МЛАДЕН М. МИЛОШЕВИЋ*
НЕНАД Р. ПУТНИК
Факултет безбедности
Београд

УДК 343.3/.7(004.391.23):351.78(497.11)
Монографска студија
Примљен: 27.04.2017
Одобрен: 23.05.2017
Страна: 177-191

САЈБЕР БЕЗБЕДНОСТ И ЗАШТИТА ОД ВИСОКОТЕХНОЛОШКОГ КРИМИНАЛА У РЕПУБЛИЦИ СРБИЈИ - СТРАТЕШКИ И ПРАВНИ ОКВИР

Сажетак: У ери глобалне информационо-комуникационе повезаности и високе технолошке зависности савременог човека, проблеми заштите од високотехнолошког криминала и изградње безбедног сајбер окружења искрсавају у први план. На међународним и националном нивоу се усвајају нормативни и стратешки документи са циљем унапређења стања безбедности и редукције хетерогених ризика по појединце, организације и државе. Република Србија активно учествује у међународним и регионалним иницијативама, а последњих година је предузела кораке ка значајнијем унапређењу националног правног оквира. Ипак, стручна јавност оцењује да домаћи правни оквир није потпун, јасан и прецизан, као и да недостају важни стратешки документи. Такође, очигледни су проблеми и пропусти у имплементацији законских решења. Аутори пружају исцрпан преглед постојећих стратешких докумената и релевантне позитивноправне регулативе и анализирају њихову функционалност и адекватност. Претходно, они се осврћу на међународноправну димензију кључних безбедносних питања у сајбер простору. Аутори дају предлоге за редефинисање одређених законских решења и стратешких докумената и указују на механизме боље имплементације постојећег стратешког и правног оквира.

Кључне речи: сајбер безбедност, високотехнолошки криминал, правни оквир, стратегија безбедности

Увод

Проблем безбедности у сајбер простору, постао је тема од глобалног значаја захваљујући огромном техничко-технолошком напретку у сфери информацино-комуникационе технологије, који је праћен развојем људских потреба у виртуелном свету и наглим повећањем зависности савременог човека од

* milosevic@fb.bg.ac.rs

функционисања ових технологија. (Boyd, 2007; Gross et al., 2002). Развој информационе и комуникационе технологије „повећао је брзину и обим интеракција у савременом друштву и тиме допринео интензивирању како друштвених односа у сфери политике, економије и културе, тако и међузависности појединаца, организација и нација широм света“ (Путник, 2009: 2).

Безбедносни ризици који се испољавају у сајбер свету су веома хетерогени и крећу се од вршења кривичних дела на штету појединаца и правних лица преко или уз помоћ рачунарских система и мрежа до сајбер операција којима се угрожава безбедност држава и међународних организација кроз спровођење аката тероризма или чак агресије.

Досадашња искуства у супротстављању безбедносним претњама у сајбер простору указују на потребу стварања кохерентног оквира који подразумева примену како превентивних, тако и репресивних мера у стварању безбедног сајбер амбијента. (Путник et al., 2013: 76).

Предмет нашег интересовања је стратешко-правни оквир за супротстављање високотехнолошком криминалу и осигуравање безбедности у сајбер простору у Републици Србији. Знајући да је сајбер безбедност феномен са израженом међународном димензијом, анализу позитивноправног оквира у нашој земљи смо употпунили уводним осртом на главне проблеме регулисаности (или: недовољне регулисаности) овог феномена у окриљу међународног права.

Проблем правне (не)регулисности сајбер операција у међународном праву – кратак осврт

У академској јавности се већ дуго расправља о проблему правне нерегулисаности конфликата у сајбер простору. Актуелно је и питање о могућим правним квалификацијама чина сајбер ратовања, будући да је велико питање може ли се и под којим условима одређен скуп сајбер операција подвести под дефиницију агресије усвојену у Резолуцији Уједињених нација, или је оправдано и довољно карактерисати га као кривично дело кажњиво по одредбама националних законодавстава. (Милошевић, Путник, 2013; Младеновић, 2012).

Агресорски рат је и пре суђења у Нирнбергу био забрањен Бријан-Келоговим пактом из 1928. године, мада тим пактом није била уведена потпуна забрана сваког рата. То ће се десити тек усвајањем Повеље УН која допушта искључиво одбрамбени рат и принудне мере самих Уједињених нација. Спречавање силе у односима између држава једно је од основних начела УН, а посебно се овим питањима баве чланови 1, 2, 33 и 39 Повеље УН. Резолуције Генералне скупштине Уједињених нација бр. 3314 из 1974. године пружа критеријуме за дефинисање агресије а наведени су и конкретни акти који се сматрају агресорским по слову резолуције. (Вучинић, 2013; Милошевић, Путник, 2013).

Мелцер (Melzer) разматра питање jus ad bellum код сајбер операција анализирајући појам силе из Повеље УН.Она не пружа правну дефиницију силе, па се садржај овог појма одређује сходно духу и смислу Повеље и међународном обичајном праву (Melzer, 2011). Аутор истиче да је теорија недвосмислена у оцени да сајбер операције чији се ефекти огледају у смрти и рањавању људи или физичком уништењу објеката могу сматрати употребом силе у међународним односима, иако се сила у Повељи схвата на рестриктиван начин у односу на стандардно значење те речи. У прилог његовом мишљењу говори и саветодавно мишљење Међународног суда правде (International Court of Justice, Legality of the Threat or Use of Nuclear Weapons, advisory opinion, 1996) у ком се исиче да се "било која употреба силе, без обзира на коришћено средство/оружје", може сматрати силом у овом смислу; а са њим се слажу и други теоретичари. (Schmitt, 1999).

