УДК 343.3::004
341.311
DOI: https://doi.org/10.5937/bastina32-39362

Прегледни рад

*Јован М. ГОРДИЋ**
Универзитет у Нишу, Правни факултет Ниш

САЈБЕР НАПАДИ СА АСПЕКТА МЕЂУНАРОДНОГ И УНУТРАШЊЕГ ПРАВА

Апстракт: Крај двадесетог и почетак 21. века обележио је експоненцијални развој информационих технологија који се огледа у развоју технологија, унапређењу комуникације и осталих сфера друштвеног живота у виртуелном – сајбер простору. Међутим, паралелно са ширењем афирмативних могућности у свим сферама друштвеног живота, информационе технологије су по основном дијалектичким принципу јединства и борбе супротности, на коме се заснива развој цивилизације, омогућиле и развој нових, криминалних активности у виртуелном, компјутерском свету, које се једном синтагмом називају сајбер напади и које представљају материјалну форму криминала у виртуелној стварности који се терминолошки одређује као сајбер криминал. Хакерски напади или сајбер злочини представљају активности које се реализују у сајбер простору и које наносе штету корисницима сајбер простора и од којих, могу али и не морају, да имају користи лица која изводе сајбер напад. Имајући у виду да се ови напади реализују у виртуелном простору у коме је тешко одредити границе (приватне, јавне, државне, материјалне или интелектуалне), да их изводе појединци, групе или организације најчешће високо стручне за рад у сајбер простору, уз коришћење најсавременијих решења информационе технологије и бројну сајбер заштиту којом се избегава откривање или сврставање ових радњи у сајбер злочине, њихова јасна класификација као криминалних активности је значајно отежана посебно на међународном нивоу. Дефинисање и тачно теоријско одређивање према сајбер нападима, као радњи сајбер криминала како на међународном, тако и на унутрашњем нивоу је значајно отежано и због различитих начина борбе против ових радњи у државама широм света. Посебан проблем у стварању међународних правних оквира у борби против сајбер напада лежи и у чињеници да субјекти сајбер напада могу бити и саме државе, односно институције и организације које стоје иза њих. Све ово утиче на проблеме стварања јединственог правног оквира у униформној законској борби против сајбер злочина са становишта међународне заједнице. Имајући у виду наведено циљ овог рада је идентификација актуелних питања међународног и унутрашњег уређења ове области права који се односе на борбу против сајбер напада и мера које се користи у области заштите безбедности сајбер простора, идентификовања учиниоца кривичног дела и његовог процесуирања.

Кључне речи: међународно право, унутрашње право, кривично право, кривични процес, сајбер напад, сајбер безбедност, сајбер претња, осумњичени.

* Докторанд, gordicjovan@gmail.com

УВОД

Настанак и развој информационих технологија представља један од највећих достигнућа у историји човечанства, који се може поредити са проналаском точка или парне машине по значају са становишта филогенезе, односно квалитативног скока у развоју цивилизације и унапређењу живота људи. Наиме, развој информационих технологија не представља само развој компјутера, већ и развој нових технологија у области индустријске производње, развој производа на нивоу микро и нанотехнологија, који имају своју примену у свим сферама друштвеног зивота и који драматично утичу на развој свих привредних грана на којима се заснива развој целокупне цивилизације. Као последица свега овога долази до сталне експанзије развоја информационо – технолошког сектора, а бројне фирме се свакодневно утркују како би још више унапредиле софтверска и хардверска решења и на тај начин остариле огромне профите и заузеле кључна места на међународном тржишту. Имајући у виду да цивилизацијски развој има своје дијалектичке закономерности, које се пре свега заснивају на јединству и борби супротности и преласку квалитета у квантитет и обрнуто, са квалитативним развојем афирмативних решења у области информационе технологије, која унапређују живот и рад људи, паралелно се квалитативно развија и супротност, која треба да отежа коришћење средстава информационе технологије и учини их небезбедним за широке народне масе. Посебан облик деструктивних решења у области савремених информационих технологија представљају софтверска решења која омогућавају да се њиховом имплементацијом у широко доступна хардверска решења информационих технологија, кроз савремене производе које човек данас користи (рачунар, телефон, таблет) изврши сајбер напад где ће се кориснику начинити материјална или духовна штета, са или без персоналне користи, коју има извођач сајбер напада.

Савремени услови живота, постојање пандемије изазване вирусом КОВИД-19, бројни ратови (Петровић 2021а; Петровић 2021б), укључујући и рат у Украјини, настанак и експанзија развоја друштвених мрежа, могућност коришћења разноразних интернет претраживача од куће, могућност спровођења финасијских трансакција, коришћење дигиталних валута, као и складиштења у разноразним регистрима и меморијама и пренос поверљивих података и службених или пословних тајни и све то уз помоћ производа без којих је незамислив свакодневни живот сваког појединца, створили су савршене услове за сајбер криминалце који мање или више успешно пливају на таласима сајбер простора, односно виртуелног простора.

