о високотехнолошком криминалу, која утврђује заједничке политике у борби против криминала ради заштите друштва од високотехнолошког криминала, усвајањем одговарајућег законодавства и унапређивањем међународне сарадње.[34] Конвенција предвиђа да државе које су је ратификовале треба да у своја законодавства уведу одређена кривична дела - као што су то дела против поверљивости, целовитости и доступности рачунарских података,[35] дела у вези са рачунарима,[36] као и облике одговорности и сакције.[37] Можемо приметити

31 Закон о ратификацији Допунског протокола уз Женевске конвенције од 12. августа 1949. године о заштити жртава међународних оружаних сукоба, „Сл. лист СФРЈ – *Међународни уговори"*, бр. 16/78), члан 36.

32 M. Schmitt, „Wired warfare 3.0: Protecting the civilian population during cyber operations", *International rewiev of the Red Cross,* 910/2019, 3.

33 Статут Међународног суда правде, члан 38.

34 Закон о потврђивању Конвенције о високотехнолошком криминалу, *Службени гласник Републике Србије,* бр 19.

35 *Ibid*. одељак 1.

36 *Ibid*. одељак 2.

37 *Ibid*. одељак 5.

да је година доношења ове Конвенције управо година када се догодио напад на Светски трговински центар у САД, те се почетак 21. века може слободно узети као условно речено прекретница у појави нових видова ратовања као што је тероризам и поред тога и сајбер напади, и њиховом порасту. Донета су и два Протокола на ову Конвенцију и то Додатни протокол уз Конвенцију о високотехнолошком криминалу који се односи на инкриминацију дела расистичке и ксенофобичне природе извршених преко рачунарских система[38] коме само име казује садржину. Поред Првог, донет је и Други додатни протокол уз Конвенцију о високотехнолошком криминалу о појачаној сарадњи и откривању електронских доказа[39], за који је Република Србија била прва држава која је предала инструмент о ратификацији. Други Протокол се бави појачаном и ефикасном сарадњом између држава , као и сарадњом у ванредним ситуацијама и непосредном сарадњом између надлежних органа и пружалаца услуга и других субјеката који поседују или контролишу релевантне информације.[40] Остаје нам да у наредном периоду будемо сведоци да ли ће се Конвенције и Протоколи примењивати и на који начин.

Са друге стране, Талински приручник се бави испитивањем да ли се постојеће норме могу применити на сајбер ратовање. Након увода следи главни садржај Приручника, који се дели на два дела, и то део 1 који разматра питања међународног права сајбер сигурности и део 2 који разматра питања права сајбер сукоба, као оружаних сукоба. Ти делови су подељени на поглавља и одељке, сваки одељак садржи правила, чији укупан број износи 95.[41] Талински приручник, међутим, не даје препоруке о томе како би закон требало појаснити или даље развијати.[42]

За даљи развој и појашњење требало би се осврнути и на досадашњу праксу сајбер напада, да би се утврдиле слабости и могућности за промене, као и евентуалне правне празнине које захтевају регулисање. Први најпознатији случај сајбер напада је такозвани Стакснет црв. Стакснет је компјутерски црв, односно вирус са могућношћу да се копира и брзо путује између рачунара. Направљен је да тихо преузме индустријске системе контроле и разбије крхке, застареле ИР-1 центрифуге које се окрећу у Натанзу, иранском постројењу за обогаћивање уранијума, који је почео да се руши неуобичајено

38 Закон о потврђивању додатног Протокола уз Конвенцију о високотехнолошком криминалу који се односи на инкриминацију дела расистичке и ксенофобичне природе извршених преко рачунарских система, *Службени гласник Републике Србије,* бр. 19.

39 Закон о потврђивању Другог додатног протокола уз Конвенцију о високотехнолошком криминалу о појачаној сарадњи и откривању електронских доказа, *Службени гласник Републике Србије,* 7/2022-18.

40 *Ibid*. преамбула.

41 R. Prpić, „Osvrt na Tallinnski priručnik o međunarodnom pravu primjenjivom na kibernetičko ratovanje", *Zagrebačka pravna revija,* 1/2017, 44–45.