Проблем, међутим, настаје код сајбер операција које не резултују непосредно људским жртвама и материјалним разарањима, али остављају друге озбиљне последице, попут масовног DDoS напада на одређене системе угрожене државе (Melzer, 2011). Други проблем лежи у чињеници да је појам оружаног напада из члана 51 Повеље ужи од појма силе из члана 2. Да би држава стекла право на индивидуалну или колективну самоодбрану, потребно је да дође до оружаног напада. Иако се поменуте сајбер операције могу сматрати употебом силе, посебно када доводе до ефеката упоредивих са кинетичким, нуклеарним, хемијским или биолошким ратовањем, недостају поуздани ослонци за доношење недвосмисленог закључка у вези изједначавања сајбер напада са оружаним нападом.

Интересантан покушај разрешења бројних недоумица је учињен од стране НАТО, када је окупљена група истакнутих правних експерата, са задатком да проучи и одговори на најважнија питања о могућности употребе правила међународног права на сајбер ратовање. Овај пројекат је резултовао издавањем Приручника о применљивости међународног права на сајбер ратовање (Tallinn Manual on the International Law Applicable to Cyber Warfare). Правило 13 Приручника јасно одређује да сајбер операција која би довела до смрти или повреда људи, треба да се сматра као оружани напад без обзира што није употребљено оружје у конвенционалном смслу. У истом смеру иде и Правило 11, које дефинише употребу силе у смислу сајбер ратовања. Дефиниција сајбер напада, дата у Правилу 30, доследно изражава исту идеју: „сајбер напад је офанзивна или дефанзивна сајбер операција за коју се основано може сматрати да ће довести до смрти или рањавања лица или уништавања или оштећења објеката" (Tallinn Manual on the International Law Applicable to Cyber Warfare, 2013).

И поред постојећих покушаја теоретичара и издавања правно необавезујућих докумената попут овог Приручника, далеко смо од јединственог одређења правног статуса сајбер операција у смислу међународног ратног и хуманитарног права, те можемо закључити да је међународноправна димензија сајбер безбедности суштински недовољно развијена, као и да обилује нејасноћама и различитим тумачењима.

Национални правни оквир заштите од високотехнолошког криминала

Правна регулатива сајбер простора у Републици Србији није адекватна и потпуна, а безбедносни изазови у виртуелном свету непрестано расту и трансформишу се. Правни оквир сајбер безбедности обухвата прописе којима се регулишу надлежности органа за управљање безбедносним ризицима у информационо-комуникационим системима и сузбијање радњи којима се функционисање ових система угрожава или нарушава, као и норме о техникама, методама и процедурама заштите, координацији између чинилаца заштите, њиховој одговорности и надзору над применом законских овлашћења и обавеза. Осим њих, нормативни оквир обухвата и норме којима се регулише заштита од високотехнолошког криминала и других противправних претњи у сајбер простору. Овде спадају прописане превентивне и репресивне мере, те материјалне и процесне норме, првенствено у сфери казненог законодавства. У наведеном смислу, правни оквир сајбер безбедности је сачињен од одредаба различитих закона, којима је безбедност информационо-комуникационих система примаран или секундаран предмет регулисања.

Дела којима се нарушава или угрожава функционисање ИКТ система, као и интегритет, доступност, аутентичност и тајност рачунарских података, санкционишу се кривичноправним одредбама, чиме се кривично право показује као инструмент заштите сајбер безбедности.

Проблем супротстављања високотехнолошком криминалу има материјалноправну и процесноправну димензију, те је српски законодавац, вођен обавезама преузетим усвајањем и ратификацијом међународних конвенција, последњих деценију и по значајно изменио законски кривичноправни оквир у овој области. Србија је потписала и ратификовала Конвенцију о високотехнолошком криминалу, коју је Савет Европе усвојио 2001. године, као и њен Додатни протокол (Закон о потврђивању Конвенције о високотехнолошком криминалу, 2009; Закон о потврђивању Додатног протокола уз Конвенцију о високотехнолошком криминалу који се односи на инкриминацију дела расистичке и ксенофобичне природе извршених преко рачунарских система, 2009). Још 2003. године, српско кривично законодавство је измењено тако да инкриминише и кривична дела против безбедности рачунарских података (Закон о изменама и допунама Кривичног закона Републике Србије, 2003). Занимљиво је да српски законодавац, инкриминишући понашања сходно начелима Конвенције, санкционише све основне облике високотехнолошких кривичних дела осим оних везаних за пресретање комуникације. Ово остаје као очигледан недостатак актуелног решења домаћег кривичног материјалног законодавства (Стојановић, 2012).