Имајући у виду наведено, као и чињеницу да су бројне добро организоване групе, појединци па чак и државе, увиделе значај сајбер простора и могућности наношења озбиљних материјалних и друштвених губитака супарничким странама, као и могућност прибављања енормних материјалних и других (политичких, војних, индустријских) користи, развој сајбер напада добија експоненцијални замах у XXI веку (Петровић 2021а; Петровић 2021б). Врло брзо, у цивилизацијском смислу се може чак рећи и тренутно, се од употребе разноразних софтерских вируса за напад појединих корисничких апликација у оквиру стандардних оперативних система уз помоћ којих су хакери могли да преузму и контролишу туђ рачунар да би украли, модификовали или уништили информацију, прешло на префињену сајбер криминалну

инфраструктуру техничко – софтверског типа помоћу које су хакерске методе почеле да добијају „префињеније“ и далеко деструктивније облике. Данас, проблем просперитета криминалне активности на рачунарским мрежама и хаковање рачунара више није проблем једне особе, компаније или државе. Коришћењем најсавременијих апликација може извршити сајбер напад на свако појединачно правно или приватно лице, на тај начин, да му се може нанети непоправљива лична или колективна штета. Случај „Викиликс“ је само један од низу који показује шта све може да уради један сајбер напад и како може да преузме енормну количину информација у сајбер простору, наносећи невероватну штету, не само појединцима, већ и међународним организацијама, мултинационалним компанијама и државама у целини.

Имајући у виду наведено, компјутерски напад или сајбер напад, данас са правом представља једну од највећих претњи на државном и међународном нивоу. У таквим условима појединци, организације, привредна и друга друштва, државе, предузимају мере за спречавање сајбер напада или умањење последица од тих напада (Петровић 2021в), а убрзано се развијају и институционални правни оквири за борбу против сајбер криминала. Ти оквири су специфични, зато што морају да регулишу област која није материјална, већ је виртуелна и припада потпуној новој димензији живота.

ПОЈМОВНО ОДРЕЂЕЊЕ САЈБЕР НАПАДА

Чињеница да развој технолошких решења у области информационе технологије представља основ четврте индустријске револуције коју прати до сада невиђена брзина цивилизацијског развоја, доводи до експанзије настанка нових стварних и виртуелних алата и појава које је потребно дефинисати како би се формирао јединствени теоријски фонд речи који би омогућио лакшу комуникацију међу људима у области коришћења, али и злоупотребе информационих технологија (Спалевић и сар. 2018). Управо нагла експанзија информационих технологија довела је до тога да се појаве нови термини и синтагме, које би људима до пре неколико деценија звучале потпуно бесмислено: сајбер простор, вискотехнолошки или сајбер криминал, сајбер безбедност, сајбер напад.

Имајући у виду специфичност апстрактне, виртуелне димензије простора и људског мишљења у којој се одвија рад и комуникација приликом употребе информационих технологија, најпре је неопходно појмовно се одредити према синтагми сајбер простора као нечему што није опипљиво и јасно димензионисано и ограничено људским чулима. Наиме, сајбер је основни појам који се односи на употребу и злупотребу информационе технологије. Сајбер представља све оно што се односи на развој и употребу рачунара, рачунарских мрежа, виртуелне рачунарске комуникације и организације и реализације рада помоћу хардверског и софтверског алата. Значи, све оно што се односи на развој, примену и пренос решења у области информационих технологија може се подвести под термин сајбер (Томић 2003). Што се тиче сајбер простора, он у суштини представља виртулени или конкретни простор у коме се одигравају сајбер активности. Без обзира на значај јасног појмовног одређења, не постоји прецизна дефиниција сајбер простора. Према Међународној унији за телекомуникације (ИТУ 2014), сајбер простор обухвата системе и сервисе повезане било директно или индиректно на интернет, телекомуникационе

системе или компјутерске мреже. Према Међународној организацији за стандардизацију (ИСО, ИСО/ИЕЦ 27032) сајбер простор представља комплексно окружење које произилази из интеракције људи, софтвера и сервиса на интернету и то посредством технолошких уређаја и мрежа са њима повезаним, а који не постоји у физичком појавном облику. Имајући у виду наведено, примењујући класичну, афирмативну дефиницију, сајбер простор се може дефинисати као виртуелно окружење у којем се примењују сва решења информационе технологије заједно са лицима која користе ова решења приликом спровођења дигиталних активности на интернету или компјутерским мрежама, са циљем виртелне комуникације или организације и извршења конкретне људске делатности.

На основу извршеног појмовног одређења сајбер простора може се закључити да се у њему, помоћу субјеката и објеката информационих технологија, спроводе активности које имају и апстрактни, али и конкретни смисао и сврху. Те активности могу бити и углавном и јесу афирмативне и корисне за појединце или друштво у целини, али могу имати и свој негативни карактер, односно могу наносити штету лицима која учествују у дигиталним активностима у сајбер простору. Ради организације и спровођења мера заштите дигиталне активности, са развојем и применом информационих технологија, настаје и успешно се развија и сајбер безбедност. Класичном афирмативном дефиницијом, сајбер безбедност можемо појмовно одредити као скуп организационих, техничких и оперативних мера људске делатности у сајбер простору, усмерених на заштиту сајбер инфраструктуре и материјалне и нематеријалне имовине појединца, група и заједница. На основу ове дефиниције, може се уочити да сајбер безбедност обухвата: мере заштите формиране на основу корисничких упутстава за употребу сајбер алата (организационе мере), мере заштите уграђене кроз сам производни процес дизајнирања хардверских, софтверских и дигиталних комуникацијских информационих решења (техничке мере) и мере заштите коју мора да спроводи сам корисник у току дигиталних активности како би унапредио сајбер безбедност (оперативне мере).