42 M. Sassoli, *op. cit.,* 534.

високим стопама.[43] Стакснет није био ограничен на самостално умножавање, већ је имао и наоружани терет који је могао да даје наређења другим програмима и представља „прву познату употребу малициозног софтвера направљеног да изазове материјалну штету нападајући национално критичну инфраструктуру.[44] САД и Израел су спровели ову операцију из разлога што је Иран у тим периоду развијао нуклеарно оружје, те су сматрали да имају основа за оваквим видом напада, у складу са Повељом Уједињених Нација и правом на самоодбрану. Али, када је Стакснет покренут, Иран је још увек био у првој фази развоја оружја. Ово показује да су САД и Израел направили превентивни (а самим тим и незаконити) напад на Иран, пре него што је Иран имао довољно шансе да уопште припреми непосредан напад.[45] Што са друге стране може подразумевати агресију од стране САД-а и Израела, уколико би се сајбер напад третирао као вид испољавања агресије. Дакле, проблематичност овог напада је то што није изведен као напад у време оружаног сукоба, нити је био део оружаног сукоба у смислу међународног хуманитарног права, па се на овај случај нису могла применити правила међународног хуманитарног права. Овај случај био је вид зачетка сајбер ратовања – доказано је да без иједне жртве на бојном пољу државе могу да нанесу велике материјалне штете другим државама, иако неки аутори сматрају да овај напад нема „ратни" карактер.[46] Али, овај случај није дошао до било какве судске инстанце, те не можемо анализирати примену правила на сајбер сукобе, већ само, условно речено, став међународно заједнице о овом питању и држање до одређених принципа приликом напада.

Поред Стакснета, најпознатији случајеви сајбер напада су сајбер напади које је Руска Федерација спроводила над Украјином. У почетку су то биле интернет преваре – фишинг, којима су руске обавештајне службе прикупљале информације и имале су утицаје на дигиталну инфраструктуру. Ово се променило у децембру 2015. године, када је први пут јавно објављено да су сајбер напади на енергетски сектор узроковали нестанак струје. Такође, сајбер напади који су нанели штете Украјини спроведени су и у 2016. години и то погађајући украјинску важну инфраструктуру (енергетски сектор – кијевску електрану, кијевски аеродром, као и финансијски сектор укључујући трезор и пензијске фондове).[47]

---

43 A. Van Dine, „After Stuxnet: Acknowledging the Cyber Threat to Nuclear Facilities", *Project on Nuclear Issues: A Collection of Papers from the 2016 Nuclear Scholars Initiative and PONI Conference Series,* (Eds. M. Cancian), Center for Strategic and International Studies (CSIS), Lanham, 2017, 102.

44 M. Roscini, *Cyber Operations and the Use of Force in International Law*, Oxford University Press, Oxford, 2014, 6.

45 W. Rubin, "Waging Wars in Cyberspace: How International Law On Aggression And Self-Defense Falls Short Of Addressing Cyber Warfare. Could Iran Legally Retaliate For The Stuxnet Attack?", *Honor papers,* 1/2016, 41.

46 J. Jansons, „Was Stuxnet an act of war?", *Security Forum,* 1/2017, 116.

47 P. Pernik, et al. "The Early Days of Cyberattacks: The Cases of Estonia, Georgia and Ukraine." (Eds Nicu Popescu and Stanislav Secrieru), *Hacks, leaks and disruptions:*

У вези са сајбер нападим Русије на Украјину тужилац Међународног кривичног суда Карим Кан је указао на могућност сајбер напада да представљају ратне злочине, злочине против човечности, геноцид и злочин агресије. Упркос томе што се сајбер злочини не помињу посебно у Римском статуту, „такво понашање потенцијално може испунити елементе многих кључних међународних злочина како су већ дефинисани".[48] Овде наилазимо на занимљиво тумачење сајбер напада – у смислу међународних кривичних дела. Уколико би се у будућности сајбер напади квалификовали као рецимо биће међународног кривичног дела – појединци који стоје иза ових напада би могли да одговарају пред Међународним кривичним судом. Из ове изјаве тужиоца можемо да увидимо да су сајбер напади препознати у међународној заједници као опасност и да постоји потреба за њиховим детаљнијим регулисањем. Поред тога, имајући у виду да се прошле године десило забрињавајући сајбер напад на системе Међународног кривичног суда, што је упад у једну од најзначајнијих међународних институција, која рукује осетљивим информацијама у вези за међународним кривичним делима[49] јасна је забринутост међународне заједнице када су у питању сајбер напади и сајбер ратовање, те сматрамо да је неопходно да дође до одређених промена у регулативи.