Пуна имплементација Конвенције је захтевала даљу законску реформу. Важан корак у том смеру представљало је усвајање Закона о организацији и надлежности државних органа за борбу против високотехнолошког криминала (Закон о организацији и надлежности државних органа за борбу против висо-

котехнолошког криминала, 2005) којим се прецизира круг кривичних дела на која се закон примењује. Ипак, остаје питање да ли је адекватно и практично решење којим се ограничава круг кривичних дела која се, уз испуњење осталих услова, сматрају делима високотехнолошког криминалитета. Можда би функционалније било решење које дозвољава поступање јавног тужилаштва посебне надлежности у свим случајевима где се као објекат или средство извршења кривичних дела јављају рачунари, рачунарски системи, рачунарске мреже и рачунарски подаци, без обзира да ли спадају у неку од поменутих глава Кривичног законика. Ова примедба се може ублажити констатацијом да су наведене групе кривичних дела свакако веома обухватно одређене те да се код њих најчешће и може јавити дело са елементима високотехнолошког криминала.

Овим законом уведене су и посебне организационе целине у надлежним тужилаштвима и судовима (Више јавно тужилаштво и Виши суд) с тим да ове одредбе ни данас нису имплементиране у потпуности. У оквиру министарства задуженог за унутрашње послове формирана је, по одредбама овог закона, служба за борбу против високотехнолошког криминала, која је смештена у оквире Управе криминалистичке полиције. Министарство надлежно за послове правосуђа добило је задатак да обезбеди средства и услове за рад новообразованих одељења.

Важно место у броби против високотехнолошког криминала заузима Законик о кривичном поступку (Законик о кривичном поступку, 2011), јер откривање, кривично гоњење и суђење за дела високотехнолошког криминала имају бројне специфичности, које препознају упоредна права (Урошевић et al., 2012: 37). Посебно вреди поменути одредбе које се односе на спровођење посебних доказних радњи у случају откривања, разјашњавања и доказивања кривичних дела високотехнолошког криминала. Посебне доказне радње могу се одредити према лицу за које постоје основи сумње да је учинило кривично дело из члана 162. Законика о кривичном поступку, а на други начин се не могу прикупити докази за кривично гоњење или би њихово прикупљање било знатно отежан. Изузетно, мере се могу одредити и према лицу за које постоје основи сумње да припрема неко од кривичних дела из става 1. овог члана, а околности случаја указују да се на други начин кривично дело не би могло открити, спречити или доказати или би то изазвало несразмерне тешкоће или велику опасност. Тачка 1. става 1 овог члана експлицитно дозвољава примену посебних радњи доказивања уколико је реч о случају у ком поступа јавно тужилаштво посебне надлежности, а став 3. члана 162 предвиђа да се мера из члана 166 Законика о кривичном поступку – тајни надзор комуникације, може применити и за кривична дела: неовлашћено искоришћавање ауторског дела или предмета сродног права, оштећење рачунарских података и програма, рачунарска саботажа, рачунарска превара и неовлашћени приступ заштићеном рачунару, рачунарској мрежи и електронској обради података.

Иако се било која од законом предвиђених посебних мера доказивања може применити на случајеве у којима поступа јавно тужилаштво надлежно за високотехнолошки криминал, две мере се издавајау по значају за област сајбер безбедности. Прва је тајни надзор комуникације.

На образложени предлог јавног тужиоца суд може одредити надзор и снимање комуникације која се обавља путем телефона или других техничких средстава или надзор електронске или друге адресе осумњиченог и заплену писама и других пошиљки. Ова мера (тајни надзор комуникације) може се одредити у трајању од три месеца, а због неопходности даљег прикупљања доказа се може продужити највише за три месеца, с тим да у случају високотехнолошког криминала и других кривичних дела у којима поступају јавна тужилаштва посебне надлежнсости, ова мера може бити продужена још највише два пута по три месеца. Наредбу о одређивању тајног надзора комуникације спроводе полиција, Безбедносно-информативна агенција или Војнобезбедносна агенција. Према члану 168 Законика о кривичном поступку поштанска, телеграфска и друга предузећа, друштва и лица регистрована за преношење информација, су задужена да надлежном органу који спроводи меру омогуће спровођење надзора и снимања комуникације и да, уз потврду пријема, предају писма и друге пошиљке. Једноставним тумачењем долазимо до закључка да се наведена мера односи и на интернет провајдере, јер електронску пошту можемо сврстати под екстензивну формулацију друге пошиљке.

Друга посебна радња доказивања која је од нарочитог значаја за ову област је рачунарско претраживање података. На образложени предлог јавног тужиоца судија за претходни поступак може одредити рачунарско претраживање већ обрађених личних и других података и њихово поређење са подацима који се односе на осумњиченог и кривично дело, под законом предвиђеним условима. Ову меру извршава полиција, Безбедносно-информативна агенција, Војнобезбедносна агенција, царинске, пореске или друге службе или други државни орган, односно правно лице које на основу закона врши јавна овлашћења.