На основу појмовног одређења сајбер простора и сајбер безбедности и њиховог јаснијег мисаоног дефинисања, могу се утврдити и околности које доводе до злоупотребе сајбер простора и нарушавања сајбер безбедности. Чин нарушавања сајбер безбедности представља сајбер напад, а њиховим извођењем материјализује се смисао синтагме сајбер криминал. Постоје разни покушаји дефинисања сајбер криминала. У складу са прописима Министарства унутрашњих послова, сајбер криминал (који се назива и високотехнолошки криминал) обухвата скуп кривичних дела где се као објекат извршења и као средство за извршење кривичног дела јављају рачунари, рачунарске мреже, рачунарски подаци, као и њихови продукти у материјалном и електронском облику (Тепавац 2019). Према овом извору сајбер криминал обухвата: велики број злоупотреба информационих технологија, као и област злоупотреба у радиодифузним технологијама у коме рачунари, који обједињују хардверске и софтверске компоненте, могу бити субјекат или објекат напада. У случају када се рачунари користе за извршење или планирање и организовање сајбер напада, они представљају субјекат сајбер напада (Роџерс 2004). У случају када су недозвољене дигиталне активности усмерене ка рачунарским системима (хардверском или софтверском алату

или подацима који су у њима похрањени или до којих се на посредан начин може доћи помоћу тог рачунарског система), рачунари представљају објекат сајбер напада.

Оштећење, злоупотреба или уништење хардверских и софтверских компоненти остварује се помоћу посебних рачунарских програма и конкретних алата произведених помоћу информационих технологија и на тај начин се злоупотребљава рад у сајбер простору уз наношење материјалне или интелектуалне штете корисницима сајбер простора. На основу изнетог, сајбер криминал се може појмовно одредити као врста криминала који се одвија у сајбер простору и који обухвата људску делатност усмерену на наношење штете корисницима сајбер простора уништењем, оштећењем или злоупотребом рачунарских и телекомуникационих средстава и система, који се користе на интернету или у другим рачунарским мрежама или за потребе реализације било које друге дигиталне активности. Може се манифестовати као класичан криминал чији је циљ наношење штете појединицима и групама корисницима сајбер простора, уз најчешће персоналну корист извођача сајбер напада, али и такође као сајбер саботажа и сајбер тероризам. Сајбер шпијунажа представља облик сајбер криминала усмереног на добијање обавештајних информација о плановима и активностима стране државе, међународне организације или конкурентске компаније применом сајбер простора уз коришћење за то, посебно оспособљених агената. Сајбер шпијунажа је усмерена пре свега на откривање државних, службених или пословних тајни супарничких држава, организација или конкурентских фирми у сајбер простору. За разлику од сајбер шпијунаже и сајбер криминала, сајбер тероризам представља делатност која се одвија у сајбер простору, чији је циљ манифестација терора као стања изазивања страха и панике код грађана или званичних институција неке државе. Овај облик тероризма се извршава помоћу рачунарских система у виртуелном рачунарском простору и производ је савременог рачунарског доба. Без обзира на све могуће разлике заједничко за све облике сајбер криминала јесте да се могу извршити помоћу сајбер напада (у ужем смислу сајбер криминал и јесте последица изведеног сајбер напада, док у ширем смислу остављa се могућност да сајбер криминал представља и последицу активности које су планиране и организоване помоћу рачунарских средстава). Сајбер напад представља злонамеран, илегалан напад на рачунарски систем, који спроводе сајбер криминалци – хакери (Клисарић 2021). Циљ ових активности, које се најчешће реализују хаковањем, је уништавање, крађа или промена корисничких информација или сајбер шпијунажа ради накнадног добијања одређене користи. Ове намерне радње не само да угрожавају безбедност и сигурност корисничких информација, већ могу произвести и огромне материјалне или нематеријалне губитке (крађа интелектуалне својине, личних података, персоналних здравствених картона и слично). Званична статистика показује да је у току пандемије 2020. године, број инцидената на рачунару је повећан за 51% у односу на 2019. годину, а тренд раста сајбер напада настављен је и у 2021. години (FSB 2021).

Упркос увреженим мишљењима да су сајбер напади углавном јефтини, да изазивају локалну штету и не достижу висок ниво интензитета, савремени сајбер напади, изведени од стране професиналних група или организација уз адекватну логистику, могу нанети значајну економску и политичку штету погођеној страни (Адонис 2021; Петровић 2021в). Добро организованим и изведеним сајбер нападима

тешко погођене могу бити и разне државне, владине, образовне или медицинске институције, као и сектор привреде, те безбедносни системи. Такође, треба истаћи да бити хакер данас постаје атрактивна активност и занимање, за чијом потребом је интересовање све веће са развојем информационих технологија (Кожовић, Ђурђевић 2019). Многи од њих више нису само заинтересовани за активности везане за крађу информација од великих корпорација уз финансијске или друге уцене и изнуде, већ све више, мете сајбер напада, од стране хакера, представљају политички актери и државне институције са тенденцијом изазивања политичких тензија и економских нестабилности уз понекад обрисе спровођења радњи чак и сајбертероризма (Јонев 2016; Лајоие 2003).