5. ЗАКЉУЧНА РАЗМАТРАЊА

Као што је наведено, технолошки развој је са собом донео предности, али и одређене мане. Једна од тих мана јесте управо употреба технологије у сврхе наношења штете државама. Сајбер ратовање као нови вид сукоба је доживело свој развој последњих деценија и поделило мишљења међународних правника у смислу да ли је међународно (хуманитарно) правно применљиво на ове сукобе. Из горенаведеног закључујемо да се на сајбер нападе предузете у моментима оружаних сукоба између две државе могу примењивати правила међународног права, а све то тумачећи правила Женевских конвенција, као и Саветодавног мишљења Међународног суда правде у случају Нуклеарног оружја. Сајбер напади и сајбер ратовање посматрају се као нови вид испољавања (неоружане) силе и могу се поставити „раме уз раме" са класичним оружаним сукобима.

Потребно је да међународна заједница утврди која правила су подобна да се примене на сајбер ратовање и да их потом у тим случајевима и примењује као и на класичне оружане сукобе. Са друге стране, сматрамо да је

Russian Cyber strategies, European Union Institute for Security Studies (EUISS), 2018. http://www.jstor.org/stable/resrep21140.9, 61.

48 Cyberattacks as war crimes, https://www.ibanet.org/Cyberattacks-as-war-crimes приступљено 9.4.2024. године.

49 War crimes tribunal ICC says it has been hacked, https://www.reuters.com/world/international-criminal-court-reports-cybersecurity-incident-2023-09-19/ приступљено 9.4.2024. године.

неопходно утврдити да ли постоје појаве у сајбер ратовању на које међународно хуманитарно право није применљиво и у складу са тим отпочети анализу на који начин је могуће регулисати те празнине. Такође, потребно је поставити питања шта уколико држава предузме сајбер напад према држави са којом није у оружаном сукобу. Да ли се такав акт може окарактерисати као акт агресије и отпочињања новог сукоба? Према дефиницији која је дата у Резолуцији број 3314 Генералне скупштине УН, агресијом се сматра „употреба оружане силе једне државе против суверенитета, територијалне целине или политичке независности друге државе, односно на било који други начин који није у сагласности са Повељом УН, како то проистиче из ове дефиниције".[50] Стога не можемо сајбер нападе подвести под акт агресије – по дефиницији, међутим треба узети у обзир да је поменута резолуција донета пре 50 година и да право треба да прати развој технологије и друштва као и могућности да се појаве нова оружја и видови ратовања какво је управо сајбер ратовање. Самим тим, због штете коју сајбер сукоби могу да нанесу државама, можемо да закључимо да би у будућности могло да дође до промена у начину сагледавања аката агресије и отпочињања сукоба између двеју или више држава. Самим тим и увести могућност одговарања пред Међународним кривичним судом особа које изврше или наређе сајбер нападе. Поред тога, потребно је утврдити механизме идентификације учинилаца сајбер напада и самим тим обезбедити лакшу примену међународног права и у смислу правила о приписивости, у смислу приписивости аката држави, али и утврђивање појединачне кривичне одговорности. Када би се обезбедила примена правила, али и сакционисање учињених дела, те би се и на неки начин утицало на предузимање сајбер напада.