Правни прописи у области сајбер безбедности и спречавања електронског насиља

Поменута одступања од начела заштите приватности и тајности комуникација, су неопходна ради остваривања циљева у борби против друштвено опасних понашања и принципијелно нису спорна. Ипак, недоумице о њиховом спровођењу и начину примене законских овлашћења су честа у стручној јавности Она, међутим, нису значајна само због борбе против високотехнолошког криминала, већ су важан аспект сајбер безбедности уопште, јер могу довести до злоупотреба везаних за кршење основних људских и мањинских права гарантованих Уставом и међународним уговорима. Законик о кривичном поступку, пак, није једини пропис који омогућава примену специјалних техника и посебних мера и процедура. Оне се могу имплементирати и на основу Закона о Безбедносно-информативној агенцији (Закона о Безбедносно-информативној агенцији , 2002; у даљем тексту: Закон о БИА) и Закона о Војнобезбедносној агенцији и Војнообавештајној агенцији (Закона о Војнобезбедносној агенцији и Војнообавештајној агенцији, 2009; у даљем тексту: Закона о ВБА и ВОА). Ови закони су се, од доношења до данас, мењали како би се ускладили са поје-

диним уставним начелима и стандардима заштите људских права. Њих ћемо, без обзира што су битни и из призме заштите од високотехнолошког криминала, првенствено разматрати из аспекта опште сајбер безбедности.

Закон о БИА, је предвиђао да директор Агенције може, ако је то потребно из разлога безбедности Републике Србије, својим решењем, а на основу претходне одлуке суда, одредити да се према одређеним физичким и правним лицима предузму одређене мере којима се одступа од начела неповредивости тајне писама и других средстава општења, у поступку утврђеном законом. Иако је стручна јавност на то упозоравала још од 2002. године, чл. 13, 14 и 15 Закона о БИА су проглашени неуставним тек 26. децембра 2013. године (Одлука Уставног суда РС, бр. предмета ИУз-252/2002).

Ова неодређена и недовољно јасна и прецизна одредба је измењена 2014. године. Њена непрецизност и подложност дискреционој одлуци извршне власти се понајвише очитује у чињеници да нису дати никакви ближи критеријуми којима би се одредио круг физичких и правних лица према којима се мере могу одредити, нити су специфициране врста и природа мера и поступака.

Важећа одредба експлицитније одређује да су посебне мере којима се одступа од неповредивости тајне писама и других средстава општења: тајни надзор и снимање комуникације без обзира на облик и техничка средства преко којих се обавља или надзор електронске или друге адресе, тајни надзор и снимање комуникације на јавним местима и местима којима је приступ ограничен или у просторијама, статистички електронски надзор комуникације и информационих система у циљу прибављања података о комуникацији или локацији коришћене мобилне терминалне опреме и рачунарско претраживање већ обрађених личних и других података и њихово упоређивање са подацима који су прикупљени применом претходно наведених мера. Садашње решење је свакако усаглашеније са Закоником о кривичном поступку.

Члан 14 Закона о БИА прописује да се посебне мере могу одредити према лицу, групи или организацији за коју постоје основи сумње да предузима или припрема радње усмерене против безбедности Републике Србије, а околности случаја указују да се на други начин те радње не би могле открити, спречити или доказати или би то изазвало несразмерне тешкоће или велику опасност. Приликом одлучивања о одређивању и трајању посебних мера нарочито се узима у обзир да ли би се исти резултат могао постићи на начин којим се мање ограничавају права грађана, у обиму неопходном да се сврха ограничавања задовољи у демократском друштву (члан 14 став 2). Примену посебне мере предлаже директор агенције, а о њој одлучује суд, и то председник Вишег суда у Београду, односно судија којег он одреди међу судијама који су распоређени у Посебно одељење тог суда за које је законом одређено да поступа у предметима кривичних дела организованог криминала, корупције и других посебно тешких кривичних дела; у року од 48 часова од подношења предлога, што говори да је поштовано начело хитности у прописивању временских оквира. У случају да суд одбије предлог директора агенције, тј. донесе негативно решење, жалба се подноси Апелационом суду у Београду. О жал-

би одлучује веће састављено од троје судија Посебног одељења овог суда, за које је законом одређено да поступа у предметима кривичних дела организованог криминала, корупције и других посебно тешких кривичних дела, у року од 48 часова од часа изјављивања жалбе. Оваквом регулативом посебних мера је начелно поштован уставни принцип по ком једино суд, на основу закона, може одобрити одступање од начела неповредивости писма и друге комуникације.

Одговарајуће одредбе Закона о ВБА и ВОА су својевремено такође успешно оспорене пред Уставним судом Србије, а касније су мењане како би се прилагодиле уставним принципима. До измена закона из 2013. године, директор ВБА је могао да изда налог за примену мере тајног електронског надзора без одобрења суда (чл. 13. ст. 1. у вези са чл. 12. ст. 1. тач. 6) и чл. 16. ст. 2. Закона о ВБА и ВОА). Уставни суд Србије је 1. јуна 2012. године ову законску одредбу прогласио неуставном (Одлука Уставног суда РС, ИУз -1218/2010, од 19.04.2012. године, објављена у Службеном гласнику РС, бр. 88/09). Проблем је што чл. 41 Устава јемчи неповредивост тајности писама и других средстава комуницирања, а одступање се дозвољава само на одређено време и на основу одлуке суда, ако је неопходно ради вођења кривичног поступка или заштите безбедности Републике Србије, на начин предвиђен законом, што је истакнуто у иницијативу за оцену уставности, а Уставни суд прихватио као правно ваљан аргумент. У образложењу одлуке се истицало и позивање на члан 8 Европске конвенције о људским правима, која гарантује право на приватност, као и праксу Европског суда за људска права (Клас и други против Немачке, бр 5029/71(1978); Малоне против Уједињеног Краљевства, бр. 8691/79 (1984); Копланд против Уједињеног Краљевства, бр. 62617/00 (2007)).