Сајбер напади се реализују путем малициозних програма (malware). Реч је о штетним програмима, које сајбер криминалци користе како би приступили туђим рачунарима наношећи штету самим рачунарским системима или корисницима тих рачунарских система. Са развојем информационих технологија развијају се малициозни програми за извођење сајбер напада. Најпознатије врсте ових програма су: вируси troyans, spyware, adware, ransomware, scarware, phishing, као и малициозни програми намењени крађи идентитета. Вируси (тројанци) се препознају по променама у раду рачунара или порукама које искачу на дисплеју паметног телефона или на монитору уз честе промене у изгледу или садржају датотека. Spayware су малициозни програми намењени за праћење, односно шпијунирање активности корисника интернета, док је adware намењен за инсталацију искачућих прозора или порука (Осаба et al. 2018). Ransomware представља сајбер изнуду и сврстава се у озбиљне облике нарушавања сајбер безбедности, где је могућ губитак контроле над информацијама, уз уцену од стране хакера који је извео сајбер напад са циљем тражења финансијских средстава за враћење нападнутих информација у првобитно стање. Scarware представља врсту преваре корисника сајбер простора усмерену на уверавању да је његов рачунар или паметан телефон нападнут вирусима и да је неопходно да се купи одређени антивирусни програм (иако у стварности није дошло ни до каквог напада). Фишинг (phishing) представља превару путем коришћења мејла, где сајбер криминалци покушавају да добију поверљиве информације попут лозинки, корисничких имена, броја рачуна, личних података. Уовом случају преваранти се најчешће представљају као неке компаније, међународне организације или државне институције са именима сличним стварним организацијама или институцијама, или као појединци у невољи, како би деловали што веродостојније.

Крађа идентитета представља изузетно опасан облик нарушавања сајбер безбедности, где сајбер криминалци, након претходно извршене крађе података (такозвано цурење података), формирају виртуелну личност уз помоћ украдених биометријских података, где се помоћу такве личности у следећем кораку обављају бројне недозвољене радње. Крађом идентитета не само да се доводи у забуну невиност лица коме је украден идентитет након откривања кривичних дела, већ често може доћи и до потенцијалне физичке угрожености лица коме је идентитет украден. У овом случају посебно је честа превара преко друштвених мрежа, што је за последицу и имало увођење Опште уредбе о заштити података о личности на основу чега је и у Републици Србији донесен Закон о заштити података о личности.

МЕЂУНАРОДНО ПРАВО И САЈБЕР НАПАД

Имајући у виду да је сајбер простор производ савременог доба, као и да експанзија развоја информационих технологија доживљава до сада у историји човечанства невиђене квалитативне скокове, пред законодавцима широм света није нимало једноставан задатак правне регулативе коришћења сајбер простора. Проблеми регулативе у овој области су бројни и огледају се у следећим чињеницама: не постоји историја законског регулисања сајбер простора; сајбер простор није нешто што је јасно, визуелно опипљиво; експоненцијални развој информационих технологија подразумева сталне промене у сајбер простору које је тешко континуирано и доследно законски дефинисати; не постоји јасно одређење средстава којима се врши сајбер напад као оружја или средства за вршење противзаконите радње; тешко је извршити прецизно одређење ко је аутор сајбер напада; детектовање сајбер злочина подразумева често високостручно профилисани кадар.

Као што је већ напоменуто, развој информационе технологије се везује искључиво за период савременог доба. Због тога не постоји историјски континуитет правног регулисања области употребе средстава информационе технологије (Goodson, Knobel, Lankshear, Mangan 2002). Законска решења ових појава се спроводе „ад хок" са развојем потенцијала угрожавања безбедности сајбер простора и фокусирана су на одређење и дефинисање као криминалних активности оних сајбер напада, који су најфреквентнији или изазивају потенцијално највише штете. У овом смислу треба истаћи и проблем откривања сајбер напада и законску регулативу којом су дефинисане и могућности коришћења средстава детекције и самог детектованог материјала, као доказног материјала на суду (Стојковић 2017). Ово је посебно важно истаћи имајући у виду чињеницу да све напредније средства информационе технологије упоредно прате и све технолошки развијенија средства и методе за извођење сајбер напада. Ово за последицу има потребу сталног унапређења и средстава за детекцију сајбер кримналних активности, као и стално ажурирање законске регулативе, класификовањем квалитативно нових врста сајбер напада као законски дефинисаних криминалних активности (Махмутчехајић, Силајџић 2019).

Проблем у међународно правној регулативи сајбер напада са циљем превенције и процесуирања учинилаца компјутерских криминалних активности и обезбеђивања безбедности сајбер окружења, представља и тешкоћа у квалификовању средстава сајбер напада као средстава „оружане силе" или „оружаног напада". Наиме, средство сајбер напада често представља обичан софтвер, који се може нарезати на диск и преносити без икакве могућности визуелног откривања његовог значења и сврхе. Средства сајбер напада не препознају класичне препреке у виду физичког и класичног техничког обезбеђења, она су разноврсна, користе их и препознају као опасност високопрофилисане стручне личности или, евентуално, хардверска и софтверска решења кроз развој и примену организационих мера заштите сајбер безбедности.

Потребно је истаћи и чињеницу да сајбер простор представља нову форму мисаоне и конкретне стварности и одигравања бројних радњи. Одсуство његовог јасног дефинисања, као и чињеница да је јако тешко одредити јасне границе овог

простора уз постојање бројних нерегулисаних девијантних тачака које могу али и не морају бити део сајбер простора, значајно отежава дефинисање локације дешавања сајбер напада са становишта правне регулативе. Све ово доводи до чињенице да значајан део држава данас не може још увек да се договори који би садржај био довољно прикладан да опише сајбер претње и сајбер нападе. Без добро дефинисаних термина, ниједна држава данас не може да оптужи за међународно противправно дело „у контексту напада компјутерског информационог система" било коју другу државу, организацију или појединца.