Став међународне заједнице је јасан и види се да постоји потреба за континуираним радом на решавању проблема сајбер напада. Можемо приметити да је и на пољу унутрашњег права дошло до новина – као што је то у Србији на пример - у Вишем јавном тужилаштву у Београду образовано је посебно одељење за борбу против високотехнолошког криминала тј. Посебно тужилаштво, који пресуђује у стварима које се тичу кривичних дела против безбедности рачунарских података одређена Кривичним закоником, кривичних дела против интелектуалне својине, имовине, привреде и правног саобраћаја, код којих се као објекат или средство извршења кривичних дела јављају рачунари, рачунарски системи, рачунарске мреже и рачунарски подаци, кривична дела против слобода и права човека и грађанина, полне слободе, јавног реда и мира и уставног уређења и безбедности Републике Србије, која се због начина извршења или употребљених средстава могу сматрати кривичним делима високотехнолошког криминала, у складу са чланом 2. став 1. овог закона.[51] Самим тим, увиђа се да је проблем

50 М. Симовић, Д. Симовић, „Агресија у међународном кривичном праву", *Годишњак факултета Правних и друштвених наука*, 3/2013, 173.

51 Портал правосуђа Србије, https://portal.sud.rs/cr/javna-tuzilastva/javna-tuzilastva-posebne-nadleznosti; приступљено 9.4.2024. године.

сајбер напада и сајбер ратовања препознат и да су предузети одређени кораци у регулисању овог новог проблема, али постоји још пуно простора за развијање ове регулативе.

ЛИТЕРАТУРА

Bokil, M., „Cyber Warfare: Taking War to Cyberspace and its Implications for International Humanitarian Law", *International Journal for Multidisciplinary Research,* 1/2023.

Van Dine, A., „After Stuxnet: Acknowledging the Cyber Threat to Nuclear Facilities", *Project on Nuclear Issues: A Collection of Papers from the 2016 Nuclear Scholars Initiative and PONI Conference Series,* (Eds. M. Cancian), Center for Strategic and International Studies (CSIS), Lanham, 2017.

Городнић Ј., „Сајбер напади са аспекта међународног и унутрашњег права", *Баштина,* 57/2022.

ICRC, What limits does the law of war impose on cyber attacks? https://www.icrc.org/en/doc/resources/documents/faq/130628-cyber-warfare-q-and-a-eng.htm (приступљено 18.3.2024. године).

Jansons, J., „Was Stuxnet an act of war?", *Security Forum,* 2017/1.

Јефтић З., Мишев Г., Обрадовић Ж., Станојевић П., „Савремени конфликти и њихове тенденције" *Војно дело,* 7/2018.

Јончић В., *Међународно хуманитарно право,* Правни факултет Универзитета у Београду, Београд, 2015.

Кривокапић, Б., „Појам рата и савремени ратови", *FBIM Transactions,* 2/2020.

Mazaraki N., Goncharova Y., „Cyber dimension of hybrid wars: Escaping a „grey zone" of international law to adress econimic damages", *Baltic Journal of Economic studies,* 8/2022.

Младеновић Д., Дракулић М., Јовановић Д., „Међународно право и сајбер ратовање", Војно дело, 1/2021.

Милисављевић Б., *Међународно хуманитарно право,* Правни факултет Универзитета у Београду, Београд, 2024.

P. Pernik, et al. "The Early Days of Cyberattacks: The Cases of Estonia, Georgia and Ukraine." (Eds Nicu Popescu and Stanislav Secrieru), *Hacks, leaks and disruptions: Russian Cyber strategies,* European Union Institute for Security Studies (EUISS), 2018

Prpić, R., „Osvrt na Tallinnski priručnik o međunarodnom pravu primjenjivom na kibernetičko ratovanje", *Zagrebačka pravna revija,* 1/2017.

Roscini, M., Cyber Operations and the Use of Force in International Law, Oxford University Press, Oxford, 2014.

Радивојевић З., „Порекло међународног хуманитарног права", Зборник радова Правног факултета у Нишу, 58/2011.