Значајно је да се у одлуци Уставног суда истиче шта обухвата појам средства комуникације, сходно пракси Европског суда за људска права: „....не само непосредан садржај комуникација, већ и податке о томе ко је и са ким остварио комуникацију, или је то покушао, у које време, колико дуго је одређени разговор трајао, колико учестало (фреквентно) је комуникација кроз преписку, разговоре или упућене поруке остваривана у одређеном периоду времена и са којих локација је вршена". Ово је касније коришћено као аргумент и приликом оспоравања релевантних одредби Закона о БИА.

На неуставност ове одредбе је упозоравала стручна јавност, а она је констатована и у годишњем извештају Европске комисије о напретку Србије из октобра 2012. године, где је подвучено како је потребно да Србија разјасни и прецизира законски оквир за праћење и надзор комуникација од стране служби безбедности.

Према важећем решењу, директор (или лице које он овласти) је сада овлашћен за предлагање али не и одлучивање о примени мере. Посебан поступак или мера се предузима на основу образложене одлуке надлежног вишег суда. Надлежан је виши суд у седишту апелационог суда чијем подручју се припрема или је предузета радња чије је откривање, праћење и онемогућавање у надлежности ВБА. Председник Вишег суда одређује судије овлашћене за доношење одлуке.

Важну улогу у изградњи правног оквира сајбер безбедности имају закони и пратећа подзаконска регулатива у области заштите података. Најважније врсте података, чије прикупљање, обрада и заштита представљају законску обавезу су су: тајни подаци; подаци о личности; информације од јавног значаја; пословне тајне и професионалне тајне (Закон о тајности података, 2009; Закон о заштити података о личности, 2009; Закон о заштити пословне тајне, 2011; Закон о слободном приступу информацијама од јавног значаја, 2004).

Вреди поменути и прописе којима се регулишу основи информационог система Републике Србије и друга питања о вези примене информационо-комуникационих технологија у свакодневном животу (Закон о информационом систему Републике Србије (Службени гласник РС, бр. 12/96); Закон о ауторским и сродним правима (Службени гласник РС, бр. 104/09, 99/11, 119/12 и 29/16); Закон о електронским комуникацијама (Службени гласник РС, бр. 44/10, 60/13 и 62/14); Закон о електронском потпису (Службени гласник РС, бр. 135/04); Закон о забрани дискриминације (Службени гласник РС, број 22/09) и Закон о заштити потрошача (Службени гласник РС, бр. 73/10 и 6/16).

Можда и најважнији нормативни ослонац сајбер безбедности представљају законске одредбе којима се успоставља систем ране детекције и успешне превенције сајбер напада, уз додељивање јасних овлашћења и обавеза надлежним субјектима. Ове одредбе се налазе у недавно донетом Закону о информационој безбедности (Закон о информационој безбедности, 2016). Члановима 14 и 15. Закона прописано је успостављање Националног ЦЕРТ-а и одређене су његове надлежности, а сам начин вршења послове из надлежности Националног ЦЕРТ-а би требало да буде уређен посебним подзаконским актом. Предуслов за доношење тог општег правног акта и касније функционисање националног ЦЕРТ-а је дефинисање техничких, организационих и правних стандарда и процедура за обављање послове ЦЕРТ-а који су прописани чланом 15 овог Закона. Национални ЦЕРТ у складу са законским одредбама, требало би да прикупља и размењује информације о ризицима за безбедност ИКТ система, као и догађајима који угрожавају безбедност информационо-комуникационих система (ИКТ) и у вези тога обавештава, упозорава и саветује лица која управљају ИКТ системима у Републици Србији, као и јавност.

Коначну слику о потпуности и адекватности нормативног оквира за супротстављање безбедносним ризицима у сајбер простору не можемо добити уколико у разматрање не узмемо и одредбе о заштити од хетерогених видова угрожавања школске деце и младих на Интернету. Електронско насиље – специфична форма вршњачког насиља која је омогућена развојем савремених информационо-комуникационих технологија и која се темељи на злоупотреби различитих технолошких платформи како би се нарушио психички, а некада и физички интегритет жртве, представља нову манифестацију насиља међу младима (Privitera, Campbell, 2009). Млади су, несумњиво, и најчешћи и најлаковерније корисници друштвених мрежа. (Путник et al., 2013: 76). Истраживања показују да је овај феномен у непрестаном порасту. (Li, 2007, Beran, Li, 2005; Поповић-Ћитић et al., 2011:412). Ипак, међу теоретичарима не постоји универ-

зално прихваћена дефиниција електронског насиља. (Patchin, Hinduja, 2006; Hinduja, Patchin, 2008; National Crime Prevention Council, 2006; Smith et al., 2008).

Експлицитан појам електронског насиља као облика вршњачког насиља у домаћем нормативном оквиру налазимо само у одредбама једног подзаконског акта, заснованог на Закону о основама система образовања и васпитања (Службени гласник РС, бр. 72/09, 52/11). Усвајањем овог закона, Србија је започела са испуњавањем обавеза преузетих ратификацијом Конвенције о правима детета и обавезе поступања по препорукама Комитета за права детета из 2008. године (Нешић, Јовић, 2011: 54). Дефиниција електронског насиља, према овом Правилнику, гласи: „електронско насиље и злостављање је злоупотреба информационих технологија која може да има за последицу повреду друге личности и угрожавање достојанства и остварује се слањем порука електронском поштом, СМС-ом, ММС-ом, путем веб-сајта (web сите), четовањем, укључивањем у форуме, социјалне мреже исл“ (Службени гласник РС, бр. 30/10).