Да би се прихватило међународно право у сајбер простору, мора се знати идентитет 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 (Hollins 2021).

Одсуство било какве просторне границе, као и анонимност, која представља једну од кључних карактеристика сајбер простора, отежавају одређивање ко је одговоран за одређени сајбер напад. Поред тога, у међународном праву још увек не постоји специфичан стандард за пружање довољно доказа, на основу којих ће држава моћи да оптужи сајбер криминалца за кривично дело (Младеновић 2016). Поред тога, често се дешава да су хакерске групе, које нападају информационе мреже, расуте по различитим земљама, што значајно отежава поступак њиховог привођења правди.

Неопходно је истаћи да у савременим условима, још увек не постоје посебна правила која се примењују у регулисању правних односа који настају у току компјутерског рада или у процесу сајбер напада на информациони систем, како наводе Ремус и Шонкартскаја (Remus 2013). Такође, основне одредбе међународно правних аката, данас су мање ефикасне против недржавних сајбер напада, као што је то случај са надзором над скривеним деловањем приватних лица, што још увек није могуће чинити због ограничених овлашћења и захтева за поштовањем права на приватност.

Одсуство међународне регулативе, нарушени међународни односи између великих сила, зачетак формирања мултиполарног света приморава многе државе, да се не придржавају међународних стандарда, већ да прибегавају сопственим облицима заштите заобилажењем општеприхваћених законских регулатива и политичких концепата. На пример, Русија и Кина промовишу приступ сајбер суверенитета који контролише држава, где влада има искључиву надлежност над националним сајбер простором, што је у складу и са њиховим државним уређењима и чврстом централистичком политиком. За разлику од њих, западне државе подржавају децентрализовани облик управљања, који је опет у функцији државних уређења ових држава и јасних геополитичких усмерења, која често не зависе од политичких идеологија него од мултинационалних компанија као извора и заштитиника овог децентрализма (Remus 2013). Све ово доводи до бројних међународних несугласица о томе шта се дешава у сајбер нападима, која су то искуства и како на основу тих искустава унапредити правну регулативу у овој области. Једноставно, недељење информација утиче на међународно правно регулисање ове области. Са одређене тачке гледишта, такав пут и избор се може сматрати прихватљивим, јер свака појединачна држава има могућност да самостално идентификује своја најугроженија места и примени

сопствене превентивне механизме да их обезбеди. Међутим, са друге стране, такав формат не даје јасна овлашћења за спровођење закона и не дозвољава да се у потпуности идентификују сајбер криминалци и спрече даљи сајбер злочини.

Може се закључити да сви наведени проблеми, свакако нарушавају могућност успостављања реда у сајбер простору. Бројна међудржавна трвења, наорочито данас, у време можда најозбиљније политичке кризе после Другог светског рата због сукоба у Украјини, не доприносе интересу усаглашавања међународних напора у сузбијању сајбер напада. Може се рећи, да су сајбер напади сада у овим околностима прерасли у сајбер ратовање ради наношења максималних политичких, војних и економских губитака у сајбер простору. Нема сумње да ће развој овог оружја, које не представља класично ватрено оружје и које не представља класичан чин агресије и оружаног напада, још више добити на замаху. У таквим условима, слабије развијене државе још више ће заостајати у области борбе против сајбер претњи и напада због: отежаног откривања сајбер напада, отежане идентификације и атрибуције нападача, као и због отежане благовремене, прецизне и правне регулације сајбер напада. Све ово, уз чињеницу да недостаје међународно правни континуитет у борби против сајбер претњи, отежава глобално институционално дефинисање законске регулативе. У овом смислу, потребно је истаћи и да се у свету као прва законска регулатива високотехнолошког криминала, појавила констатација Интерпола 1982. године, када је званично саопштено следеће: „Данас у савременом свету постоји још један велики усавршени фронт који је присутан у светским размерама. Велики криминалитет, организације криминалаца, све више се оријентишу на акције пљачки у којима је објекат компјутер. Електроника се злоупотребљава. Не бележи се пад класичних пљачки, али се из године у годину повећава нова врста криминалитета у коме се електроника користи као средство да се криминалци домогну милионских свота новца". Ово говори у прилог томе колико је ова област млада са становишта филогенетског развоја цивилизације (Китаровић 1998).

Претходно наведено јасно указује на то колико је тешко правно регулисати криминалитет у сајбер простору, иако је он препознат као озбиљан проблем транснационалне природе, који на жалост има политизован каратер. Као главни фактори који детерминишу процес доношења закона о глобалном сајбер простору су: релевантне институције које делују под покровитељством Организације Уједињених нација, законодавство регионалних и специјализованих међународних организација, као и углавном високо развијене земље које имају интерес да ова питања регулишу како би повећале своју националну безбедност и заштитиле своју привреду (Xinmin 2016).

У оквиру ОУН постоје четири главне међународне инситуције, које су укључене у активности постављања законодавних стандарда у сајбер простору. Те институције су следеће: Светски самит о информационом друштву; Група владиних стручњака за безбедност информација под комитетом Генералне скупштине УН; Група експерата УН за сајбер криминал и Међународна унија за телекомуникације.