Rubin W., "Waging Wars in Cyberspace: How International Law On Aggression And Self-Defense Falls Short Of Addressing Cyber Warfare. Could Iran Legally Retaliate For The Stuxnet Attack?", *Honor papers,* 1/2016

Sassoli M., *International Humanitarian Law: Rules, Solutions to Problems Arising in Warfare and Controversies (*Principles of International Law series), Edward Elgar Pub, 2019.
Schmitt M., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge University Press, Cambridge, 2017.
Schmitt, M., „Wired warfare 3.0: Protecting the civilian population during cyber operations", *International rewiev of the Red Cross,* 910/2019.
Симовић, М., Симовић Д., „Агресија у међународном кривичном праву", *Годишњак факултета Правних и друштвених наука*, 3/2013.
Старчевић М., *Извори међународног хуманитарног права – Приручник за професионалне војнике, правнике и активисте Црвеног крста,* Међународни Комитет Црвеног Крста, Београд, 2002.
Szyłkowska M., „Attributes of cyber conflict in the context of armed conflict – an outline of the problem", *Defence science review*, 11/2021.
Шикман М., „Трансформативне технологије и криминал (облици испољавања и мере сузбијања)", *Трансформативне технологије: Правни и етички изазови 21. век Зборник радова,* (ур. Игор Милинковић), Правни факултет Универзитета у Бањој Луци, Бања Лука, 2020.

ПРАВНИ ИЗВОРИ

Закон о потврђивању Конвенције о високотехнолошком криминалу, *Службени гласник Републике Србије,* бр 19.
Закон о ратификацији Допунског протокола уз Женевске конвенције од 12. августа 1949. године о заштити жртава међународних оружаних сукоба, „Сл. лист СФРЈ – *Међународни уговори",* бр. 16/78)
Закон о потврђивању додатног Протокола уз Конвенцију о високотехнолошком криминалу који се односи на инкриминацију дела расистичке и ксенофобичне природе извршених преко рачунарских система, *Службени гласник Републике Србије,* бр. 19.
Закон о потврђивању Другог додатног протокола уз Конвенцију о високотехнолошком криминалу о појачаној сарадњи и откривању електронских доказа, *Службени гласник Републике Србије,* 7/2022-18.
Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, I.C.J. Reports 1996.
Статут Међународног суда правде.

ИНТЕРНЕТ ИЗВОРИ

Портал правосуђа Србије, https://portal.sud.rs/cr/javna-tuzilastva/javna-tuzilastva-posebne-nadleznosti; приступљено 9.4.2024. године.
War crimes tribunal ICC says it has been hacked, https://www.reuters.com/world/international-criminal-court-reports-cybersecurity-incident-2023-09-19/ приступљено 9.4.2024. године.

Cyberattacks as war crimes, https://www.ibanet.org/Cyberattacks-as-war-crimes приступљено 9.4.2024. године.
Cyber ratovanje - potpuno novi oblik ratovanja, https://duplico.io/cyber-ratovanje-potpuno-novi-oblik-ratovanja/, приступљено 30.03.2024. године.

Anđelija Stevanović*

CYBER WARFARE – NEW TYPES OF CONFLICT IN INTERNATIONAL LAW[52]

Summary

Although war as such is prohibited by the Charter of the United Nations, we are witnessing that armed conflicts still occur. The development of technology leads to the appearance of new types of conflict, which could not even be imagined until a few decades ago. The paper presents cyberwarfare as a new way of manifesting aggression in international law, as well as the possibility of applying the existing rules of international humanitarian law to these new types of conflict between states. Is it time to change the existing or adopt new rules? The impact of cyber wars on international relations and on international humanitarian law itself is analyzed. It compares cyberwarfare with classic armed conflicts and discusses ways to prevent such attacks in the future. Then, at the end, an analysis is made of the Convention on High-tech Crime, which was adopted under the auspices of the Council of Europe in 2001, as well as its Protocols, in order to conclude whether international law is on the right track towards regulation, and therefore hopefully , preventing these conflicts.

Keywords: cyber wars, armed conflicts, Convention on high-tech crime, international humanitarian law, Tallin Manual.

* Doctoral student at the University of Belgrade – Faculty of Law, international law scientific field and research trainee at the Institute of Social Sciences in Belgrade, andjelija.stevanovic21@gmail.com.

52 The paper was written as part of the Research Program of the Institute of Social Sciences for 2024, which is supported by the Ministry of Science, Technological Development and Innovation of the Republic of Serbia.