Дефинисање појма електронског насиља даје нормативни основ за санкционисање понашања која се не могу обухватити појмом високотехнолошког криминала, али заслужују да буду санкционисана, и потребно је радити и на њиховој превенцији.

Стратешки оквир сајбер безбедности у Републици Србији

Уколико одемо корак даље у истом правцу, можемо закључити да би сајбер безбедност, као део ширег комплекса националне безбедности, требало да буде обухваћена и одредбама општих правних аката и политичко-правних докумената чији су предмет национална безбедност и одбрана. (Стратегија националне безбедности Републике Србије, 2009; Стратегија одбране Републике Србије, 2009; Закон о БИА, 2002; Закон о ВБА и ВОА, 2009; Закон о приватном обезбеђењу, 2013).

У поглављу Стратегије националне безбедности посвећеном представљању најважнијих ризика, изазова и претњи по националну безбедност РС, проблем безбедности сајбер простора (у ограниченом смислу) је елаборирaн у једној реченици: „тенденција повећаног коришћења информационо-комуникационих технологија праћена је константним повећањем ризика од високотехнолошког криминала и угрожавања информационих и телекомуникационих система. Ризик у овом погледу постоји од угрожавања споља, али и у могућности злоупотребе података о грађанима и правним лицима.“ Чини нам се да је ово недовољно за представљање једног од водећих глобалних безбедносних изазова савременог света.

Занимљиво је да творци Стратегије, набрајајући елементе политике националне безбедности, потпуно превиђају потребу за формулисањем политике информационе (сајбер) безбедности као засебног елемента, чиме се овом важном безбедносном изазову даје другоразредни значај. У нескладу са актуелном

безбедносном ситуацијом је и опредељење носилаца Стратегије да у оквире структуре система националне безбедности не укључе посебне органе/институције које би се бавиле информационом (сајбер) безбедношћу.

Иако се у закључку Стратегије наводи да је она заснована на савременим теоријским сазнањима у области безбедности, националним искуствима и безбедносним потребама друштва, као и искуствима других држава у креирању система националне безбедности и решавању ризика и претњи безбедности, очигледни су крупни превиди којима је област од суштинског значаја за националну безбедност стављена у други план.

Проблему сајбер безбедности не посвећује довољно пажње ни Стратегија одбране Републике Србије, о којој се он помиње једино у одељку о безбедносним ризицима, изазовима и претњама, где се истиче: „Развојем савремених информационих технологија које су битан део системског уређења и остваривања функција државе, настају нове околности за деловање различитих група и недржавних актера у остваривању њихових циљева. На тај начин може да дође до угрожавања функционисања битних елемената система одбране кроз деловање сајбер претњи. Због тога је неопходно континуирано развијати технолошку и процедуралну заштиту елемената система одбране на свим нивоима организовања“ (Стратегија одбране Републике Србије, 2009: 9).

Закључна разматрања

Проблем стварања безбедног сајбер окружења је вишедимензионалан и захтева координисано деловање различитих чинилаца. Нормативна регулатива у сфери сајбер безбедности је од великог значаја, али уколико изостану стратегије, политике, акциони планови и мере којима се имплементирају законска решења, сви напори законодавца остају узалудни. Република Србија је последњих година унапредила национални правни оквир за супротстављање високотехнолошком криминалу и изградњу безбеднијег сајбер простора, али, на основу изнете анализе, закључујемо да исти још увек није на потребном нивоу.

Ово се посебно односи на чињеницу да још увек нису донете посебне стратегије сајбер безбедности и сајбер одбране (иако су надлежни скупштински одбор и владина Канцеларија Савета за националну безбедност указивали на неопходност њеног доношења још од 2013. године), што указује на непостојање системског приступа питању које је од суштинске важности за очување националне безбедности. Новодонети Закон о информационој безбедности није праћен одговарајућом подзаконском регулативом иако су законски рокови за њено доношење истекли. Хармонизација нашег права са одговарајућим међународним стандардима ће остати пуко испуњавање форме уколико се не предузму конкретни потези за усаглашавање друштвене и нормативне стварности, како би потоња постала чврст оквир за одговор на актуелне безбедносне ризике.

Забрињавајуће је и што одредбе закона којима се додељују овлашћења за предузимање специјалних истражних техника, посебних мера и поступака, низ година нису били усклађени са Уставом и међународним уговорима и стандардима заштите неповредивости тајности писма и других средстава комуникације. Иако су, након одговарајућих одлука Уставног суда и каснијих законодавних промена, отклоњене неусаглашености са Уставом, не чини се практичним и функционалним да закони који регулишу рад различитих служби безбедности, те Законик о кривичном поступку, имају неуједначену терминологију, па се и врсте посебних мера и поступака разликују (можда не суштински, али и ту остаје простор за недоумице и различита тумачења).