Поред наведних институција у оквиру ОУН, законска регулатива која је усвојена од стране регионалних и специјализованих међународних организација, такође представља саставни део процеса доношења правила о начину коришћења глобалног

сајбер простора. Један од најважнијих међународних докуметната за борбу против сајбер напада, а који је усаглашен са више националних законских оквира, и који побољшава методе истраге и унапређује сарадњу међу земљама по питањима сајбер безбедности је „Конвенција о сајбер криминалу". У оквиру ове конвенције проучавана си и идентификована питања као што су државни суверенитет у сајбер простору, легално коришћење сајбер простора и методе и средства борбе против сајбер криминала. Међутим, треба схватити да је међународно право првенствено засновано на поштовању правних поредака држава (и субјеката њиховог правног, политичког, економског, војног или неког другог удруживања– међународне организације). Међународни закони и прописи немају монопол над потпуном законском регулативом сајбер простора и не могу регулисати понашање компанија или појединих запослених у области информационо-комуникационих технологија у потпуности. На основу свега наведеног може се закључити да је развијање међународне правне регулативе у овој области један озбиљан и дуготрајан индуктивно – дедуктивни процес који мора бит заснован на симбиози свих међународних субјеката од појединачних држава до кредибилних међународних организација.

УНУТРАШЊЕ РЕГУЛИСАЊЕ (ПРОЦЕСУИРАЊЕ) САЈБЕР НАПАДА

У одељењу за високотехнолошки криминал обављају се послови и задаци из надлежности Републичког јавног тужилаштва у вези са кривичним делима високотехнолошког криминала, извршавање обавеза преузетих Законом о потврђивању Конвенције о високотехнолошком криминалу, остварује координација рада са посебним одељењем Вишег јавног тужилаштва у Београду за високотехнолошки криминал, као и координација рада са тужилаштвима опште надлежности, а у вези са кривичним делима високотехнолошког криминала.

У домаћем законодавству регулисање ове области извршено је Законом о организацији и надлежности државних органа у борби против високотехнолошког криминала. Овим законом уређена је организација, надлежност и овлшћења државних органа у циљу откривања, кривичног гоњена и суђења за кривична дела која су одређења овим кривичним законом. Овим законом се високотехногошки криминал представља вршење кривичних дела као средство извршења користе рачунари, рачунарске мреже, рачунарски подаци и њихови производи у материјалном или електронском облику. Под производима подразумевамо рачунарске програме и ауторска дела која се могу употребити у електронском облику.

Закон се примењује ради откривања, кривичног гоњења и суђења за кривична дела против безбедности рачунарских података одређених КЗ, кд против интелектуалне својине, привреде и правног саобраћаја код којих се у извршењу користе рачунари, рачунарски програми, мреже и подаци, где број примерака ауторских дела прелази 2000 примерака, или материјална штета прелази износ од 1.000.000 динара. Такође, закон се примењује за кривична дела против слобода и права човека и грађанина, јавног реда и мира, полне слободе, уставног уређења и безбедности Републике Србије, због начина извршења сматрају кривична дела високотехнолошког криминала.

У Републици Србији за поступање у вези кривичних дела из области високотехнолошког криминала надлежно је Више јавно тужилаштво у Београду. У оквиру тужилаштва основано је одељење чија је област деловања борба против високотехнолошког криминала. Одељењем управља посебни тужилац за високотехнолошки криминал.

Када се у кривичном предмету сазна да се ради о делу предвиђеном чланом 3. Закона, посебни тужилац обавештава Републичког јавног тужиоца и захтева од њега да му се повери надлежост за поступање у таквом предмету. Посебни тужилац поред законом прописаних услова, поседује и информатичка знања.

У оквиру МУП-а Републике Србије – Управе криминалистичке полиције формирано је Одељење за борбу против високотехнолошког криминала, чији је задатак откривање и процесуирање кривичних дела и учиниоца истих из области високотехнолошког криминала. Одељење поступа по захтеву посебног тужиоца. Од оснивања одељења, велики број учинилаца кривичних дела из области високотехнолошког криминала је откривен и процесуиран. Можемо навести као пример једну од најобимнијих акција под називом Армагедон, која има за циљ борбу против онлајн педофилије, која траје преко 10 година и још увек траје, у којој је до сада откривено и процесуирано преко 210 учинилаца кривичних дела. Такође, поднето је преко 220 кривичних пријава због различитих кривичних дела из ове области.

Република Србија је осим наведеног закона, а у складу са Поглављем 24 које се односи на процес евроинтеграција, усвојила и Стратегију која се односи на борбу против високотехнолошког криминала, за период од 2019. – 2023. године. У оквиру стратегије, као циљ се наводи усклађивање унутрашњег права и права ЕУ, јачање надлежних органа као и усклађивање и блиска сарадња надлежних органа и институција у Републици Србији, како би се борба против високотехнолошког криминала подгла на виши ниво. Такође наша земља је и потписница Конвенције о високотехнолошком криминалу из 2009. године.

Из свега наведеног, закључујемо да се улажу велики напори и помаци у борби против високотехнолошког криминала у нашој земљи. Сматрамо да је неопходно константно пратити развој технологија, и са њиховим развојем, развијати и унапређивати правну регулативу везану за ову област, како би заштитили грађане, институције и саму државу од злоупотребе технологије.

ЗАКЉУЧАК

Нема сумње да ће међународно као и унутрашње правно регулисање коришћења сајбер простора бити једна од најбитнијих тема у блиској будућности. Наиме, развој информационих технологија, као и решења која ове технологије нуде, а која се користе у сајбер простору, у будућности ће значајно још више квалитативно унапредити живот како појединца, тако и државних и међународних структура. Као предлог за унапређење наводимо пример формирања заједничких истражних тимова, из разлога што су врло често извршиоци дела из више земаља и делују у саизвршилаштву. Формирањем таквих кривично-правних тимова из више земаља,

може се постићи циљ идентификовања учинилаца, прибављање неопходних доказа и самог процесуирања учиницала кривичних дела.

Како смо већ нагласили, сама брзина развоја модерне технологије, као и могућност злоупотребе исте, намеће потребу свакој држави да развија систем одбране институција и грађана од овакве врсте претњи. Високотехнолошки криминал не познаје границе, и мета може бити било која држава, институција или појединац, што наводи на закључак је поред унутрашњег уређења ове области, неопходна и нужна међународна сарадња, како би се на адекватан начин супротставили овој врсти криминала.

Такође, смиривање тензија између најразвијенијих држава на свету, до кога мора доћи у једном тренутку, повећаће интерес за решавањем међународно – правних ограничења употребе сајбер простора са циљем повећања националне безбедности у сајбер простору и стварања услова за економским развојем држава и формирањем светског и регионалног тржишта. На крају, може се закључити, да је нормативно – правно међународно регулисање коришћења сајбер простора и спречавање злоупотреба модерних информационо – комуникационих технологија, предуслов даљег напретка човечанства. Све ово ће у будућности довести до блиске сарадње свих међународно релевантних фактора у развоју заједничких стандарда и правила, дефинисања заједничких механизама одговора на сајбер нападе и формирање заједничке безбедоносне сајбер инфраструктуре са циљем спречавања сајбер напада и повећања сајбер безбедности на глобалном нивоу.

ЛИТЕРАТУРА

Adonis 2020: Abid Adonis. *International Law on Cyber Security in the Age of Digital Sovereignty: E-InternationalRelations*, <International Law on Cyber Security in the Age of Digital Sovereignty (e-ir.info)>. [12.02.2022.].

FSB 2021: Financial Stability Board. *Cyber Incident Reporting: Existing Approaches and Next Steps for Broader Convergence.* <Cyber Incident Reporting: Existing Approaches and Next Steps for Broader Convergence (fsb.org)>. [12.02.2022].

Goodson, Knobel, Lankshear, Mangan 2002: Ivor Goodson, Michelle Knobel, Colin Lankshear, Marshall J. Mangan. „Cyber spaces/social spaces". *Cyber Spaces/Social Spaces,* Ed.Ivor Goodson, Michelle Knobel, Marshall J. Mangan. New York: Palgrave Macmillan, 1-17.

Hollis 2021: Duncan Hollis. *A Brief Primer on International Law and Cyberspace: Carnegie Endowment for International Peace,*<Hollis_Law_and_Cyberspace.pdf (carnegieendowment.org)>. [15.02.2022].

ICRC 1972: *Convention on the Prohibition of Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on their Destruction.* <1972 Convention on the Prohibition of Biological Weapons | International Committee of the Red Cross (icrc.org)>. [10.03.2022.].

ISO 2012:*ISO/IEC 27032.*<ISO/IEC 27032:2012(en), Information technology – Security techniques – Guidelines for cybersecurity> [05.03.2022.].

ITU 2014:*ITU standardization.*<T-GEN-OVW-2014-PDF-E.pdf (itu.int)> [03.03.2022.].

Lajoie 2003: Mark Kajoie. „Psihoanaliza i sajber-prostor". *Култура*, br. 107-108, 77-98.

Mahmutučehajić, Siladžić 2019: Fatima Mahmutčehajić, Vedad Silajdžić. Etika i pravo u cyber--prostoru. *Sarajevo social review*, vol. 8, br. 1-2, 173-192.

OPCW 1997: Organisation for the Prohibition of Chemical Weapons. *Convention on the prohibition of the development, production, stockpiling and use of chemical weapons and on their destruction.* <Download the Convention | OPCW>. [12.02.2022.].

Osaba, Pierdicca, Malinverni, Khromova, Álvarez, Bahillo 2018: Eneko Osaba, Roberto Pierdicca, Eva Savina Malinverni, Anna Khromova, Fernando Alvarez, Alfonso Bahillo. "A smartphone-based system for outdoor data gathering using a wireless beacon network and GPS data: From cyber spaces to senseable spaces". *ISPRS International Journal of Geo--Information*, vol. 7, no. 5, 190, https://doi.org/10.3390/ijgi7050190

Remus 2013: Titiriga Remus. "Cyber-attacks and international law of armed conflicts; a jus ad bellum perspective". Journal of International Commercial Law and Technology, vol. 8, no. 3, 179-189.

Rodžers 2004: Mark Rodžers. „The psychology of cyber-terrorism". *Bezbednost*, vol. 46, no.1, 126-132.

Spalević, Ilić, Spalević 2018: Žaklina Spalević, Miloš Ilić, Petar Spalević. „Upotreba dela intelektualne svojine u cyber prostoru". Ur. Milovan Stanišić. *Синтеза 2018-International Scientific Conference on Information Technology and Data Related Research,* Beograd: Singidunum University, 50-57. DOI: 10.15308/Синтеза-2018-50-57

Xinmin 2016: Ma Xinmin. „Key issues and future development of international cyberspace law". *China Quarterly of International Strategic Studies*, vol. 2, no.1, 119-133.