Ово се посебно односи на Закон о БИА и Закон о ВБА и ВОА, који би, с једне стране, свакао требали да се појмовно и материјално ускладе са Закоником о кривичном поступку, али, са друге стране, и да се међусобно поклапају. Можда би боље решење било да Закон о основама уређења служби безбедности на јединствен начин пропише врсте и начин примене посебних мера и поступака служби безбедности, а да предметни закони регулишу само специфичности у начину предузимања мере (посебно у односу на врсту физичких и правних лица према којима се одређују, услед различитог опсега деловања војних служби безбедности). На овај начин би се постигла већа правна сигурност грађана, а обавештајно-безбедносни подсистем сектора националне безбедности би деловао јединственије и хармоничније. Свакако, треба имати у виду да висок степен тајности нужно карактерише рад са обавештајно-безбедносним подацима, услед чега је потребно поштовати и начело ефикасности и економичности рада служби безбедности, које не сме бити нарушено неоправдано рестриктивним приступом законодавца. Очигледно, у овој области је неопходно еквилибрирати између различитих захтева – транспарентности и демократске контроле и заштите безбедности државе, при чему тасови на ваги не смеју отићи исувише на једну или другу страну.

Литература:

1. Beran, T. N., Li, Q. (2005). Cyber-harassment: A study of a new method for an old behavior. *Journal of Educational Computing Research*, 32(3), 265-277.
2. Boyd, D. (2007).Why youth (heart) social networks site: The role of networked publics in teenage social life. In D. Buckingham (ed.), *MacArthur Foundation Series on Digital Learning – Youth, Identity, and Digital Media Volume*. Cambridge, MA: MIT Press.
3. Vučinić Z. *(*2001). *Međunarodno ratno i humanitarno pravo*. Beograd: Vojnoizdavački zavod.
4. Gross, E. F., Juvonen, J., Gable, S. L. (2002). Internet use and well-being in adolescence. *Journal of Social Issues*, 58(1), 75-90.
5. Zakon o autorskim i srodnim pravima (Službeni glasnik RS, br. 104/09, 99/11, 119/12 i 29/16)
6. Zakon o Bezbednosno-informativnoj agenciji, (Sl. glasnik RS", br. 42/2002, 111/2009, 65/2014 - odluka US i 66/2014)

7. Zakon o vojnobezbednosnoj agencijiji i vojnoobaveštajnoj agenciji (Sl. glasnik RS", br. 88/2009, 55/2012 - odluka US i 17/2013)
8. Zakon o elektronskim komunikacijama (Službeni glasnik RS, br. 44/10, 60/13 i 62/14)
9. Zakon o elektronskom potpisu (Službeni glasnik RS, br. 135/04)
10. Zakon o informacionom sistemu Republike Srbije (Službeni glasnik RS, br. 12/96)
11. Zakon o izmenama i dopunama Krivičnog zakona Republike Srbije (Sl. glasnik RS br. 39/03)
12. Zakon o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala, Službeni glasnik Republike Srbije br. 61/05, 104/09.
13. Zakon o osnovama sistema obrazovanja i vaspitanja (Službeni glasnik RS, br. 72/09, 52/11
14. Zakon o potvrđivanju Dodatnog protokola uz Konvenciju o visokotehnološkom kriminalu koji se odnosi na inkriminaciju dela rasističke i ksenofobične prirode izvršenih preko računarskih sistema, Službeni glasnik Republike Srbije broj 19/09
15. Zakon o potvrđivanju Konvencije o visokotehnološkom kriminalu, Službeni glasnik Republike Srbije broj 19/09
16. Zakon o potvrđivanju Konvencije o pravima deteta, "Službeni list SFRJ-Međunarodni ugovori", br.15/90)
17. Zakon o privatnom obezbeđenju, (Sl. glasnik RS br. 104/2013 i 42/2015)
18. Zakonom o slobodnom pristupu informacijama od javnog značaja (Sl. glasnik RS br. 120/04, 54/07, 104/09, 36/10)
19. Zakon o tajnosti podataka ((Sl. glasnik RS br. 104/09)
20. Zakon o zabrani diskriminacije (Službeni glasnik RS, broj 22/09)
21. Zakon o zaštiti podataka o ličnosti (Sl. glasnik RS br. 97/08, 104/09 - dr. zakon, 68/12 - US, 107/12)
22. Zakon o zaštiti poslovne tajne (Sl. glasnik RS br. 72/11)
23. Zakon o zaštiti potrošača (Službeni glasnik RS, br. 73/10 i 6/16)
24. Zakon o zaštiti podataka o ličnosti (Službeni glasnik RS, br. 97/08, 104/09, 68/12 i 107/12)
25. Zakonik o krivičnom postupku (*Službeni glasnik RS*, br. 72/11, 101/11, 121/12, 32/13, 45/13, 55/14)
26. Convention on Cybercrime, Council of Europe, *Convention on Cybercrime*, 23 November 2001, Dostupno na: http://www.refworld.org/docid/47fdfb202.html
27. International Court of Justice, Legality of the Threat or Use of Nuclear Weapons, advisory opinion, 1996
28. Krivični zakonik Republike Srbije (Službeni glasnik RS br. 85/2005, 88/2005 - ispr., 107/2005 - ispr., 72/2009, 111/2009, 121/2012, 104/2013, 108/2014 i 94/16)
29. Li, Q. (2007). New bottle but old wine: A research of cyberbullying in schools. *Computers in Human Behavior*, 23(4), 1777-1791.
30. Milošević, M., Putnik, N. (2014). Problem pravne (ne)regulisanosti konflikata u kiber prostoru, *Treći program*, ISSN 0564-7010, sveska br. 162 (2/2014)
31. Mladenović, D. (2012). *Međunarodni aspekt sajber ratovanja*. Beograd: Medija centar „Odbrana“.
32. Melzer, N. (2011). *Cyberwarfare and International Law.* Geneva: UNIDIR.
33. National Crime Prevention Council (2006). *Cyberbullying*. http://www.ncpc.org/cyberbullying
34. Nešić, S., Jović, N. (2011). *Zaštita dece od nasilja u školama – izveštaj zaštitnika građana i panela mladih savetnika*. Beograd: Zaštitnik građana
35. Odluka Ustavnog suda RS, IUz -1218/2010, od 19.04.2012. godine, objavljena u Službenom glasniku RS, br. 88/09.