Јонев 2016: Катарина Јонев. „Сајбер тероризам и употреба сајбер простора у терористичке сврхе". *Безбедност,* број 2, 206-222.

Klisarić 2021: Sanja Klisarić. „Hacker attacks as a form of cyaber terrorism". *Међатренд ревија*, vol. 18, no.2, 223-232.

Кривични законик („Сл. гласник РС", р. 85 од 6. октобра 2005, 88 од 14. октобра 2005 - исправка, 107 од 2. децембра 2005 - исправка, 72 од 3. септембра 2009, 111 од 29. децембра 2009, 121 од 24. децембра 2012, 104 од 27. новембра 2013, 108 од 10. октобра 2014, 94 од 24. новембра 2016, 35 од 21. маја 2019.)

Законик о кривичном поступку („Сл. гласник РС", бр. 72 од 28. септембра 2011, 101 од 30. децембра 2011, 121 од 24. децембра 2012, 32 од 8. априла 2013, 45 од 22. маја 2013, 55 од 23. маја 2014, 35 од 21. маја 2019, 27 од 24. марта 2021 - УС, 62 од 17. јуна 2021 – УС)

Закон о организацији и надлежности државних органа за борбу против високотехнолошког криминала („Сл. гласник РС", бр. 72 од 28. септембра 2011, 101 од 30. децембра 2011, 121 од 24. децембра 2012, 32 од 8. априла 2013, 45 од 22. маја 2013, 55 од 23. маја 2014, 35 од 21. маја 2019, 27 од 24. марта 2021 - УС, 62 од 17. јуна 2021 – УС)

Китаровић 1998: Никола Китаревић. „Компјутерски криминалитет". *Билтен судске праксе Врховног суда Србије*, број 2–3, 52–53.

Ковачевић 2014: Божо Ковачевић. „Америчко јавно-приватно партнерство и сајбер сигурност". *Политичка Мисао*, вол, 51, бр. 3, 76-100.

Кожовић, Ђурђевић 2019: Дејан Кожовић, Драган Ђурђевић. „Сајбер безбедност у авијацији". *Међатренд Ревиеw*, вол. 16, бр. 2, 39-56.

Младеновић 2016: Драган Младеновић. *Мултидисциплинарни аспекти сајбер ратовања*. Докторски рад. Београд: ФОН.

Младеновић, Дракулић, Јовановић 2012: Драган Младеновић, Мирјана Дракулић, Данко Јовановић. „Међународно право и сајбер ратовање". *Војно дело*, 2, 9-39.

Петровић 2021а: Јелена Петровић. „Улога медија у психолошком рату". Баштина, вол. 31, бр. 53, 283-297.

Петровић 2021б: Јелена Петровић. „Психолошки рат и војне науке". Баштина, вол. 31, но. 55, 267-278.

Петровић 2021в: Јелена Петровић. *Војна психологија и психолошки рат: достигнућа и перспективе*. Лепосавић: Институт за српску културу, Приштина – Лепосавић.

Стојановић 2017: Александар Стојановић. „Анализа дискурса секуритизације у сајбер-простору". *Комуникација и култура онлине*, вол. 4, бр. 4, 216-231.

Тепавац 2019: Дејан Тепавац. „Облици и субјекти угрожавања пословних информација у сајбер простору". *Војно дело*, вол. 71, бр. 6, 59-72.

Томић 2003: Зорица Томић. „Сајбер-простор и проблеми разграничења". *Култура*, бр. 107-108, 9-19.

Jovan M. GORDIĆ

CYBER ATTACKS FROM THE ASPECT OF INTERNATIONAL AND DOMESTIC LAW

Summary

There is no doubt that international as well as internal legal regulation of the use of cyber space will be one of the most important topics in the near future. Namely, the development of information technologies, as well as the solutions that these technologies offer, which are used in cyberspace, will significantly improve the quality of international life structures and thus the individual structure in the future

As a proposal for comparison, we cite an example of the formation of joint investigative teams, due to the fact that very often the perpetrators are from several countries and act in co-perpetration. By forming such criminal-legal teams from several countries, the goal of identifying the perpetrators, obtaining the necessary evidence and prosecuting the perpetrators of criminal acts can be achieved.

As we have already emphasized, the very speed of development of modern technology, as well as the possibility of its misuse, imposes the need for every state to develop a system of defense of institutions and citizens against this type of threats. High-tech crime knows no borders, and the target can be any country, institution or individual, which leads to the conclusion that in addition to the internal regulation of this area, international cooperation is also necessary in order to adequately oppose this type of crime.

Also, the calming of tensions between the most developed countries in the world, which must happen at some point, will increase the interest in solving international legal restrictions on the use of cyberspace with the aim of increasing national security in cyberspace and creating conditions for the economic development of countries and the formation of world and regional markets. In the end, it can be concluded that the normative - legal international regulation of the use of cyberspace and the prevention of misuse of modern information and communication technologies is a prerequisite for the further progress of humanity.

In the future, all this will lead to close cooperation of all internationally relevant factors in the development of common standards and rules, the definition of common response mechanisms to cyber attacks and the formation of a common security cyber infrastructure with the aim of preventing cyber attacks and increasing cyber security on a global level.

Key words: international public law, domestic law, criminal law, criminal process, cyber-attack, cyber security, cyber threat, suspects.

Рад је предат 25. јуна 2022. године, а након мишљења рецензената, одлуком одговорног уредника *Баштине,* одобрен за штампу