36. Odluka Ustavnog suda RS, IUz -252/2002, od 26. decembra 2013. godine, objavljena u Službenom glasniku RS, br. 65/2014. Tekst dostupan na: http://www.ustavni.sud.rs/Storage/Global/Documents/Misc/%D0%9E%D0%B4%D0%BB%D1%83%D0%BA%D0%B0%20I%D0%A3%D0%B7-252-2002.pdf
37. Patchin, J. W., Hinduja, S. (2006). Bullies move beyound the schoolyard: A preliminary look at cyberbullying. *Youth violence and juvenile justice*, 4(2), 148-169.
38. Popović-Ćitić, Djurić, Cvetković. (2011). The prevalence of cyberbullying among adolescents: A case study of middle schools in Serbia. *School Psychology International*, 32(4), 412–424.
39. Pravilnik o protokolu postupanja u ustanovi u odgovoru na nasilje, zlostavljanje i zanemarivanje (*Službeni glasnik RS*, br. 30/10)
40. Privitera, C., Campbell, M. (2009). Cyberbullying: The new face of workplace bullying? *CyberPsychology & Behavior*, 12(4), 395-400.
41. Putnik, N. (2009). *Sajber prostor i bezbednosni izazovi*. Beograd: Fakultet bezbednosti.
42. Putnik N., Milošević, M., Cvetković, V. (2013). Problem zaštite obrazovno-vaspitnih ustanova od visokotehnološkog kriminala i elektronskog nasilja. *Sociološki pregled,* Vol. XLVII (januar-mart 2013), br. 1, 75 – 92.
43. Smith, P. K., Mahdavi, J., Carvalho, M., Fisher, S., Russell, S., Tippett, N. (2008). Cyberbullying: Its nature and impact in secondary school pupils. *The Journal of Child Psychology and Psychiatry and Allied Disciplines*, 49(4), 376-385.
44. Stojanović, Z. (2012). Komentar Krivičnog zakonika. Beograd, Srbija: Službeni glasnik.
45. Strategija nacionalne bezbednosti Republike Srbije, 2009
46. Strategija odbrane Republike Srbije, 2009
47. Strategija razvoja informacionog društva u Republici Srbiji do 2020. godine, Službeni glasnik Republike Srbije broj 51/2010
48. *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Michael N. Schmitt (Ed.). Cambridge, New York: Cambridge University Press, 2013.
49. Urošević, V., Ivanović, Z., Uljanov, S. (2012). *Mač u world wide web-u*. Beograd: Eternal mix,
50. Hinduja, S., Patchin, J. (2008). Cyberbullying: An exploratory analysis of factors related to offending and victimization. *Deviant Behavior*, 29(2), 129-156.

CYBER SECURITY AND THE PROTECTION FROM CYBER CRIME IN SERBIA – STRATEGIC AND LEGAL FRAMEWORK

Summary: Due to outburst of contemporary informational tehnologies and growing IT dependence of post-modern society, cyber security developed into one of the most important fields of security studies. This interdisciplinary area requires multidimensional approach and strong coordination of all concerned subjects. The adequate strategic and legal framework is sine qua non condition for establishing solid ground in fight against cyber crime and other forms of cyber insecurity. International humanitarian law, with its contractual regimes, principles and regulations is developed as a normative framework for conventional warfare but it lacks precise norms tahta could regulate the legal status of cyber operations. The interpretations of existing international law, es extensive as it can be, still don't provide undoubtfull answers to all of the basic questions. National normative framework in Serbia consists of numerous laws and regulations, which are primiraly, focused on other fields, but partially regulate the matter of cyber security. Recently adopted Law on informational security is an important step ahead but it will not provide needed results until gover-

mental regulations based on this Law are adopted in order to secure the implementation. The authors present and analyze mentioned laws and regulations, pointing to certain unappropriate solutions and the lack of complete and precise norms. Also, the authors provide insight into strategic documents in this area and underline the fact that Serbia still lacks strategy of cyber security and defense. Finnaly, the authors deal with problem that arise from certain doubtfull legal solutions in the matter of the use of special investigative techniques and methods by security services and the subjects of criminal procedure and suggest legislative changes that could lead to safer cybrspace and bettet results in fight against cyber threats.

Key words: cyber security, high-tech crime, legislation, security strategy